kaspersky

Kaspersky Endpoint Security 14.2 for Windows

© 2026 AO Kaspersky Lab

Sommario

Guida di Kaspersky Endpoint Security for Windows
- Novità
- Problemi risolti
- Domande frequenti

Kaspersky Endpoint Security for Windows
- Modalità dell'applicazione: Standard, EDR Agent, Light Agent
- Kit di distribuzione
- Requisiti hardware e software
- Confronto tra le funzionalità delle applicazioni disponibili a seconda del tipo di sistema operativo
- Confronto tra le funzioni dell'applicazione in base agli strumenti di gestione
- Compatibilità con altre applicazioni

Installazione e rimozione dell'applicazione
- Distribuzione tramite Kaspersky Security Center
  - Installazione standard dell'applicazione
  - Creazione di un pacchetto di installazione
  - Aggiornamento dei database nel pacchetto di installazione
  - Creazione di un'attività di installazione remota
- Installazione dell'applicazione in locale tramite la procedura guidata
- Installazione remota dell'applicazione tramite System Center Configuration Manager
- Descrizione delle impostazioni di installazione del file setup.ini
- Processi di Kaspersky Endpoint Security for Windows
- Modifica componenti dell'applicazione
- Upgrade di una versione precedente dell'applicazione
  - Upgrade dell'applicazione senza un riavvio
  - Aggiornamento SMU dell'applicazione
- Rimozione dell'applicazione

Licensing dell'applicazione
- Informazioni sul Contratto di licenza con l'utente finale
- Informazioni sulla licenza
- Informazioni sul certificato di licenza
- Informazioni sull'abbonamento
- Informazioni sulla chiave di licenza
- Informazioni sul codice di attivazione
- Informazioni sul file chiave
- Confronto delle funzionalità dell'applicazione in base al tipo di licenza per le workstation
- Confronto delle funzionalità dell'applicazione in base al tipo di licenza per i server
- Attivazione dell'applicazione
- Rimozione di una chiave di licenza
- Visualizzazione delle informazioni sulla licenza
- Acquisto di una licenza
- Rinnovo dell'abbonamento

Guida introduttiva
- Informazioni sul plug-in di gestione di Kaspersky Endpoint Security for Windows
- Considerazioni speciali in caso di utilizzo di versioni diverse dei plug-in di gestione
- Considerazioni speciali quando si utilizzano protocolli criptati per l'interazione con servizi esterni
- Interfaccia dell'applicazione
  - Icona dell'applicazione nell'area di notifica della barra delle applicazioni
  - Interfaccia dell'applicazione semplificata
  - Configurazione della visualizzazione dell'interfaccia dell'applicazione
- Preparazione dell'applicazione per l'utilizzo
- Gestione dei criteri
  - Creazione di un criterio
  - Esportazione e importazione di un criterio
  - Indicatore del livello di sicurezza
- Gestione attività
- Configurazione delle impostazioni locali dell'applicazione
- Avvio e arresto di Kaspersky Endpoint Security
- Sospensione e ripresa della protezione e del controllo del computer
- Creazione e utilizzo di un file di configurazione
- Ripristino delle impostazioni predefinite dell'applicazione
- Prestazioni di Kaspersky Endpoint Security e compatibilità con altre applicazioni
  - Abilitazione o disabilitazione della modalità di risparmio energetico
  - Abilitazione o disabilitazione della concessione di risorse ad altre applicazioni
  - Best practice per l'ottimizzazione delle prestazioni di Kaspersky Endpoint Security

Scansione malware
- Scansione del computer
- Scansione delle unità rimovibili quando vengono connesse al computer
- Scansione in background
- Scansione dal menu di scelta rapida
- Controllo dell'integrità dell'applicazione
- Modifica dell'ambito della scansione
- Esecuzione di una scansione pianificata
- Esecuzione di una scansione come utente diverso
- Ottimizzazione della scansione

Aggiornamento di database e moduli software dell'applicazione
- Scenari di aggiornamento dei database e dei moduli dell'applicazione
  - Aggiornamento da un archivio server
  - Aggiornamento da una cartella condivisa
  - Aggiornamento tramite Kaspersky Update Utility
  - Aggiornamento in modalità mobile
- Avvio e arresto di un'attività di aggiornamento
- Avvio di un'attività di aggiornamento tramite i diritti di un account utente differente
- Selezione della modalità di esecuzione dell'attività di aggiornamento
- Aggiunta di una sorgente degli aggiornamenti
- Aggiornamento dei moduli dell'applicazione
- Utilizzo di un server proxy per gli aggiornamenti
- Ultimo rollback degli aggiornamenti

Tecnologia Disinfezione avanzata
Disinfezione delle minacce attive nelle workstation
Disinfezione delle minacce attive nei server
Eliminazione delle minacce non elaborate
Protezione del computer
Stato della protezione in tempo reale
Protezione minacce file
Abilitazione e disabilitazione di Protezione minacce file
Sospensione automatica di Protezione minacce file
Modifica dell'azione eseguita sui file infetti dal componente Protezione minacce file
Creazione dell'ambito di protezione del componente Protezione minacce file
Utilizzo dei metodi di scansione
Utilizzo delle tecnologie di scansione durante l'esecuzione del componente Protezione minacce file
Ottimizzazione della scansione dei file
Scansione dei file compositi
Modifica della modalità di scansione
Scansione dei contenitori
Prevenzione Intrusioni Host
Abilitazione e disabilitazione di Prevenzione Intrusioni Host
Gestione dei gruppi di attendibilità delle applicazioni
Modifica del gruppo di attendibilità di un'applicazione
Configurazione dei diritti dei gruppi di attendibilità
Selezione di un gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security
Selezione di un gruppo di attendibilità per le applicazioni sconosciute
Selezione di un gruppo di attendibilità per le applicazioni firmate digitalmente
Gestione dei diritti delle applicazioni
Protezione delle risorse del sistema operativo e dei dati di identità
Eliminazione delle informazioni relative alle applicazioni inutilizzate
Monitoraggio di Prevenzione Intrusioni Host
Protezione dell'accesso ad audio e video
Prevenzione Attacchi BadUSB
Abilitazione e disabilitazione di Prevenzione Attacchi BadUSB
Utilizzo di Tastiera sullo schermo per l'autorizzazione di dispositivi USB
Autorizzazione del lettore di codici a barre
Protezione AMSI
Abilitazione e disabilitazione di Protezione AMSI
Ottimizzazione della scansione dei file tramite Protezione AMSI
Protezione minacce Web
Abilitazione e disabilitazione di Protezione minacce web
Configurazione dei metodi di rilevamento degli indirizzi Web dannosi
Anti-Phishing
Creazione dell'elenco di indirizzi Web attendibili
Esportazione e importazione dell'elenco degli indirizzi Web attendibili
Protezione minacce di posta
Abilitazione e disabilitazione di Protezione minacce di posta
Modifica dell'azione da eseguire sui messaggi e-mail infetti
Creazione dell'ambito di protezione del componente Protezione minacce di posta

- Scansione dei file compositi allegati ai messaggi e-mail
- Filtraggio degli allegati dei messaggi e-mail
- Esportazione e importazione delle estensioni per il filtro degli allegati
- Scansione dei messaggi e-mail in Microsoft Office Outlook
- Scansione delle e-mail in Thunderbird, MyOffice, R7-Office

Protezione minacce di rete
- Abilitazione e disabilitazione di Protezione minacce di Rete
- Blocco di un computer che ha originato l'attacco
- Configurazione degli indirizzi delle esclusioni dal blocco
- Esportazione e importazione dell'elenco delle esclusioni dal blocco
- Configurazione di Protezione minacce di rete in base al tipo

Firewall
- Abilitazione o disabilitazione di Firewall
- Modifica del tipo di connessione di rete
- Gestione delle regole per i pacchetti di rete
  - Creazione di una regola per i pacchetti di rete
  - Abilitazione o disabilitazione di una regola per i pacchetti di rete
  - Modifica dell'azione eseguita da Firewall per una regola per i pacchetti di rete
  - Modifica della priorità di una regola per i pacchetti di rete
  - Esportazione e importazione di regole per i pacchetti di rete
  - Definizione delle regole per i pacchetti di rete in XML
- Gestione delle regole di rete delle applicazioni
  - Creazione di una regola di rete dell'applicazione
  - Abilitazione e disabilitazione di una regola di rete per un'applicazione
  - Modifica dell'azione eseguita da Firewall per una regola di rete per un'applicazione
  - Modifica della priorità di una regola di rete per un'applicazione
- Monitor di Rete

Prevenzione Exploit
- Abilitazione e disabilitazione di Prevenzione Exploit
- Protezione della memoria dei processi di sistema

Rilevamento del Comportamento

Anti-Cryptor
- Abilitazione e disabilitazione della protezione delle cartelle condivise dal criptaggio esterno
- Configurazione del periodo di blocco di un computer non attendibile
- Modifica dell'ambito di protezione
- Aggiunta di computer attendibili per il criptaggio dei dati esterni
- Esportazione e importazione di un elenco di esclusioni dalla protezione delle cartelle condivise dal criptaggio esterno

Motore di Remediation

Kaspersky Security Network
- Abilitazione e disabilitazione dell'utilizzo di Kaspersky Security Network
- Limitazioni di Kaspersky Private Security Network
- Abilitazione e disabilitazione della modalità cloud per i componenti della protezione
- Impostazioni proxy KSN
- Controllo della reputazione di un file in Kaspersky Security Network

Scansione delle connessioni criptate
- Abilitazione della scansione delle connessioni criptate
- Installazione di certificati radice attendibili

Scansione delle connessioni criptate con un certificato non attendibile
Aggiunta del certificato Kaspersky al proprio archivio certificati
Esclusione delle connessioni criptate dalla scansione
Blocco dell'accesso ai domini con certificati non attendibili
Cancella dati
Controllo del computer
Controllo Web
Aggiunta di una regola di accesso alle risorse Web
Filtro in base agli indirizzi delle risorse Web
Filtro in base ai contenuti delle risorse Web
Verifica delle regole di accesso alle risorse Web
Esportazione e importazione delle regole di Controllo Web
Esportazione e importazione di indirizzi di risorse Web della regola di Controllo Web
Monitoraggio dell'attività Internet dell'utente
Modifica dei modelli dei messaggi di Controllo Web
Modifica delle maschere per gli indirizzi di risorse Web
Controllo Web per macchine virtuali
Variabili nei modelli di messaggi di Controllo Web
Controllo dispositivi
Informazioni sulle regole di accesso
Recupero di informazioni sui dispositivi installati
Gestione dell'accesso ai dispositivi in base al tipo
Gestione dell'accesso ai dispositivi tramite il bus di connessione
Differenziazione dei diritti di accesso degli utenti ai dispositivi
Gestione dell'accesso ai dispositivi mobili
Gestione dell'accesso ai dispositivi Bluetooth
Controllo della stampa
Controllo delle connessioni Wi-Fi
Monitoraggio dell'utilizzo delle unità rimovibili
Modificare la durata della memorizzazione nella cache
Azioni con i dispositivi attendibili
Aggiunta di un dispositivo all'elenco dei dispositivi attendibili
Esportazione e importazione dell'elenco dei dispositivi attendibili
Ottenimento dell'accesso a un dispositivo bloccato
Modalità online per la concessione dell'accesso
Modalità offline per la concessione dell'accesso
Modifica dei modelli dei messaggi di Controllo dispositivi
Anti-Bridging
Abilitazione di Anti-Bridging
Modifica dello stato di una regola di connessione
Modificare la priorità di una regola di connessione
Controllo adattivo delle anomalie
Addestramento di Controllo adattivo delle anomalie
Abilitazione e disabilitazione di una regola di Controllo adattivo delle anomalie
Modifica dell'azione eseguita quando viene attivata una regola di Controllo adattivo delle anomalie
Creazione di un'esclusione per una regola di Controllo adattivo delle anomalie
Esportazione e importazione delle esclusioni per le regole di Controllo adattivo delle anomalie

- Applicazione degli aggiornamenti per le regole di Controllo adattivo delle anomalie
- Modifica dei modelli dei messaggi di Controllo adattivo delle anomalie
- Monitoraggio delle operazioni di Controllo adattivo delle anomalie

Controllo applicazioni

- Limitazioni delle funzionalità di Controllo applicazioni
- Ottenimento di informazioni sulle applicazioni installate
- Come abilitare la modalità Applicazioni bloccate
- Controllo applicazioni basato su un computer di base
- Gestione delle regole di Controllo applicazioni
  - Aggiunta di una condizione di attivazione per la regola di Controllo applicazioni
  - Aggiunta di file eseguibili dalla cartella File eseguibili alla categoria di applicazioni
  - Aggiunta di file eseguibili correlati agli eventi alla categoria di applicazioni
  - Aggiunta di una regola di Controllo applicazioni
  - Modifica dello stato di una regola di Controllo applicazioni tramite Kaspersky Security Center
  - Esportazione e importazione delle regole di Controllo applicazioni
  - Visualizzazione degli eventi generati dall'esecuzione del componente Controllo applicazioni
  - Visualizzazione di un rapporto sulle applicazioni bloccate
- Verifica delle regole di Controllo applicazioni
  - Abilitazione e disabilitazione del test delle regole di controllo delle applicazioni
  - Visualizzazione di un rapporto sulle applicazioni bloccate in modalità di test
  - Visualizzazione degli eventi generati dall'operazione di test del componente Controllo applicazioni
- Monitor attività applicazioni
- Regole per la creazione delle maschere dei nomi per file o cartelle
- Modifica dei modelli dei messaggi di Controllo applicazioni
- Variabili nei modelli di messaggi di Controllo applicazioni
- Procedure consigliate per l'inventario dei file eseguibili
- Best practice per l'implementazione di un elenco di applicazioni consentite
  - Configurazione della modalità Lista consentiti per le applicazioni
  - Test della modalità Lista consentiti
  - Supporto per la modalità Lista consentiti

Monitoraggio delle porte di rete

- Abilitazione del monitoraggio di tutte le porte di rete
- Creazione di un elenco di porte di rete monitorate
- Creazione di un elenco di applicazioni per cui monitorare tutte le porte di rete
- Esportazione e importazione degli elenchi delle porte monitorate

Log Inspection

- Configurazione delle regole predefinite
- Aggiunta delle regole personalizzate

Monitoraggio integrità di sistema

- Informazioni sulle regole di Monitoraggio integrità di sistema
- Monitoraggio integrità di sistema in tempo reale
- Controllo integrità di sistema su richiesta
- Esportazione e importazione delle regole di Monitoraggio integrità di sistema
- Visualizzazione dei rapporti di Monitoraggio integrità di sistema
- Ripristino dello stato di integrità del sistema

Cloud Discovery

Area attendibile
Creazione di un'esclusione dalla scansione
Creazione di un'esclusione in base al tipo di oggetti rilevati
Modifica dell'elenco di applicazioni attendibili
Creazione di un'area attendibile locale
Esportazione e importazione dell'area attendibile
Gestione delle applicazioni con una firma digitale attendibile
Appendice. Esclusioni dalle scansioni predefinite e applicazioni attendibili.
Microsoft SQL Server
Microsoft Exchange Server
Microsoft System Center Configuration Manager
Citrix
VMware
Deduplicazione dei dati in Microsoft Windows Server
Gestione di Backup
Configurazione del periodo massimo di archiviazione per i file in Backup
Configurazione della dimensione massima di Backup
Ripristino di file da Backup
Eliminazione delle copie di backup dei file da Backup
Servizio di notifica
Configurazione delle impostazioni del registro eventi
Configurazione della visualizzazione e dell'invio delle notifiche
Configurazione della visualizzazione degli avvisi sullo stato dell'applicazione nell'area di notifica
Invio di messaggi tra gli utenti e l'amministratore
Gestione dei rapporti
Visualizzazione dei rapporti
Configurazione del periodo massimo di archiviazione dei rapporti
Configurazione della dimensione massima dei file del rapporto
Salvataggio di un rapporto in un file
Eliminazione dei rapporti
Auto-difesa di Kaspersky Endpoint Security
Abilitazione e disabilitazione di Auto-difesa
Abilitazione e disabilitazione del supporto AM-PPL
Protezione dei servizi applicativi contro la gestione esterna
Supporto delle applicazioni di amministrazione remota
Protezione tramite password
Abilitazione della protezione tramite password
Concessione delle autorizzazioni a singoli utenti o gruppi
Utilizzo di una password provvisoria per concedere le autorizzazioni
Revoca delle password provvisorie
Caratteristiche speciali delle autorizzazioni di Protezione tramite password
Reimpostazione della password KLAdmin
Protezione della connessione ad Administration Server
Criptaggio dei dati
Limitazioni della funzionalità di criptaggio
Modifica della lunghezza della chiave di criptaggio (AES56 / AES256)

Criptaggio disco Kaspersky
- Funzionalità speciali di criptaggio dell'unità SSD
- Avvio di Criptaggio disco Kaspersky
- Creazione di un elenco di dischi rigidi esclusi dal criptaggio
- Esportazione e importazione di un elenco di dischi rigidi esclusi dal criptaggio
- Abilitazione della tecnologia Single Sign-On (SSO)
- Gestisci account dell'Agente di Autenticazione
- Utilizzo di un token o una smart card con l'agente di autenticazione
- Decriptaggio dei dischi rigidi
- Ripristino dell'accesso a un'unità protetta dalla tecnologia Criptaggio disco Kaspersky
- Accesso con l'account di servizio dell'Agente di Autenticazione
- Aggiornamento del sistema operativo
- Eliminazione degli errori di aggiornamento della funzionalità di criptaggio
- Tracciamento dell'Agente di Autenticazione
- Modifica del testo della Guida dell'Agente di Autenticazione
- Rimozione di oggetti e dati rimanenti dopo aver verificato il funzionamento dell'Agente di Autenticazione

BitLocker Management
- Avvio di Crittografia unità BitLocker
- Decriptaggio di un disco rigido protetto da BitLocker
- Ripristino dell'accesso a un'unità protetta da BitLocker
- Sospensione della protezione BitLocker per aggiornare il software

Criptaggio a livello di file nelle unità locali del computer
- Criptaggio dei file nelle unità locali del computer
- Creazione delle regole di accesso ai file criptati per le applicazioni
- Criptaggio dei file creati o modificati da applicazioni specifiche
- Generazione di una regola di decriptaggio
- Decriptaggio dei file nelle unità locali del computer
- Creazione di pacchetti criptati
- Ripristino dell'accesso ai file criptati
- Ripristino dell'accesso ai dati criptati dopo un errore del sistema operativo
- Modifica dei modelli di messaggi per l'accesso ai file criptati

Criptaggio unità rimovibili
- Avvio del criptaggio delle unità rimovibili
- Aggiunta di una regola di criptaggio per le unità rimovibili
- Esportazione e importazione di un elenco di regole di criptaggio per unità rimovibili
- Modalità portatile per l'accesso ai file criptati nelle unità rimovibili
- Decriptaggio delle unità rimovibili

Visualizzazione dei dettagli sul criptaggio dei dati
- Visualizzazione dello stato di criptaggio
- Visualizzazione delle statistiche di criptaggio nei dashboard di Kaspersky Security Center
- Visualizzazione degli errori di criptaggio dei file nelle unità locali del computer
- Visualizzazione del rapporto sul criptaggio dei dati

Utilizzo dei dispositivi criptati quando non è possibile accedervi
- Ripristino dei dati utilizzando l'utilità di ripristino FDERT
- Creazione di un Rescue Disk del sistema operativo

Soluzioni Detection and Response
- Licenze di MDR ed EDR Optimum
- Compatibilità con le soluzioni EDR di terzi
- Kaspersky Endpoint Agent
  - Migrazione della configurazione [KES+KEA] alla configurazione [KES+agente integrato]
  - Migrazione di criteri e attività per Kaspersky Endpoint Agent
- Endpoint Detection and Response Agent (EDR Agent)
  - Installazione di EDR Agent
  - Integrazione di EDR Agent con MDR
  - Integrazione di EDR Agent con EDR (KATA)
  - Integrazione di EDR Agent con NDR (KATA)
  - Integrazione di EDR Agent con EDR Expert (on-premises)
  - Compatibilità con le applicazioni EPP di terzi
- Managed Detection and Response
  - Integrazione dell'agente integrato con MDR
  - Guida alla migrazione da KEA a KES per MDR
- Endpoint Detection and Response
  - Integrazione dell'agente integrato con EDR Optimum/EDR Expert
  - Scansione degli indicatori di compromissione (attività standard)
  - Telemetria estesa per la scansione IOC
  - Sposta il file in Quarantena
  - Ottieni file
  - Elimina file
  - Avvio del processo
  - Termina processo
  - Prevenzione dell'esecuzione
  - Isolamento di rete del computer
  - Sandbox cloud
  - Guida alla migrazione da KEA a KES per EDR Optimum
- Kaspersky Sandbox
  - Integrazione dell'agente integrato con Kaspersky Sandbox
  - Scansione degli indicatori di compromissione (attività standalone)
  - Guida alla migrazione da KEA a KES per Kaspersky Sandbox
- Kaspersky Anti Targeted Attack Platform
  - Integrazione dell'agente integrato con EDR / NDR (KATA)
  - Configurazione della telemetria EDR (KATA).
  - Esclusioni della telemetria EDR (KATA)
    - Esempio 1. Processi esclusi
    - Esempio 2. Comunicazioni di rete escluse
    - Esempio 3. Operazioni sui file escluse
    - Esempio 4. Modifiche al Registro di sistema escluse
  - KATA Sandbox
    - Integrazione dell'agente integrato con KATA Sandbox
    - Configurazione delle azioni di risposta alle minacce
  - Guida alla migrazione da KEA a KES per EDR (KATA)

- Endpoint Detection and Response Expert (on-premises)
  - Integrazione dell'agente integrato con EDR Expert (on-premises)
  - Configurazione delle impostazioni di telemetria EDR Expert (on-premises)
  - Esclusioni della telemetria EDR Expert (on-premises)
  - Esportazione e importazione dei filtri eventi EDR Expert (on-premises).
  - Considerazioni speciali sull'utilizzo dei profili criterio per configurare l'integrazione con EDR Expert (on-premises) ed EDR (KATA)
- Endpoint Detection and Response Expert (cloud)
  - Integrazione dell'agente integrato con EDR Expert (cloud)
  - Configurazione delle impostazioni di telemetria EDR Expert (cloud)
  - Esclusioni della telemetria EDR Expert (cloud)
  - Come esportare o importare i filtri degli eventi di EDR Expert (cloud)
- Gestione della quarantena
  - Configurazione della dimensione massima della quarantena
  - Invio dei dati relativi ai file in quarantena a Kaspersky Security Center
  - Ripristino dei file dalla quarantena
- Monitoraggio delle azioni EDR

Kaspersky Unified Monitoring and Analysis Platform (KUMA)
- Integrazione di Kaspersky Endpoint Security con KUMA
  - Preparazione dell'integrazione di KES con KUMA
  - Connessione di KES a KUMA
- Filtraggio degli eventi da inviare a KUMA
- Esportazione e importazione di filtri degli eventi KUMA

Guida alla migrazione da KSWS a KES
- Corrispondenza dei componenti di KSWS e KES
- Corrispondenza delle impostazioni di KSWS e KES
- Migrazione dei componenti di KSWS
- Migrazione delle attività e dei criteri di KSWS
- Migrazione della zona attendibile di KSWS
- Migrazione delle regole di Controllo degli avvii delle applicazioni di KSWS
- Installazione di KES anziché KSWS
- Migrazione della configurazione [KSWS+KEA] alla configurazione [KES+agente integrato]
- Assicurarsi che Kaspersky Security for Windows Server sia stato rimosso correttamente
- Attivazione di KES con una chiave di KSWS
- Considerazioni speciali per la migrazione di server a carico elevato
- Gestione dell'applicazione in un server in modalità Server Core
- Migrazione da [KSWS+KEA] a [KES+agente integrato]

Modalità Light Agent per proteggere le macchine virtuali
- Considerazioni speciali sulla modalità Light Agent
- Configurazione preliminare della macchina virtuale
  - Compatibilità con la tecnologia Citrix App Layering
  - Compatibilità con la tecnologia Citrix Provisioning (Citrix Provisioning Services)
  - Compatibilità con la tecnologia Omnissa App Volumes
- Installazione di Light Agent
- Connessione di Light Agent alla SVM
  - Rilevamento di SVM
  - Configurazione dell'algoritmo di selezione delle SVM per Light Agent

Distribuzione delle connessioni dei Light Agent alle SVM (tag)
Protezione della connessione tra un Light Agent e SVM
Attivazione di Light Agent
Guida alla migrazione da KSVLA Light Agent a KES Light Agent
Installazione di KES Light Agent anziché di KSVLA Light Agent
Corrispondenza dei componenti di KSVLA Light Agent e KES Light Agent
Migrazione di attività e criteri di KSVLA Light Agent
Migrazione della configurazione [KSVLA Light Agent+KEA] alla configurazione [KES Light Agent+agente integrato]
Gestione dell'applicazione dalla riga di comando
Setup. Installazione dell'applicazione
Setup /x. Rimozione dell'applicazione
msiexec /i. Recupero dell'applicazione
Comandi AVP
SCAN. Scansione malware
UPDATE. Aggiornamento di database e moduli software dell'applicazione
ROLLBACK. Ultimo rollback degli aggiornamenti
TRACES. Tracciamento
START. Avvio di un profilo
STOP. Arresto di un profilo
STATUS. Stato del profilo
STATISTICS. Statistiche sul funzionamento del profilo
RESTORE. Ripristino di file da Backup
EXPORT. Esportazione delle impostazioni dell'applicazione
IMPORT. Importazione delle impostazioni dell'applicazione
ADDKEY. Applicazione di un file chiave
LICENSE. Gestione delle licenze
RENEW. Acquisto di una licenza
PBATESTRESET. Ripristino dei risultati del controllo del disco prima di criptare il disco
EXIT. Chiusura dell'applicazione
EXITPOLICY. Disabilitazione del criterio
STARTPOLICY. Abilitazione del criterio
DISABLE. Disabilitazione della protezione
SPYWARE. Rilevamento spyware
KSN. Passaggio da KSN a KPSN e viceversa
SERVERBINDINGDISABLE. Disabilitazione della protezione della connessione al server
Comandi KESCLI
Scan. Scansione malware
GetScanState. Stato di completamento della scansione
GetLastScanTime. Definizione del tempo di completamento della scansione
GetThreats. Ottenimento dei dati sulle minacce rilevate
UpdateDefinitions. Aggiornamento di database e moduli software dell'applicazione
GetDefinitionState. Determinazione della data e dell'ora dell'ultimo aggiornamento dei database
EnableRTP. Abilitazione della protezione
GetRealTimeProtectionState. Stato di Protezione minacce file
GetEncryptionState. Stato di criptaggio del disco
Version. Identificazione della versione dell'applicazione

- Comandi di gestione di Detection and Response
  - SANDBOX. Gestione di Sandbox
  - PREVENTION. Gestione della prevenzione dell'esecuzione
  - ISOLATION. Gestione dell'isolamento di rete
  - RESTORE. Ripristino dei file dalla quarantena
  - IOCSCAN. Scansione degli indicatori di compromissione (IOC)
  - MDRLICENSE. Attivazione MDR
  - EDRKATA. Integrazione EDR (KATA)
  - EDRExpertOnPrem. Integrazione con EDR Expert (on-premises)
  - KUMA. Integrazione di KUMA
  - YARA. Esecuzione della scansione YARA
  - TELEMETRYFILTERS. Filtraggio degli eventi da inviare a KUMA
- Comandi di gestione di Light Agent
  - KSVLAINFO. Determinazione della modalità Light Agent
  - VIISINFO. Stato della connessione di Light Agent al server di integrazione
  - SVMINFO. Stato della connessione di Light Agent al server di protezione
- Codici di errore
- Appendice. Profili dell'applicazione

Gestione dell'applicazione tramite REST API
- Installazione dell'applicazione con REST API
- Utilizzo dell'API

Fonti di informazioni sull'applicazione

Come contattare l'assistenza tecnica
- Contenuto e archiviazione dei file di traccia
- Tracciamento del funzionamento dell'applicazione
- Tracciamento delle prestazioni dell'applicazione
- Scrittura di dump
- Protezione dei file di dump e dei file di traccia
- Recupero dei dati del sistema operativo (Kaspersky Get System Info)

Limitazioni e avvisi

Glossario
- Agente di Autenticazione
- Ambito della protezione
- Ambito della scansione
- Archivio
- Attività
- Autenticazione Kerberos
- Autorità di emissione del certificato
- Certificato di licenza
- Chiave attiva
- Cloud Discovery
- Database anti-virus
- Database di indirizzi Web dannosi
- Database di indirizzi Web di phishing
- Disinfezione
- Falso allarme
- File infettabile

File infetto
File IOC
Forma normalizzata dell'indirizzo di una risorsa Web
Gruppo di amministrazione
IOC
Light Agent
Maschera
Network Agent
Oggetto OLE
OpenIOC
Portable File Manager
Server di integrazione
SVM
Trusted Platform Module
Appendici
Appendice 1. Impostazioni applicazione
Protezione minacce file
Protezione minacce Web
Protezione minacce di posta
Protezione minacce di rete
Firewall
Prevenzione Attacchi BadUSB
Protezione AMSI
Prevenzione Exploit
Rilevamento del Comportamento
Prevenzione Intrusioni Host
Motore di Remediation
Kaspersky Security Network
Log Inspection
Anti-Cryptor
Controllo Web
Controllo dispositivi
Controllo applicazioni
Controllo adattivo delle anomalie
Monitoraggio integrità di sistema
Sensore Endpoint
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
Integrazione di KUMA
Criptaggio dell'intero disco
Criptaggio a livello di file
Criptaggio unità rimovibili
Modelli (criptaggio dei dati)
Esclusioni

Impostazioni applicazione
Rapporti e archivi
Impostazioni di Rete
Interfaccia
Gestione impostazioni
Aggiornamento di database e moduli software dell'applicazione
Appendice 2. Gruppi di attendibilità delle applicazioni
Appendice 3. Estensioni file per la scansione rapida delle unità rimovibili
Appendice 4. Tipi di file per il filtro allegati di Protezione minacce di posta
Appendice 5. Impostazioni di rete per l'interazione con servizi esterni
Appendice 6. Eventi applicativi
Critico
Errore funzionale
Avviso
Messaggio informativo
Appendice 7. Estensioni di file supportate per Prevenzione dell'esecuzione
Appendice 8. Interpreti di script supportati per la prevenzione dell'esecuzione
Appendice 9. Ambito della scansione IOC nel Registro di sistema (RegistryItem)
Appendice 10. Requisiti del file IOC
Appendice 11. API per la risposta alle minacce EDR
Appendice 12. Account utente nelle regole dei componenti dell'applicazione
Informazioni legali
Trasmissione dei dati
Trasmissione dei dati nell'ambito del Contratto di licenza con l'utente finale
Trasmissione dei dati durante l'utilizzo di Kaspersky Security Network
Trasmissione dei dati quando si utilizzano le soluzioni Detection and Response
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Integrazione con Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Conformità alla legislazione dell'Unione Europea (GDPR)
Note relative ai marchi
Informazioni sul codice di terze parti

Guida di Kaspersky Endpoint Security for Windows

Novità della versione 14.2

Aggiunto il supporto dell'autenticazione basata su token per Protezione tramite password

Novità di ogni versione di Kaspersky Endpoint Security for Windows

Guida introduttiva

Distribuzione di Kaspersky Endpoint Security for Windows

Configurazione iniziale di Kaspersky Endpoint Security for Windows

Concessione della licenza di Kaspersky Endpoint Security for Windows

Trasmissione dei dati

Ai sensi del Contratto di licenza con l'utente finale

Quando si utilizza KSN

GDPR

Eliminazione delle minacce

Sulle workstation

Sui server

Reazione al rilevamento di un indicatore di compromissione (Isolamento di rete → Quarantena → Prevenzione dell'esecuzione)

Best practice

Ottimizzazione delle prestazioni dell'applicazione

Implementazione della modalità di rifiuto predefinita in Controllo applicazioni

Migrazione da KEA a KES con l'agente integrato

Utilizzo di KES come parte di altre soluzioni

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

Novità

Aggiornamento 14.2

Kaspersky Endpoint Security 14.2 for Windows introduce i seguenti miglioramenti e funzionalità:

1. È stato modificato il set di componenti installati per impostazione predefinita. La configurazione predefinita dell'applicazione ora include Prevenzione Attacchi BadUSB, Gestione BitLocker e l'agente integrato EDR Optimum.

2. È stato aggiunto il supporto per l'autenticazione basata su token (Protezione tramite password). Ora, per accedere all'applicazione, è possibile utilizzare il nome utente e la password, una password temporanea fornita dall'amministratore oppure un token. L'autenticazione basata su token può essere utilizzata, ad esempio, per gli account utente di servizio che non richiedono una password.

3. È stato aggiunto un nuovo criterio di complessità della password per BitLocker: controllo della cronologia delle password. L'applicazione impedisce agli utenti di impostare una password già utilizzata in precedenza.

4. È stato aggiunto il supporto per la modifica della lingua dell'interfaccia di Kaspersky Endpoint Security durante l'aggiornamento dell'applicazione mediante l'attività *Installa applicazione in remoto*. Ora non è necessario reinstallare l'applicazione se è stata selezionata la lingua dell'interfaccia errata.

5. Sono stati aggiunti nuovi eventi di telemetria per gli utenti delle soluzioni Kaspersky Endpoint Detection and Response: GPO Change, SCCM Local Config Mismatch, SCCM Config Change, SCCM Deployment Task, Smb Connection Open. Questi nuovi eventi migliorano le funzionalità di rilevamento delle minacce delle soluzioni EDR.

6. È stato aggiunto il supporto per una nuova azione di risposta alle minacce, *Posiziona file*, per gli utenti di Kaspersky Endpoint Detection and Response Expert (on-premises). Questa attività consente di distribuire nei computer file di configurazione, script di risposta alle minacce, utilità per mitigare gli effetti degli attacchi e così via. L'attività *Posiziona file* è disponibile nella console OSMP in cui è distribuita la versione 9.0 della soluzione Kaspersky EDR Expert (on-premises).

7. È stato migliorato il comportamento delle azioni di risposta alle minacce per gli utenti di Kaspersky Endpoint Detection and Response Optimum. Ora, prima di eseguire l'azione (*Elimina file*, *Sposta file in Quarantena* o *Prevenzione dell'esecuzione*), l'applicazione verifica se l'oggetto è critico per il sistema (System Critical Object, SCO) e avvisa del potenziale impatto sulla stabilità del sistema. Non è consigliabile applicare queste azioni ai file SCO (System Critical Object).

8. È stato aggiunto il supporto per consentire agli utenti di Kaspersky Security for Virtualization Light Agent di utilizzare l'applicazione nell'ambito di un cluster ad alta disponibilità di Server di integrazione. Un cluster ad alta disponibilità di Server di integrazione garantisce la protezione ininterrotta dell'ambiente virtuale grazie al failover delle SVM e dei Light Agent su un Server di integrazione di backup in caso di malfunzionamento del Server di integrazione primario.

9. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security, sono state integrate le modifiche incluse nelle seguenti patch private: PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF22065, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF23095, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF24037, PF24043, PF24048, PF25013, PF25016, PF25019, PF25030.

Aggiornamento 14.1

Kaspersky Endpoint Security 14.1 for Windows introduce i seguenti miglioramenti e funzionalità:

1. È stato aggiunto il supporto per il sistema operativo Windows Server 2025.

2. Il limite per il numero di regole di filtraggio degli eventi di telemetria per Endpoint Detection and Response Expert (on-premises) e Kaspersky Endpoint Detection and Response Expert (cloud) è stato aumentato. Kaspersky Endpoint Security ora supporta fino a 10.000 regole di filtraggio incluse ed esclusive in totale.

3. Ora è possibile configurare le attività per l'esecuzione solo in giorni della settimana specifici, a un intervallo specificato in settimane. La pianificazione è disponibile in Kaspersky Security Center 16.1 o versioni successive.

4. Per l'attività *Scansione malware*, ora è possibile specificare un intervallo di tempo durante il quale l'attività verrà sospesa, ad esempio per ridurre al minimo l'impatto sulle prestazioni del computer durante i periodi di maggiore carico.

5. Le prestazioni del sottosistema del disco rigido nel computer protetto sono state ottimizzate riducendo il numero di operazioni di I/O.

6. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security, sono state integrate le modifiche incluse nelle seguenti patch private: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

Aggiornamento 14.0

Kaspersky Endpoint Security 14.0 for Windows introduce i seguenti miglioramenti e funzionalità:

1. I computer basati su Arm ora sono supportati. È possibile installare l'applicazione in modalità standard o in modalità EDR Agent. L'applicazione presenta tuttavia diverse limitazioni (ad esempio, tra le tecnologie di criptaggio dei dati è supportato solo BitLocker).

2. Il controllo esteso dei criteri è supportato in Kaspersky Security Center Web Console versione 15.0 o successiva. Ora è possibile visualizzare le revisioni dei criteri e salvarle in un file. Una *revisione* è un set di parametri modificati salvati dall'utente. Le revisioni consentono di confrontare e annullare le modifiche ai parametri del criterio.

3. I nuovi eventi di telemetria sono ora disponibili per gli utenti di Kaspersky Endpoint Detection and Response. Questi nuovi eventi migliorano le funzionalità di rilevamento delle minacce mediante le soluzioni Kaspersky EDR.

4. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security for Windows, sono state integrate le modifiche incluse nelle seguenti patch private: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Aggiornamento 12.12

Kaspersky Endpoint Security 12.12 for Windows introduce i seguenti miglioramenti e funzionalità:

1. La protezione delle cartelle condivise dal criptaggio esterno che prima faceva parte del componente Rilevamento del Comportamento è ora un componente separato, Anti-Cryptor.

2. È stato aggiunto il supporto per il protocollo Kerberos per l'autenticazione dell'applicazione tramite un server proxy per l'accesso a Internet.

3. Adesso è possibile specificare un hash di file per un'applicazione attendibile e non solo un percorso completo.

4. Sono disponibili ulteriori funzionalità dell'attività *Scansione IOC* per gli utenti delle soluzioni Endpoint Detection and Response (EDR). è ora disponibile la funzionalità Scansione IOC retrospettiva. *Scansione IOC retrospettiva* è una modalità dell'attività *Scansione IOC* in cui Kaspersky Endpoint Security esegue la scansione degli indicatori di compromissione utilizzando i dati per un determinato periodo di tempo. Questa modalità è destinata al rilevamento degli indicatori di compromissione nei dati delle attività di rete del computer. Kaspersky Endpoint Security analizza i dati nei registri del sistema operativo e del browser nel computer.

5. Gli utenti di Kaspersky Endpoint Detection and Response (EDR) possono rimuovere il limite delle dimensioni della quarantena. Questa operazione potrebbe essere necessaria per la scansione YARA poiché l'applicazione può salvare un file di dump della memoria di grandi dimensioni. Adesso è possibile utilizzare tutto lo spazio libero su disco per la quarantena.

6. La compressione HTTPS ora è supportata per l'ottimizzazione dell'esportazione degli eventi in Kaspersky Unified Monitoring and Analysis Platform (KUMA). Questo aiuta a ridurre il traffico in uscita.

7. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security for Windows, sono state integrate le modifiche incluse nelle seguenti patch private: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Aggiornamento 12.11

Kaspersky Endpoint Security 12.11 for Windows offre i seguenti miglioramenti e funzionalità:

1. L'applicazione controlla la configurazione dei componenti di controllo prima di salvare le impostazioni. Il controllo è stato aggiunto per i componenti Controllo applicazioni, Controllo dispositivi e Monitoraggio integrità di sistema. L'applicazione ora mostra un avviso se le impostazioni correnti del componente di controllo possono aumentare il carico sul computer o causare errori del sistema. Ad esempio, nel caso di Controllo applicazioni, se è stata selezionata la modalità che blocca tutte le applicazioni ad eccezione di quelle consentite e non è stata aggiunta alcuna regola di autorizzazione, l'applicazione mostra un avviso poiché tale configurazione potrebbe causare errori del sistema.

2. Aggiunto supporto per l'invio automatico dei file a KATA Sandbox per la revisione. *KATA Sandbox* è un componente di Kaspersky Anti Targeted Attack Platform che esegue file su immagini virtuali dei sistemi operativi. Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Sandbox). Per il funzionamento di KATA Sandbox in modalità automatica, è necessario distribuire Kaspersky Anti Targeted Attack Platform 8.0 o versioni successive.

3. Invio della telemetria EDR ottimizzato. Ora è possibile specificare la lunghezza massima del pacchetto.

4. Diagnostica della connessione a Kaspersky Security Network migliorata. Dettagli degli errori di connessione espansi per Kaspersky Security Network per risolvere potenziali problemi.

5. È stato aggiunto il supporto per la configurazione degli elenchi di eventi da inviare a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Ora, oltre agli elenchi di eventi predefiniti in KUMA, è possibile aggiungere manualmente eventi alla telemetria o escludere gli eventi in base al relativo ID nel registro eventi di Windows.

6. Aggiornata l'interfaccia dei criteri in Web Console. Il layout delle sezioni dei criteri è stato modificato per un accesso più rapido alle funzionalità essenziali.

7. Supporto per Windows 11 25H2.

8. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security for Windows, sono state integrate le modifiche incluse nelle seguenti patch private: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Aggiornamento 12.10

Kaspersky Endpoint Security 12.10 for Windows offre i seguenti miglioramenti e funzionalità:

1. Per il componente Prevenzione Attacchi BadUSB, è stata aggiunta l'opzione per autorizzare i lettori di codici a barre leggendo un codice a barre dallo schermo. Adesso non è necessario immettere un codice utilizzando la tastiera su schermo per autorizzare gli scanner di codici a barre.

2. Le funzionalità e i miglioramenti seguenti sono disponibili per gli utenti delle soluzioni Endpoint Detection and Response (EDR) di Kaspersky:

   - Ora è possibile gestire l'isolamento della rete del computer nei dettagli dell'avviso. Nei dettagli degli avvisi è inoltre possibile specificare il periodo di isolamento della rete del computer e aggiungere esclusioni.

   - Compilazione dei dettagli degli avvisi con nuovi dati. Ora i dettagli degli avvisi contengono più informazioni sulla minaccia, incluso il comportamento dell'applicazione quando risponde alle minacce EDR.

   - L'elaborazione dei file IOC è stata migliorata. Adesso è possibile visualizzare e modificare il contenuto dei file IOC nell'interfaccia di Kaspersky Security Center Web Console. Dopo il caricamento di un file IOC, l'applicazione mostra un rapporto sui termini IOC dell'applicazione.

   - Risposta migliorata agli IOC rilevati. Adesso è possibile mettere in quarantena i file rilevati dall'attività *Scansione IOC* direttamente nei risultati del rilevamento di IOC nelle proprietà dell'attività. È inoltre possibile isolare i computer dalla rete nelle proprietà dell'attività.

   - Ora è possibile creare file IOC direttamente nelle proprietà dell'attività *Scansione CIO* basata sugli elenchi di hash di file, indirizzi IP o nomi DNS generati in un file TXT.

   - Ambito di scansione esteso per l'attività *Scansione IOC*. Adesso è possibile definire un ambito per la scansione IOC del Registro di sistema di Windows (**Registro di sistema di Windows – Registryltem**). Nelle versioni precedenti dell'applicazione era possibile utilizzare solo un ambito Scansione IOC predefinito nel Registro di sistema.

3. Nuova autorizzazione di protezione tramite password aggiunta, *Impostazioni di esportazione*. Per impostazione predefinita, solo l'utente KLAdmin può creare un file di configurazione con le impostazioni di Kaspersky Endpoint Security nell'interfaccia dell'applicazione. Per concedere l'accesso ad altri utenti, è necessario concedere loro l'autorizzazione corrispondente.

4. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security for Windows, sono state integrate le modifiche incluse nelle seguenti patch private: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Aggiornamento 12.9

Kaspersky Endpoint Security 12.9 for Windows offre i seguenti miglioramenti e funzionalità:

1. È stata aggiunta la nuova funzionalità per la *gestione delle password temporanee*. La password temporanea consente di fornire l'accesso a Kaspersky Endpoint Security con Protezione tramite password abilitata per un singolo computer. La gestione delle password temporanee consente di salvare la cronologia delle password (fino a 30 giorni), monitorare lo stato delle password temporanee (*Attivo*, *Scaduto*, *Revocato*) e revocare le password temporanee.

2. È stata aggiunta l'opzione per interrompere la connessione alle risorse Web vietate dalle regole di Controllo Web subito dopo l'applicazione del criterio. Nelle versioni precedenti dell'applicazione, Controllo Web limitava solo le nuove connessioni alle risorse Web vietate.

3. Per gli utenti di Kaspersky Anti Targeted Attack Platform è stata aggiunta un'opzione per eseguire il controllo YARA in locale nel computer. A tale scopo, è necessario scaricare un file con le regole YARA ed eseguire il comando in CMD.

4. È stato corretto il comportamento dell'applicazione quando BitLocker è abilitato nei computer in cui le unità sono già protette da BitLocker utilizzando strumenti di terze parti. Kaspersky Endpoint Security avvia la procedura di ripristino per l'invio della chiave di ripristino a Kaspersky Security Center. Pertanto, la gestione di BitLocker viene trasferita alla console Kaspersky Security Center.

5. Una nuova sezione **Cronologia risposte**, è disponibile per gli utenti delle soluzioni Detection and Response di Kaspersky. Questa sezione contiene informazioni sulle azioni di reazione alle minacce eseguite nel computer. Tali azioni includono, ad esempio, l'esecuzione dell'attività *Termina processo* o l'isolamento del computer dalla rete. La cronologia delle risposte è disponibile solo per gli utenti delle seguenti soluzioni Kaspersky: MDR, EDR, KATA.

6. Per gli utenti di Kaspersky Unified Monitoring and Analysis Platform, è ora disponibile il supporto per le azioni di risposta alle minacce EDR. Quando risponde alle minacce, KUMA esegue script che creano le attività EDR corrispondenti. Per eseguire attività EDR, è necessario creare una regola di risposta per lo script personalizzato nella console KUMA e selezionare gli eventi.

7. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security for Windows, sono state integrate le modifiche incluse nelle seguenti patch private: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Aggiornamento 12.8

Kaspersky Endpoint Security 12.8 for Windows offre i seguenti miglioramenti e funzionalità:

1. L'applicazione ora supporta la modalità Light Agent per la protezione degli ambienti virtuali. Ora è possibile distribuire l'applicazione come Light Agent come parte della soluzione Kaspersky Security for Virtualization Light Agent 6.2.

2. L'intercettazione delle operazioni sui file nei contenitori Docker sui server ora è supportata. Un *contenitore* è un ambiente isolato in cui un'applicazione può essere eseguita senza interagire direttamente con il sistema operativo. Kaspersky Endpoint Security esamina i file all'interno dei contenitori a cui l'utente può accedere. Quando viene rilevata una minaccia, le applicazioni la bloccano e tentano di disinfettare il file all'interno del contenitore. Se non è possibile disinfettare il file, l'applicazione arresta il contenitore.

3. Ora è possibile definire un ambito di protezione per la protezione delle cartelle condivise dal criptaggio esterno (componente Rilevamento del Comportamento). Ora è possibile specificare le cartelle condivise di cui l'applicazione deve monitorare le attività si file. È inoltre possibile escludere file dall'ambito di protezione. Nelle versioni precedenti dell'applicazione, il componente Rilevamento del Comportamento monitorava tutte le cartelle condivise per rilevare eventuali attività sui file.

4. Ora è possibile configurare diversi set di componenti per diversi tipi di sistemi operativi nel pacchetto di installazione. In altre parole, è possibile distribuire l'applicazione a workstation e server utilizzando lo stesso pacchetto di installazione. I componenti che non sono disponibili per un determinato tipo di sistema operativo vengono automaticamente esclusi nelle proprietà del pacchetto di installazione.

5. È stata aggiunta l'opzione che consente di selezionare le esclusioni dalle scansioni e le applicazioni attendibili. Le esclusioni di scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente l'area attendibile per l'applicazione in un ambiente virtuale (Citrix, VMware). Tali esclusioni comprendono, ad esempio, i file di macchine virtuali VHD e VHDX. È possibile aggiungere esclusioni durante l'installazione di un pacchetto di installazione dell'applicazione, la creazione di un criterio o l'installazione di Kaspersky Endpoint Security.

6. La telemetria EDR ora include gli eventi per le operazioni con i dispositivi connessi tramite USB. È anche possibile aggiungere questi eventi alle esclusioni dalla telemetria EDR.

7. È stata aggiunta l'opzione per bloccare le connessioni di rete tramite il protocollo TLS 1.0 obsoleto. TLS 1.0 dispone di un livello di protezione basso, pertanto è consigliabile disabilitare questo protocollo e utilizzare le versioni di TLS 1.2 o TLS 1.3 più recenti. Per impostazione predefinita, Kaspersky Endpoint Security blocca le connessioni TLS 1.0. Dopo l'aggiornamento della versione dell'applicazione, l'esecuzione dei servizi di terze parti che utilizzano il protocollo TLS 1.0 potrebbe non riuscire. Per evitare problemi durante il funzionamento dei servizi di terze parti, è possibile consentire l'utilizzo del protocollo TLS 1.0 nel criterio di gruppo prima di aggiornare la versione dell'applicazione.

8. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security for Windows, sono state integrate le modifiche incluse nelle seguenti patch private: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Aggiornamento 12.7

Kaspersky Endpoint Security 12.7 for Windows offre i seguenti miglioramenti e funzionalità:

1. Ora è possibile limitare l'utilizzo delle risorse della CPU per le attività *Scansione malware*. A tale scopo, nelle impostazioni dell'applicazione, specificare la percentuale di carico CPU massima per tutti i core che è possibile utilizzare durante la scansione del computer.

2. Ora è possibile manualmente inviare i file per la scansione in KATA Sandbox. *KATA Sandbox* è un componente di Kaspersky Anti Targeted Attack Platform che esegue file su immagini virtuali dei sistemi operativi. Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Sandbox). Per inviare un file per la scansione a KATA Sandbox, selezionare il comando pertinente nel menu di scelta rapida del file.

3. Ora è possibile configurare l'integrazione con la soluzione che protegge la LAN aziendale, *Kaspersky Network Detection and Response*. Kaspersky Network Detection and Response (NDR) fa parte di Kaspersky Anti Targeted Attack Platform. È possibile configurare l'interazione con NDR in modalità standard, nonché in modalità EDR Agent.

4. All'estensione Protezione minacce di posta è stato aggiunto il supporto per il client di posta elettronica Microsoft Office Outlook versione 2021. L'estensione consente la scansione dei messaggi a livello di un client di posta anziché a livello di protocollo. Oltre ai messaggi, l'estensione consente di eseguire la scansione degli oggetti ricevuti tramite l'interfaccia MAPI dagli archivi di Microsoft Exchange (ad esempio, gli oggetti nel Calendario). Questa scansione avviene nel client di posta.

5. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security for Windows, sono state integrate le modifiche incluse nelle seguenti patch private: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Aggiornamento 12.6

Kaspersky Endpoint Security 12.6 for Windows offre i seguenti miglioramenti e funzionalità:

1. È stata aggiunta la funzionalità per l'integrazione con la soluzione Kaspersky SIEM - *Kaspersky Unified Monitoring and Analysis Platform (KUMA).* Adesso è possibile inviare eventi dai registri eventi di Windows al servizio di raccolta di KUMA. Ciò consente a KUMA di ricevere gli eventi di Windows (è supportato un set limitato di EventID) da tutti i computer in cui è installato Kaspersky Endpoint Security, senza installare gli agenti KUMA in questi computer.

2. Un nuovo componente *Monitoraggio integrità di sistema* è stato aggiunto a sostituzione del componente Monitoraggio integrità file. Il componente Monitoraggio integrità di sistema include tutte le funzionalità di Monitoraggio integrità file e consente inoltre di monitorare le modifiche al Registro di sistema e la connessione dei dispositivi esterni. Il componente Monitoraggio integrità di sistema monitora le modifiche nel sistema operativo che potrebbero indicare violazioni della sicurezza del computer. Quando vengono rilevate tali modifiche, Kaspersky Endpoint Security genera gli eventi corrispondenti e avvisa l'amministratore. Monitoraggio integrità file non fa più parte dell'applicazione. Le impostazioni di Monitoraggio integrità file vengono migrate automaticamente in Monitoraggio integrità di sistema quando si aggiorna l'applicazione. Per garantire il corretto funzionamento di Monitoraggio integrità di sistema, sia l'applicazione Kaspersky Endpoint Security che il plug-in di gestione devono essere aggiornati alla versione 12.6.

3. Lo stato di EDR Agent (KATA) integrato installato è stato aggiunto alle proprietà del computer nella console di Kaspersky Security Center. Ora, se è installato un EDR Agent (KATA) integrato, la colonna **Stato del Endpoint Sensor** mostra lo stato corrente del componente (ad es. *In esecuzione*, *Interrotto*, *Non supportato dalla licenza* ecc.)

4. È stata aggiunta l'opzione che consente di selezionare le esclusioni dalle scansioni e le applicazioni attendibili. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente l'area attendibile quando si utilizza l'applicazione nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Tali esclusioni comprendono, ad esempio, i file di database MDF e LDF. È possibile aggiungere esclusioni durante la creazione di un nuovo criterio, la modifica di un criterio esistente o l'installazione di Kaspersky Endpoint Security.

5. La visualizzazione dei dettagli degli avvisi per Kaspersky Endpoint Detection and Response Optimum è stata spostata dal plug-in di gestione di Kaspersky Endpoint Security a un plug-in di gestione separato di Kaspersky Endpoint Detection and Response. Il plug-in di gestione EDR è un plug-in singolo per l'utilizzo degli agenti nei sistemi operativi Windows, Mac e Linux. Ora, quando si utilizza EDR Optimum, sarà necessario il plug-in di gestione di Kaspersky Endpoint Security per creare attività di risposta alle minacce e il plug-in di gestione EDR per visualizzare i dettagli degli avvisi.

6. Supporto per Windows 11 24H2.

7. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security for Windows, sono state incorporate le modifiche incluse nelle seguenti patch private: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Aggiornamento 12.5

Kaspersky Endpoint Security 12.5 for Windows offre i seguenti miglioramenti e funzionalità:

1. È stata aggiunta l'opzione per configurare le esclusioni di telemetria. *Telemetria* è un elenco di eventi che si sono verificati nel computer protetto. I dati di telemetria vengono utilizzati da Kaspersky Anti Targeted Attack Platform (EDR) per monitorare e proteggere l'infrastruttura IT dell'organizzazione. La configurazione delle esclusioni di telemetria contribuisce a migliorare le prestazioni del computer e ottimizzare la trasmissione dei dati al server di raccolta della telemetria.

2. L'interfaccia dell'area attendibile dell'applicazione è stata migliorata. Kaspersky Endpoint Security ora nasconde all'utente gli oggetti dell'area attendibile se l'amministratore ha vietato all'utente di aggiungere le proprie esclusioni di scansione (locali) e applicazioni attendibili. Questo impedisce l'accesso non autorizzato all'area attendibile da parte di un intruso, aumentando il livello di protezione del computer.

3. È stata aggiunta l'opzione per la scansione del traffico per i client di posta MyOffice Mail e R7-Office Organizer. Il componente Protezione minacce di posta ora esegue la scansione non solo degli allegati dei messaggi al momento del download, ma anche dei messaggi inviati e ricevuti.

4. È stata aggiunta una nuova categoria di risorse Web *Strumenti di IA generativa*. È possibile configurare l'accesso ai siti Web della nuova categoria utilizzando Controllo Web.

5. Ora è possibile selezionare la posizione di una regola per i pacchetti di rete nell'elenco Firewall. La posizione di una regola per i pacchetti di rete nell'elenco ne determina la priorità. Nelle versioni precedenti dell'applicazione era possibile aggiungere una nuova regola solo alla fine dell'elenco, dopodiché era necessario spostare manualmente la regola nell'elenco per stabilire la priorità. Ora, quando si aggiunge una regola, è possibile scegliere se la regola deve essere posizionata all'inizio, alla fine dell'elenco o accanto alla regola selezionata.

6. Nelle regole dei componenti di Kaspersky Endpoint Security ora è possibile selezionare gli utenti non solo da Active Directory, ma anche dall'elenco degli utenti in Kaspersky Security Center. È inoltre possibile immettere manualmente i dati dell'account utente locale. Questa possibilità è stata aggiunta per le regole dei seguenti componenti: Controllo applicazioni, Controllo dispositivi, Controllo Web, Controllo adattivo delle anomalie e Log Inspection.

7. Il rapporto sul rilevamento degli attacchi di rete ora include una colonna con l'indirizzo MAC del computer che ha originato l'attacco il componente Protezione minacce di rete. Ora nel rapporto è possibile visualizzare, oltre al suo indirizzo IP, anche l'indirizzo MAC del computer che ha originato l'attacco. Questo è utile per le indagini sugli incidenti. I rapporti, che contengono l'indirizzo MAC del computer che ha sferrato l'attacco, saranno disponibili anche nella console Linux di Kaspersky Security Center versione 15.1 e successive.

8. Il livello dei requisiti di protezione del computer è stato aumentato. Il livello di protezione elevato ora richiede l'abilitazione della protezione dei servizi applicativi contro la gestione esterna. Controllare l'indicatore del livello di sicurezza nella parte superiore della finestra dei criteri. Se si dispone di un livello di protezione medio o basso, è possibile abilitare la protezione dei servizi applicativi contro la gestione esterna nella finestra dei suggerimenti dell'indicatore del livello di sicurezza.

9. È stato aggiunto il supporto di nuovi eventi di rilevamento degli oggetti quando l'applicazione è in esecuzione nella configurazione Endpoint Detection and Response Agent (EDR Agent). Questi eventi erano già supportati nella configurazione [KES+agente integrato].

10. Durante lo sviluppo di questa versione di Kaspersky Endpoint Security for Windows, sono state incorporate le modifiche incluse nelle seguenti patch private: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Aggiornamento 12.4

Kaspersky Endpoint Security 12.4 for Windows offre i seguenti miglioramenti e funzionalità:

1. Aggiunta nuova funzionalità per proteggere la connessione del computer a Kaspersky Security Center. La nuova attività *Protezione della connessione ad Administration Server* consente di impostare una password per la connessione a un server attendibile. Questo significa che non è possibile riconnettersi al computer ed eseguire comandi da un altro server senza questa password.

2. Per il componente Protezione tramite password è stata aggiunta la possibilità di selezionare utenti manualmente e non solo da Active Directory. In altre parole, è possibile specificare manualmente un nome utente e una password e assegnare i diritti di accesso a Kaspersky Endpoint Security per questo account. In questo modo, non è necessario condividere la password di KLAdmin con altri utenti o creare nuovi account di Active Directory per controllare l'accesso all'applicazione.

3. Supporto per Windows 11 23H2.

Aggiornamento 12.3

Kaspersky Endpoint Security 12.3 for Windows offre i seguenti miglioramenti e funzionalità:

1. Ora è possibile installare l'applicazione nella configurazione Endpoint Detection and Response Agent. Questa configurazione consente di installare l'applicazione con una serie di componenti richiesti dalle soluzioni Detection and Response di Kaspersky: Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform (EDR). È possibile installare l'applicazione in questa configurazione insieme a soluzioni di terzi (ad esempio Dr.Web, Dallas Lock, ESET). Ciò consente di utilizzare strumenti di sicurezza dell'infrastruttura di terzi insieme a Kaspersky Detection and Response.

2. L'utilizzo di Kaspersky Endpoint Security con i dispositivi Bluetooth è stato migliorato. Ora è possibile configurare le esclusioni e limitare l'accesso a tutti i dispositivi Bluetooth, ad eccezione dei dispositivi di input (tastiere wireless, mouse ecc.).

3. Il funzionamento del componente Controllo applicazioni con il database dei file eseguibili è stato ottimizzato. Kaspersky Endpoint Security ora rimuove automaticamente le informazioni dei file dal database se i file vengono eliminati dal computer. Ciò consente di mantenere aggiornato il database e di risparmiare le risorse di Kaspersky Security Center.

4. Il livello dei requisiti di protezione del computer è stato aumentato. L'elevato livello di protezione ora richiede l'abilitazione della protezione tramite password. Controllare l'indicatore del livello di sicurezza nella parte superiore della finestra dei criteri. Se è stato impostato un livello di protezione medio o basso, è possibile abilitare Protezione tramite password nella finestra dei suggerimenti dell'indicatore del livello di sicurezza.

5. È stato aggiunto il supporto del protocollo HTTPS per consentire l'utilizzo dell'applicazione con Kaspersky Security Network. Abilitare l'utilizzo di HTTPS nelle proprietà di Administration Server nelle impostazioni del server proxy KSN.

Aggiornamento 12.2

Kaspersky Endpoint Security 12.2 for Windows offre i seguenti miglioramenti e funzionalità:

1. È stato aggiunto il supporto del protocollo WPA3 per controllare le connessioni alle reti Wi-Fi (Controllo dispositivi). Ora è possibile selezionare il protocollo WPA3 nelle impostazioni della rete Wi-Fi attendibile e negare la connessione alla rete utilizzando un protocollo meno sicuro.

2. Ora è possibile scegliere un protocollo e porte per le esclusioni di Protezione minacce di rete. Ora, oltre a specificare gli indirizzi IP dei dispositivi attendibili, è anche possibile selezionare una porta e un protocollo. Ciò consente di escludere singoli flussi di dati e prevenire attacchi di rete da indirizzi IP attendibili.

3. Ordine diverso delle sorgenti degli aggiornamenti per l'attività locale *Aggiornamento di database e moduli dell'applicazione* se un criterio viene applicato al computer. Il server Kaspersky Security Center viene ora utilizzato per impostazione predefinita come prima sorgente degli aggiornamenti invece dei server Kaspersky. Ciò consente di risparmiare traffico quando l'utente esegue l'attività locale *Aggiornamento di database e moduli dell'applicazione*.

Aggiornamento 12.1

Kaspersky Endpoint Security 12.1 for Windows offre i seguenti miglioramenti e funzionalità:

1. È stato aggiunto un agente integrato per la soluzione Kaspersky Anti Targeted Attack Platform. Per utilizzare Kaspersky Endpoint Agent, non è più necessario EDR (KATA). Tutte le funzioni di Kaspersky Endpoint Agent verranno eseguite da Kaspersky Endpoint Security. Per eseguire la migrazione di tutti i criteri di Kaspersky Endpoint Agent, usare la migrazione guidata. Dopo aver aggiornato l'applicazione, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent. Kaspersky Endpoint Agent è stato aggiunto all'elenco del software incompatibile. Kaspersky Endpoint Security dispone di agenti integrati per tutte le soluzioni di Detection and Response, pertanto non è più necessario installare Kaspersky Endpoint Agent per l'integrazione con tali soluzioni.

2. La modalità di compatibilità di Azure WVD è ora supportata. Questa funzionalità garantisce la corretta visualizzazione dello stato della macchina virtuale di Azure nella console Kaspersky Anti Targeted Attack Platform. La modalità di compatibilità Azure WVD consente di assegnare un ID sensore univoco permanente a queste macchine virtuali.

3. Ora è possibile configurare l'accesso degli utenti ai dispositivi mobili in iTunes o applicazioni simili. In altre parole, è ad esempio possibile consentire l'utilizzo del dispositivo mobile solo in iTunes e bloccare l'utilizzo del dispositivo mobile come unità rimovibile. L'applicazione supporta anche queste regole per l'applicazione Android Debug Bridge (ADB).

4. Kaspersky Security Center versione 11 non è più supportato. Effettuare l'upgrade di Kaspersky Security Center all'ultima versione.

Problemi risolti

La tabella seguente elenca tutti i problemi rilevati nelle versioni precedenti di Kaspersky Endpoint Security e risolti nella versione corrente.

Elenco dei problemi risolti nella versione 14.2

Identificatore	Descrizione
10110351	Il componente Controllo dispositivi consente l'accesso a un dispositivo MTD (scheda SD) quando è selezionata l'azione **Blocca** per il tipo di dispositivo **Unità rimovibili**.
10068496	In un dispositivo protetto, è possibile modificare la modalità di Protezione dallo spoofing MAC quando le impostazioni di Protezione minacce di Rete sono bloccate nel criterio padre.
10095087	Quando la scansione delle connessioni criptate è abilitata, l'accesso a qualsiasi sito Web tramite un firewall di nuova generazione (NGFW) con un certificato revocato attiva una notifica relativa al reindirizzamento a un dominio con un certificato non attendibile.
10140912	Con l'applicazione installata, il computer non rileva il dispositivo PDA BHT1100B con Windows Mobile.
10141009	Se il componente Criptaggio file è installato, l'applicazione Anthropic Claude potrebbe non avviarsi.
10610853	Dopo l'aggiornamento alla nuova versione, non è possibile aprire il criterio perché le impostazioni di Controllo dispositivi nella nuova versione includono dispositivi non supportati nella versione precedente.

Identificatore	Descrizione
10720516	Con l'applicazione installata, gli allegati contenuti nei file in formato Office potrebbero non aprirsi.
10421967	L'accesso a una casella di posta condivisa non riesce se questa è stata aggiunta come account separato.

Elenco dei problemi risolti nel plug-in Web 14.2.0.8289

Identificatore	Descrizione
9946286	Quando si aggiunge l'indirizzo di un sito Web a una regola di Controllo Web, non è possibile utilizzare una maschera senza un punto tra il dominio e la zona del dominio.
10054657 10507166	Dopo la migrazione alla nuova versione, alcuni componenti, come Controllo dispositivi e Controllo applicazioni, non possono essere gestiti tramite criterio.
10084390	Nelle impostazioni del componente Controllo dispositivi, il tipo di dispositivo **Disco rigido** è duplicato, causando il blocco dei dischi rigidi degli utenti.
10113718	In alcuni casi, le regole personalizzate di Firewall non vengono visualizzate.
10311613	Nelle impostazioni del componente Prevenzione Intrusioni Host, non è possibile aggiungere una risorsa protetta tramite una maschera che utilizza il carattere `*`.
10391923	In Controllo Applicazioni, quando si crea una categoria di applicazioni basata sull'hash MD5 di un file, non viene visualizzato alcun avviso che indichi che la categoria non è valida e non funzionerà.
10571790	Per il componente Controllo applicazioni, è stato corretto il titolo dell'elenco delle regole di blocco in modalità **Consenti tutto tranne l'elenco di regole**.
10592891 10689065	Nell'area attendibile, il campo **Commento** non viene visualizzato per le esclusioni nella sezione **Esclusioni dalla scansione malware**.
10613015 10689049 10592534	Nel componente Controllo dispositivi, il campo **Commento** non viene visualizzato per i dispositivi attendibili.
10645068 10689057	L'attività *Rimuovi chiave* non viene eseguita se viene selezionato un file della chiave di licenza in formato KEY.
10685370 10685422	Nel componente Controllo dispositivi, non è possibile aggiungere un nuovo dispositivo all'elenco dei dispositivi attendibili se nell'elenco è già presente un dispositivo con lo stesso nome.
10721136	Non è possibile salvare le attività di gruppo se nelle impostazioni di pianificazione non è specificata una data di completamento.
10753509	La modifica dell'elenco di utenti e gruppi per i dispositivi attendibili nel componente Controllo dispositivi può cambiare i tipi di record, impedendo l'applicazione delle impostazioni al dispositivo.
10773402	In alcuni casi, le modifiche alle impostazioni del criterio potrebbero non essere salvate a causa di profili danneggiati.
10822620	Le impostazioni del componente Anti-Cryptor non vengono visualizzate nel criterio e le modifiche alle impostazioni di notifica non vengono salvate.
10817035	In un criterio figlio è consentito aggiungere un dispositivo attendibile anche se questa impostazione è disabilitata nel criterio padre ("lucchetto chiuso"). Tuttavia, il dispositivo aggiunto non viene salvato.
10678009	Nel plug-in Web di Kaspersky Endpoint Security, l'aggiunta di una nuova regola di Firewall a un criterio non riesce se in precedenza è stata creata una regola utilizzando un intervallo di indirizzi IP.

Elenco dei problemi risolti nella versione 14.1

Identificatore	Descrizione
10140523	L'abilitazione di NVMe nativo in Windows 11 può causare un comportamento instabile dell'applicazione.
9340076	In un dispositivo in cui è installata l'applicazione e il componente Criptaggio file è abilitato, Esplora risorse non aggiorna automaticamente il contenuto di una cartella di rete dopo che questa viene modificata da un altro dispositivo.

Identificatore	Descrizione
9722863	Il rapporto di Controllo dispositivi non include l'evento di disconnessione del token USB.
10006481	Dopo l'applicazione di una regola che nega il traffico in entrata, le connessioni TCP attive ai servizi esterni possono essere terminate anticipatamente a causa di un calcolo del timeout errato.
10140912	L'applicazione non rileva il dispositivo PDA BHT1100B.
10157563	Folder Redirection potrebbe non funzionare dopo un riavvio nelle workstation VDI.
10158494	Controllo dispositivi registra più eventi di connessione e disconnessione di un dispositivo rimovibile senza che venga fisicamente ricollegato.

Domande frequenti

GENERALE

In quali computer può funzionare Kaspersky Endpoint Security?

Che cosa è cambiato dall'ultima versione?

Con quali altre applicazioni Kaspersky può funzionare Kaspersky Endpoint Security?

Come è possibile tutelare le risorse del computer durante il funzionamento di Kaspersky Endpoint Security?

DISTRIBUZIONE

Come è possibile installare Kaspersky Endpoint Security in tutti i computer di un'organizzazione?

Quali impostazioni di installazione possono essere configurate nella riga di comando?

Come è possibile disinstallare in remoto Kaspersky Endpoint Security?

AGGIORNAMENTO

Quali metodi sono disponibili per aggiornare i database?

Che cosa bisogna fare se si verificano problemi dopo un aggiornamento?

Come è possibile aggiornare i database fuori dalla rete aziendale?

È possibile utilizzare un server proxy per gli aggiornamenti?

PROTEZIONE

In che modo Kaspersky Endpoint Security esamina i messaggi e-mail?

Come si esclude un file affidabile dalle scansioni?

Come è possibile proteggere un computer dai virus contenuti in un'unità flash?

Come è possibile eseguire una scansione malware nascosta all'utente?

Come è possibile sospendere temporaneamente la protezione di Kaspersky Endpoint Security?

Come è possibile ripristinare un file eliminato per errore da Kaspersky Endpoint Security?

Come è possibile proteggere Kaspersky Endpoint Security dalla disinstallazione da parte di un utente?

INTERNET

Kaspersky Endpoint Security esamina le connessioni criptate (HTTPS)?

Come è possibile consentire agli utenti di connettersi solo alle reti Wi-Fi attendibili?

Come è possibile bloccare i social network?

APPLICAZIONI

Come è possibile sapere quali applicazioni sono installate nel computer di un utente (inventario)?

Come è possibile impedire l'esecuzione dei giochi per computer?

Come è possibile verificare che Controllo applicazioni sia stato configurato correttamente?

Come è possibile aggiungere un'applicazione all'elenco delle applicazioni attendibili?

DISPOSITIVI

Come è possibile bloccare l'utilizzo delle unità flash?

Come è possibile aggiungere un dispositivo all'elenco dei dispositivi attendibili?

È possibile ottenere l'accesso a un dispositivo bloccato?

CRIPTAGGIO

In quali condizioni è impossibile il criptaggio?

Come è possibile utilizzare una password per limitare l'accesso a un archivio?

È possibile utilizzare smart card e token con il criptaggio?

È possibile ottenere l'accesso ai dati criptati se non è disponibile la connessione con Kaspersky Security Center?

Che cosa bisogna fare se si verifica un errore del sistema operativo del computer ma i dati rimangono criptati?

ASSISTENZA

Dove viene archiviato il file del rapporto?

Come è possibile creare un file di traccia?

Come è possibile abilitare la scrittura di dump?

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows (di seguito denominato anche Kaspersky Endpoint Security) offre la protezione completa del computer da diversi tipi di minacce, attacchi di phishing e di rete.

L'applicazione non è destinata all'utilizzo nei processi tecnologici che implicano sistemi di controllo automatizzati. Per proteggere i dispositivi in tali sistemi, si consiglia di utilizzare l'applicazione Kaspersky Industrial CyberSecurity for Nodes.

Tecnologie di rilevamento delle minacce



Machine learning

Kaspersky Endpoint Security usa un modello basato sul machine learning. Il modello è sviluppato dagli esperti di Kaspersky. Il modello viene continuamente alimentato con i dati sulle minacce di KSN (addestramento del modello).



Analisi cloud

Kaspersky Endpoint Security riceve i dati relativi alle minacce da Kaspersky Security Network. *Kaspersky Security Network (KSN)* è un'infrastruttura di servizi cloud che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software.



Analisi degli esperti

Kaspersky Endpoint Security usa i dati relativi alle minacce aggiunti dagli analisti anti-virus di Kaspersky. Gli analisti dei virus valutano gli oggetti se non è possibile determinare automaticamente la reputazione di un oggetto.



Analisi del comportamento

Kaspersky Endpoint Security analizza l'attività di un oggetto in tempo reale.



Analisi automatica

Kaspersky Endpoint Security riceve i dati dal sistema automatico di analisi degli oggetti. Il sistema elabora tutti gli oggetti inviati a Kaspersky. Il sistema determina quindi la reputazione dell'oggetto e aggiunge i dati ai database anti-virus. Se il sistema non è in grado di determinare la reputazione dell'oggetto, il sistema interroga gli analisti dei virus di Kaspersky.



Sandbox

Kaspersky Endpoint Security elabora l'oggetto in una macchina virtuale. Kaspersky Sandbox analizza il comportamento dell'oggetto e prende una decisione in merito alla reputazione. Questa tecnologia è disponibile solo se si utilizza la soluzione Kaspersky Sandbox.



Sandbox cloud

Kaspersky Endpoint Security esegue la scansione degli oggetti in un ambiente isolato fornito da Kaspersky. La tecnologia Sandbox cloud è sempre abilitata ed è disponibile per tutti gli utenti di Kaspersky Security Network indipendentemente dal tipo di licenza in uso. Se la soluzione Endpoint Detection and Response è già stata distribuita, è possibile abilitare un contatore separato per le minacce rilevate da Sandbox cloud.

Struttura di selezione

Ogni tipo di minaccia viene gestito da uno specifico componente. I componenti possono essere abilitati o disabilitati indipendentemente e le relative impostazioni possono essere configurate.

Sezione	Componente
Protezione minacce essenziale 	**Protezione minacce file** Il componente Protezione minacce file consente di impedire l'infezione del file system del computer. Per impostazione predefinita, il componente Protezione minacce file risiede permanentemente nella RAM del computer ed esegue la scansione di tutti i file aperti, salvati e avviati in tempo reale. Questo componente esegue la scansione dei file in tutte le unità del computer, incluse le unità collegate. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica. **Protezione minacce Web** Il componente Protezione minacce Web impedisce il download di file dannosi da Internet e blocca inoltre la connessione a siti Web dannosi e di phishing. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica. **Protezione minacce di posta** Il componente Protezione minacce di posta esamina gli allegati dei messaggi e-mail in entrata e in uscita alla ricerca di virus e altre minacce. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica. Protezione minacce di posta può eseguire la scansione sia dei messaggi in entrata che di quelli in uscita. L'applicazione supporta POP3, SMTP, IMAP e NNTP nei seguenti client di posta: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Per eseguire la scansione del traffico nei client di posta Thunderbird, MyOffice Mail e R7-Office Organizer, è necessario aggiungere il certificato Kaspersky all'archivio certificati e selezionare il proprio archivio certificati. Protezione minacce di posta non supporta altri protocolli e client di posta. Protezione minacce di posta potrebbe non essere sempre in grado di ottenere l'accesso a *livello di protocollo* ai messaggi (ad esempio, quando si utilizza la soluzione Microsoft Exchange). Per questo motivo, Protezione minacce di posta include un'estensione per Microsoft Office Outlook. L'estensione consente la scansione dei messaggi al *livello del client di posta*. L'estensione Protezione minacce di posta supporta le versioni a 32 bit e a 64 bit di Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365. Nei computer basati su Arm l'estensione Protezione minacce di posta supporta le versioni a 32 bit e a 64 bit di Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 per Arm64. **Protezione minacce di rete** Il componente *Protezione minacce di rete* (chiamato anche Intrusion Detection System, IDS) monitora il traffico di rete in entrata per verifiche le caratteristiche delle attività degli attacchi di rete. Quando l'applicazione rileva un tentativo di attacco di rete nel computer dell'utente, blocca la connessione di rete con il computer che ha originato l'attacco. Nei database dell'applicazione è inclusa una descrizione degli attacchi di rete attualmente conosciuti, nonché dei metodi utilizzati per contrastarli. L'elenco degli attacchi di rete che il componente Protezione minacce di Rete è in grado di rilevare viene aggiornato durante gli aggiornamenti dei database e dei moduli dell'applicazione. **Firewall** Il componente Firewall blocca le connessioni non autorizzate al computer in Internet o sulla rete locale. Firewall controlla anche l'attività di rete delle applicazioni nel computer. Questo consente di proteggere la LAN aziendale dal furto di identità e da altri attacchi. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e *regole di rete* predefinite. **Prevenzione Attacchi BadUSB** Il componente Prevenzione Attacchi BadUSB impedisce la connessione al computer di dispositivi USB infetti che emulano una tastiera. **Protezione AMSI** Il componente Protezione AMSI è progettato per il supporto dell'interfaccia AMSI (Antimalware Scan Interface) di Microsoft. *AMSI (Antimalware Scan Interface)* consente ad applicazioni di terzi con il supporto AMSI di inviare oggetti (ad esempio script di PowerShell) a Kaspersky Endpoint Security per un'ulteriore analisi e quindi di ricevere i risultati della scansione di questi oggetti.

Sezione	Componente
Protezione minacce avanzata 	**Kaspersky Security Network** *Kaspersky Security Network (KSN)* è un'infrastruttura di servizi cloud che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce risposte più rapide da parte di Kaspersky Endpoint Security alle nuove minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi positivi. Se si partecipa a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla reputazione degli indirizzi Web scansionati, nonché informazioni sulla categoria e sulla reputazione dei file scansionati. **Rilevamento del Comportamento** Il componente Rilevamento del Comportamento riceve dati sulle azioni delle applicazioni nel computer e fornisce tali informazioni ad altri componenti della protezione per migliorarne le prestazioni. Il componente Rilevamento del Comportamento utilizza le firme Behavior Stream Signatures (BSS) per le applicazioni. Se l'attività di un'applicazione corrisponde a uno schema BSS, Kaspersky Endpoint Security esegue l'azione di risposta selezionata. La funzionalità di Kaspersky Endpoint Security basata sugli schemi Behavior Stream Signatures e assicura una difesa proattiva del computer. Il componente Rilevamento del Comportamento consente inoltre di monitorare le porte di rete alla ricerca di processi delle applicazioni che possono minacciare la sicurezza del computer. L'applicazione ottiene informazioni su tali processi con i database anti-virus. **Anti-Cryptor** Il componente Anti-Cryptor analizza le attività nelle cartelle condivise. Se questa attività corrisponde a una firma BSS tipica del criptaggio esterno, Kaspersky Endpoint Security esegue l'azione selezionata. **Prevenzione Exploit** Il componente Prevenzione Exploit rileva il codice del programma che sfrutta le vulnerabilità del computer per sfruttare i privilegi di amministratore o eseguire attività dannose. Gli exploit possono ad esempio utilizzare un attacco di overflow del buffer. A tale scopo, l'exploit invia una grande quantità di dati a un'applicazione vulnerabile. Durante l'elaborazione di questi dati, l'applicazione vulnerabile esegue un codice dannoso. In seguito a questo attacco, l'exploit può avviare un'installazione non autorizzata di malware. In caso di tentativo di esecuzione di un file eseguibile da un'applicazione vulnerabile non eseguito dall'utente, Kaspersky Endpoint Security blocca l'esecuzione di questo file o invia una notifica all'utente. Il componente Prevenzione Exploit consente inoltre di monitorare le porte di rete alla ricerca di processi delle applicazioni che possono minacciare la sicurezza del computer. L'applicazione ottiene informazioni su tali processi con i database anti-virus. **Prevenzione Intrusioni Host** Il componente Prevenzione Intrusioni Host impedisce alle applicazioni di eseguire azioni che possono essere pericolose per il sistema operativo, assicurando il controllo dell'accesso alle risorse del sistema operativo e ai dati personali. Il componente garantisce la protezione del computer mediante database anti-virus e il servizio cloud Kaspersky Security Network. **Motore di Remediation** Il componente Motore di Remediation consente a Kaspersky Endpoint Security di eseguire il rollback delle azioni eseguite dal malware nel sistema operativo.
Controlli di sicurezza 	**Controllo applicazioni** Controllo applicazioni gestisce l'avvio delle applicazioni nei computer degli utenti. Ciò consente di implementare un criterio di sicurezza aziendale quando si utilizzano le applicazioni. Controllo applicazioni riduce anche il rischio di infezione del computer limitando l'accesso alle applicazioni. **Controllo dispositivi** Controllo dispositivi consente di gestire l'accesso dell'utente ai dispositivi installati nel computer o connessi al computer (ad esempio dischi rigidi, fotocamere o moduli Wi-Fi). In questo modo è possibile proteggere il computer dalle infezioni quando tali dispositivi sono connessi e prevenire perdite o fughe di dati. **Controllo Web** Controllo Web gestisce l'accesso degli utenti alle risorse Web. Questo consente di ridurre il traffico e l'utilizzo inappropriato dell'orario di lavoro. Quando un utente tenta di aprire un sito Web sottoposto a restrizioni da Controllo Web, Kaspersky Endpoint Security blocca l'accesso o mostra un avviso. **Controllo adattivo delle anomalie** Il componente Controllo adattivo delle anomalie monitora e blocca le azioni non tipiche dei computer in una rete aziendale. Controllo adattivo delle anomalie utilizza un set di regole per monitorare i comportamenti non tipici (ad esempio, la regola *Avvio di Microsoft PowerShell dall'applicazione Office*). Le regole vengono create dagli esperti di Kaspersky in base agli scenari tipici delle attività dannose. È possibile configurare la modalità di gestione di ogni regola da parte di Controllo adattivo delle anomalie e, ad esempio, consentire l'esecuzione degli script PowerShell per l'automazione di determinate attività del flusso di lavoro. Kaspersky Endpoint Security aggiorna il set di regole insieme ai database dell'applicazione. **Log Inspection** Log Inspection monitora l'integrità dell'ambiente protetto in base all'analisi del Registro eventi di Windows. Quando l'applicazione rileva segnali di comportamento atipico nel sistema, ne informa l'amministratore, poiché questo comportamento potrebbe indicare un tentativo di attacco informatico. **Monitoraggio integrità di sistema** Il componente Monitoraggio integrità di sistema monitora le modifiche nel sistema operativo che potrebbero indicare violazioni della sicurezza del computer. Quando vengono rilevate tali modifiche, Kaspersky Endpoint Security genera gli eventi corrispondenti e avvisa l'amministratore.

Sezione	Componente
Attività 	**Scansione malware** Kaspersky Endpoint Security esamina la presenza di eventuali virus e altre minacce nel computer. Scansione malware consente di eliminare la possibilità che si diffondano malware non rilevati dai componenti della protezione, ad esempio a causa di un livello di sicurezza basso. **Aggiornamento di database e moduli dell'applicazione** Kaspersky Endpoint Security esegue il download dei database e dei moduli dell'applicazione aggiornati. L'aggiornamento mantiene il computer protetto dai virus più recenti e altre minacce. Per impostazione predefinita, l'impostazione viene aggiornata automaticamente, ma è possibile aggiornare manualmente i database e i moduli dell'applicazione, se necessario. **Rollback dell'ultimo aggiornamento** Kaspersky Endpoint Security esegue il rollback dell'ultimo aggiornamento di database e moduli. Questo consente di eseguire il rollback dei database e dei moduli dell'applicazione alle versioni precedenti se necessario, ad esempio quando la nuova versione dei database contiene una firma non valida che determina il blocco di un'applicazione sicura da parte di Kaspersky Endpoint Security. **Controllo integrità applicazione** Kaspersky Endpoint Security verifica se i moduli dell'applicazione nella cartella di installazione dell'applicazione risultano danneggiati o modificati. Se un modulo dell'applicazione ha una firma digitale errata, il modulo viene considerato danneggiato.
Criptaggio dei dati 	**Criptaggio a livello di file** Il componente consente di creare regole di criptaggio dei file. È possibile selezionare cartelle predefinite per il criptaggio, selezionare una cartella manualmente o selezionare singoli file in base all'estensione. **Criptaggio dell'intero disco** Il componente consente di criptare il disco rigido utilizzando Criptaggio disco Kaspersky o Crittografia unità BitLocker. **Criptaggio unità rimovibili** Il componente consente di proteggere i dati su unità rimovibili. È possibile utilizzare il Criptaggio dell'intero disco (FDE) o il Criptaggio a livello di file (FLE).

Sezione	Componente
Detection and Response 	**Endpoint Detection and Response Optimum** Agente integrato per la soluzione Kaspersky Endpoint Detection and Response Optimum (di seguito denominato anche "EDR Optimum"). *Kaspersky Endpoint Detection and Response* è una soluzione che consente di proteggere l'infrastruttura IT aziendale dalle minacce informatiche avanzate. La funzionalità della soluzione combina il rilevamento automatico delle minacce con la capacità di reagire a tali minacce per contrastare gli attacchi avanzati, inclusi nuovi exploit, ransomware, attacchi fileless, nonché metodi che utilizzano strumenti di sistemi legittimi. Per ulteriori informazioni sulla soluzione, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** Agente integrato per la soluzione Kaspersky Endpoint Detection and Response Expert (di seguito denominata anche "EDR Expert"). EDR Expert offre più funzionalità di monitoraggio e risposta delle minacce rispetto a EDR Optimal. Per ulteriori informazioni sulla soluzione, consultare la Guida di Kaspersky Endpoint Detection and Response Expert. **Endpoint Detection and Response Expert (on-premises)** e **Network Detection and Response (KATA)** Agenti integrati per la gestione dei componenti Endpoint Detection and Response e Network Detection and Response che fanno parte della soluzione Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* è una soluzione progettata per il rilevamento tempestivo di minacce sofisticate come attacchi mirati, minacce APT (Advanced Persistent Threat), attacchi zero-day e di altro tipo. Kaspersky Anti Targeted Attack Platform include tre unità funzionali: • Kaspersky Anti Targeted Attack Platform (*KATA*) • Kaspersky Endpoint Detection and Response (*EDR (KATA)*) • Network Detection and Response (*NDR (KATA)*) È possibile acquistare tutte le unità funzionali o le singole unità funzionali separatamente. Per informazioni dettagliate sulla soluzione, consultare la Guida di Kaspersky Anti Targeted Attack Platform. **Sandbox** Agente integrato per Sandbox. Il componente *Sandbox* rileva e blocca automaticamente le minacce avanzate sui computer. Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Sandbox). Per informazioni dettagliate sulla soluzione, consultare la Guida di Kaspersky Sandbox Help e la Guida di Kaspersky Anti Targeted Attack Platform. **Managed Detection and Response** Agente integrato per supportare il funzionamento della soluzione Kaspersky Managed Detection and Response. La soluzione *Kaspersky Managed Detection and Response (MDR)* rileva e analizza automaticamente gli incidenti di sicurezza nell'infrastruttura. A tale scopo, MDR utilizza i dati di telemetria ricevuti dagli endpoint e dal Machine Learning. MDR invia i dati sugli incidenti agli esperti di Kaspersky. Gli esperti possono quindi elaborare l'incidente e, ad esempio, aggiungere una nuova voce ai database anti-virus. In alternativa, gli esperti possono proporre suggerimenti sull'elaborazione dell'incidente e, ad esempio, suggerire di isolare il computer dalla rete. Per informazioni dettagliate sul funzionamento della soluzione, consultare la Guida di Kaspersky Managed Detection and Response.

Modalità dell'applicazione: Standard, EDR Agent, Light Agent

Kaspersky Endpoint Security for Windows fa parte di molte soluzioni Kaspersky. A seconda della soluzione, è necessario selezionare una modalità per l'applicazione.



Modalità Standard

Questa è la modalità principale e predefinita dell'applicazione. È possibile installare l'applicazione in questa modalità come parte delle soluzioni Kaspersky EPP (Endpoint Protection Platform). Ad esempio, Kaspersky Endpoint Security in modalità Standard fa parte di Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security offre una protezione completa di workstation e server da varie minacce, attacchi di rete e truffe. In modalità standard, sono inoltre disponibili agenti integrati per l'integrazione con le soluzioni Kaspersky Detection and Response, inclusi EDR, MDR, KUMA e altri.



EDR Agent

Questa modalità consente di distribuire le soluzioni Kaspersky Detection and Response insieme a soluzioni EPP di terze parti. Le soluzioni Detection and Response includono Kaspersky Managed Detection and Response (MDR) e Kaspersky Anti Targeted Attack Platform (KATA). EDR Agent supporta anche la soluzione Kaspersky SIEM, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

In questa modalità, i componenti standard della protezione come Protezione minacce file o Protezione minacce Web non sono disponibili. La protezione standard del computer è fornita dalla soluzione PPE di terze parti. EDR Agent monitora continuamente i processi in esecuzione su questi computer, le connessioni di rete aperte e i file modificati e interagisce con le soluzioni Detection and Response.



Light Agent

Questa modalità viene utilizzata per proteggere gli ambienti virtuali. Kaspersky Endpoint Security in modalità Light Agent fa parte della soluzione Kaspersky Hybrid Cloud Security. Light Agent protegge le macchine virtuali con sistemi operativi guest per workstation e server. Gli stessi componenti di protezione e controllo sono disponibili in questa modalità come nella modalità Standard. La differenza è che gli oggetti vengono esaminati alla ricerca di virus e altro malware da uno speciale componente della soluzione installato in una macchina virtuale separata, SVM (Secure Virtual Machine). Pertanto, Light Agent utilizza le risorse della SVM per garantire la sicurezza dell'infrastruttura anziché le risorse della macchina virtuale.

Kit di distribuzione

Il kit di distribuzione include i seguenti pacchetti di distribuzione:

- **AES256**

  Questo pacchetto di distribuzione è destinato all'installazione nei computer con architettura x86/x64. Questo pacchetto di distribuzione contiene strumenti crittografici che implementano l'algoritmo di criptaggio AES (Advanced Encryption Standard) con una lunghezza effettiva della chiave di 256 bit.

- **AES56**

  Questo pacchetto di distribuzione è destinato all'installazione nei computer con architettura x86/x64. Questo pacchetto di distribuzione contiene strumenti di criptaggio che implementano l'algoritmo di criptaggio AES con una lunghezza della chiave effettiva di 56 bit.

- **Arm64**

  Questo pacchetto di distribuzione è destinato all'installazione nei computer basati su Arm. Questo pacchetto di distribuzione non è destinato all'installazione nei server.

Prima dell'installazione, assicurarsi che il pacchetto di distribuzione corrisponda all'architettura del processore. Se il pacchetto di distribuzione non corrisponde all'architettura del processore, il programma di installazione terminerà l'installazione con un errore.

Il pacchetto di distribuzione è un archivio a estrazione automatica in formato EXE. Per visualizzare il contenuto del pacchetto di distribuzione, è necessario estrarre l'archivio in una cartella separata. Ogni pacchetto di distribuzione contiene i seguenti file:

`kes_win.msi`	Pacchetto di installazione di Kaspersky Endpoint Security.
`setup_kes.exe`	File necessari per l'installazione dell'applicazione con uno dei metodi disponibili.
`kes_win.kud`	File per la creazione di pacchetti di installazione per Kaspersky Endpoint Security.
`klcfginst.msi`	Pacchetto di installazione per il plug-in di gestione dell'applicazione in Kaspersky Security Center Administration Console.
`bases.cab`	File di pacchetti di aggiornamento utilizzati durante l'installazione.
`cleaner_v2.cab` `cleanerapi_v2.cab`	File per la rimozione del software incompatibile.
`incompatible.txt`	File che contiene l'elenco del software che può causare problemi di compatibilità con Kaspersky Endpoint Security. Kaspersky non garantisce la compatibilità di Kaspersky Endpoint Security con il software presente nell'elenco.
`ksn_<language ID>.txt`	File in cui è possibile leggere le condizioni di partecipazione a Kaspersky Security Network.
`license.txt`	File in cui è possibile leggere il Contratto di licenza con l'utente finale e l'Informativa sulla privacy.
`installer.ini`	File contenente le impostazioni interne del kit di distribuzione.
`kes.cab`	File per l'interfaccia grafica dell'applicazione.
`aes256.cab` / `aes56.cab`	File per l'algoritmo crittografico AES (non incluso nel pacchetto di distribuzione Arm64).
`package.kcat`	File con le firme del kit di distribuzione dell'applicazione. La firma digitale garantisce l'autenticità e l'integrità del kit di distribuzione dell'applicazione.

Non è consigliabile modificare i valori di queste impostazioni. Se si desidera modificare le opzioni di installazione, utilizzare il file setup.ini.

Requisiti hardware e software

In questo articolo sono elencate le versioni del software su cui l'applicazione è stata testata e per le quali ne è garantito il corretto funzionamento. L'applicazione può funzionare anche con altre versioni del software, ma tali configurazioni non sono state sottoposte a un ciclo completo di test e non sono incluse nell'elenco delle versioni con supporto garantito.

Per il corretto funzionamento di Kaspersky Endpoint Security, il computer deve soddisfare i seguenti requisiti:

Per installare l'applicazione, sono necessari diritti di amministratore per il computer.

Requisiti minimi generali

Requisiti minimi	Workstation (x86/x64)	Server (x86/x64)	Arm
Storage	2 GB	2 GB	2 GB
CPU	1 GHz, supporto delle istruzioni SSE2.	1,4 GHz, supporto delle istruzioni SSE2.	1 GHz, architettura Armv8.1
RAM	Workstation (x86): 1 GB Workstation (x64): 2 GB	2 GB Nota: il server richiede 8 GB di memoria per installare l'applicazione con l'agente integrato per l'integrazione con Kaspersky Anti Targeted Attack Platform.	4 GB
Microsoft .NET Framework	4 o versioni successive	4 o versioni successive	4.8 o versioni successive

Workstation

Sistemi operativi supportati per workstation:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- Windows 8 Professional/Enterprise;
- Windows 8.1 Professional/Enterprise;
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessione;
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessione;
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

I sistemi operativi Windows, a partire dalla versione 11 24H2, supportano la tecnologia UDP Receive Segment Coalescing Offload (URO). La tecnologia è abilitata per impostazione predefinita se nel computer sono installati una scheda di rete e driver compatibili. La disabilitazione di URO nel computer di un utente può ridurre significativamente le prestazioni dell'applicazione.

Per garantire il corretto funzionamento di Kaspersky Endpoint Security, il servizio Windows Security Center (wscsvc) deve essere in esecuzione nel computer dell'utente.

Kaspersky Endpoint Security non può essere installato in Microsoft Windows 7 senza gli aggiornamenti del sistema operativo installati: KB4490628 (12 marzo 2019) e KB4474419 (23 settembre 2019). Per informazioni dettagliate, consultare la Knowledge Base dell'Assistenza tecnica.

Per informazioni dettagliate sul supporto per il sistema operativo Microsoft Windows 10, fare riferimento alla

Knowledge Base dell'Assistenza tecnica.

Per informazioni dettagliate sul supporto per il sistema operativo Microsoft Windows 11, fare riferimento alla Knowledge Base dell'Assistenza tecnica.

Server

Kaspersky Endpoint Security supporta i componenti principali dell'applicazione nei computer in cui viene eseguito il sistema operativo Windows per server. È possibile utilizzare Kaspersky Endpoint Security for Windows anziché Kaspersky Security for Windows Server nei server e nei cluster dell'organizzazione (Cluster Mode). L'applicazione supporta anche la Server Core Mode (vedere i problemi noti).

Sistemi operativi supportati per server:

- Windows Small Business Server 2011 Essentials/Standard (64 bit);

  Microsoft Small Business Server 2011 Standard (64 bit) è supportato solo in caso di installazione del Service Pack 1 per Microsoft Windows Server 2008 R2.

- Windows MultiPoint Server 2011 (64 bit);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (inclusa la modalità Server Core);
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (inclusa la modalità Server Core);
- Windows Server 2016 Essentials / Standard / Datacenter (inclusa la modalità Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (inclusa la modalità Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (inclusa la modalità Server Core);
- Windows Server 2025 Standard / Datacenter.

Kaspersky Endpoint Security non può essere installato in Microsoft Windows Server 2008 R2 senza gli aggiornamenti del sistema operativo installati: KB4490628 (12 marzo 2019) e KB4474419 (23 settembre 2019).

Per informazioni dettagliate sul supporto per i sistemi operativi Microsoft Windows Server 2016 e Microsoft Windows Server 2019, fare riferimento alla Knowledge Base dell'Assistenza tecnica.

Per informazioni dettagliate sul supporto per il sistema operativo Microsoft Windows Server 2022, consultare la Knowledge Base dell'Assistenza tecnica.

Sistemi operativi per server non supportati:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

Piattaforme virtuali

Piattaforme virtuali supportate per il funzionamento dell'applicazione in modalità standard:

- VMware Workstation Pro 15.5.2;
- VMware ESXi 7.0 Patch Release ESXi 7.0b
- Windows Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7 2009;
- Citrix Provisioning 2009;
- Citrix Hypervisor 8.2 LTSR

L'applicazione supporta le macchine virtuali in cui viene eseguito Windows 11 Pro Arm64 create utilizzando Hyper-V.

Macchine virtuali per l'installazione di Light Agent

L'installazione di Kaspersky Endpoint Security in modalità Light Agent in macchine virtuali basate su Arm non è supportata.

Il BIOS nelle macchine virtuali deve supportare la specifica SMBIOS versione 2.1 o successiva.

Nelle macchine virtuali, è necessario installare i seguenti pacchetti e utilità:

- Quando si usa il pacchetto Microsoft Hyper-V - Integration Services.
- Quando si utilizza VMware vSphere - Pacchetto VMware Tools.
- Quando si utilizza il pacchetto XenServer - XenTools.
- Quando si utilizza il pacchetto HUAWEI FusionSphere - HUAWEI Tools.
- Quando si utilizzano hypervisor basati su KVM: QEMU Guest Agent.

Consultare la Guida Kaspersky Security for Virtualization Light Agent per i requisiti dell'infrastruttura virtuale per eseguire l'applicazione in modalità Light Agent.

Per il corretto funzionamento dell'applicazione, utilizzare un'interfaccia di rete virtualizzata con una larghezza di banda di almeno 100 Mbit/s.

Terminal server

Tipi di terminal server supportati:

- Microsoft Remote Desktop Services basato su Windows Server 2008 R2 SP1
- Microsoft Remote Desktop Services basato su Windows Server 2012
- Microsoft Remote Desktop Services basato su Windows Server 2012 R2
- Microsoft Remote Desktop Services basato su Windows Server 2016
- Microsoft Remote Desktop Services basato su Windows Server 2019
- Microsoft Remote Desktop Services basato su Windows Server 2022
- Microsoft Remote Desktop Services basato su Windows Server 2025
- Citrix RDSH da Citrix Virtual Apps and Desktops 7 2507 LTSR

Supporto di Kaspersky Security Center

Kaspersky Endpoint Security supporta il funzionamento con le seguenti versioni di Kaspersky Security Center:

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16

- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2
- Kaspersky Security Center Linux 16.3
- Kaspersky Security Center Linux 17

Confronto tra le funzionalità delle applicazioni disponibili a seconda del tipo di sistema operativo

Il set di funzionalità Kaspersky Endpoint Security disponibili dipende dal tipo di sistema operativo: workstation o server (vedere la tabella di seguito).

A partire da Kaspersky Endpoint Security12.8 for Windows, è possibile configurare diversi set di componenti per diversi tipi di sistemi operativi nel pacchetto di installazione. In altre parole, è possibile distribuire l'applicazione a workstation e server utilizzando lo stesso pacchetto di installazione.

L'installazione di Kaspersky Endpoint Security in modalità Light Agent in macchine virtuali basate su Arm non è supportata.

Confronto delle funzionalità Kaspersky Endpoint Security

Funzionalità	Workstation	Workstation basata su Arm	Server	Modalità Server Core
Protezione minacce avanzata				
Kaspersky Security Network	✓	✓	✓	✓
Rilevamento del Comportamento	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓
Prevenzione Exploit	✓	✓	✓	✓
Prevenzione Intrusioni Host	✓	✓	–	–
Motore di Remediation	✓	✓	✓	✓
Protezione minacce essenziale				
Protezione minacce file	✓	✓	✓	✓
Protezione minacce Web	✓	✓	✓	–
Protezione minacce di posta	✓	✓	✓	–
Firewall	✓	✓	✓	✓
Protezione minacce di rete	✓	✓	✓	✓
Prevenzione Attacchi BadUSB	✓	✓	✓	–
Protezione AMSI	✓	✓	✓	✓
Controlli di sicurezza				
Log Inspection	–	–	✓	–
Controllo applicazioni	✓	✓	✓	✓
Controllo dispositivi	✓	✓	✓	✓
Controllo Web	✓	✓	✓	–

Funzionalità	Workstation	Workstation basata su Arm	Server	Modalità Server Core
Controllo adattivo delle anomalie	✓	✓	–	–
Monitoraggio integrità di sistema	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Criptaggio dei dati				
Criptaggio disco Kaspersky	✓	–	–	–
Crittografia unità BitLocker	✓	✓	✓	✓
Criptaggio a livello di file	✓	–	–	–
Criptaggio unità rimovibili	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
Integrazione KUMA	✓	✓	✓	✓

Confronto tra le funzioni dell'applicazione in base agli strumenti di gestione

Il set di funzioni disponibili in Kaspersky Endpoint Security dipende dagli strumenti di gestione (vedere la tabella seguente).

È possibile gestire l'applicazione utilizzando le seguenti console di Kaspersky Security Center:

- Administration Console. Snap-in di MMC (Microsoft Management Console) installata nella workstation dell'amministratore.
- Web Console. Componente di Kaspersky Security Center installato in Administration Server. È possibile utilizzare Web Console tramite un browser su qualsiasi computer.

È inoltre possibile gestire l'applicazione utilizzando Kaspersky Security Center Cloud Console. *Kaspersky Security Center Cloud Console* è la versione cloud di Kaspersky Security Center. Questo significa che Administration Server e altri componenti di Kaspersky Security Center sono installati nell'infrastruttura cloud di Kaspersky. Per informazioni dettagliate sulla gestione dell'applicazione tramite Kaspersky Security Center Cloud Console, consultare la Guida di Kaspersky Security Center Cloud.

Kaspersky Endpoint Security fa parte della soluzione Kaspersky Next Pro View. Per ulteriori informazioni sulle funzionalità dell'applicazione disponibili quando funziona come parte di questa soluzione, consultare la Guida di Kaspersky Next.

Funzionalità	Kaspersky Security Center		Kaspersky Security Center
	Administration Console	Web Console	Cloud Console
Protezione minacce avanzata			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Rilevamento del Comportamento	✓	✓	✓
Anti-Cryptor			
Prevenzione Exploit	✓	✓	✓
Prevenzione Intrusioni Host	✓	✓	✓
Motore di Remediation	✓	✓	✓
Protezione minacce essenziale			
Protezione minacce file	✓	✓	✓
Protezione minacce Web	✓	✓	✓
Protezione minacce di posta	✓	✓	✓
Firewall	✓	✓	✓
Protezione minacce di rete	✓	✓	✓
Prevenzione Attacchi BadUSB	✓	✓	✓
Protezione AMSI	✓	✓	✓
Controlli di sicurezza			
Log Inspection	✓	✓	✓
Controllo applicazioni	✓	✓	✓
Controllo dispositivi	✓	✓	✓
Controllo Web	✓	✓	✓
Controllo adattivo delle anomalie	✓	✓	✓
Monitoraggio integrità di sistema	✓	✓	✓
Cloud Discovery	–	–	✓
Criptaggio dei dati			
Criptaggio disco Kaspersky	✓	✓	–
Crittografia unità BitLocker	✓	✓	✓
Criptaggio a livello di file	✓	✓	–
Criptaggio unità rimovibili	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Integrazione KUMA	✓	✓	✓
Attività			

Funzionalità	Kaspersky Security Center		Kaspersky Security Center
	Administration Console	Web Console	Cloud Console
Aggiungi chiave	✓	✓	✓
Modifica i componenti dell'applicazione	✓	✓	✓
Inventario	✓	✓	✓
Aggiornamento	✓	✓	✓
Rollback degli aggiornamenti	✓	✓	✓
Scansione malware	✓	✓	✓
Controllo integrità applicazione	✓	✓	–
Cancella dati	✓	✓	✓
Gestisci account dell'Agente di Autenticazione (Criptaggio disco Kaspersky)	✓	✓	–
Scansione IOC (EDR)	–	✓	✓
Sposta file in Quarantena (EDR)	–	✓	✓
Ottieni file (EDR)	–	✓	✓
Elimina il file (EDR)	–	✓	✓
Avvia processo (EDR)	–	✓	✓
Termina processo (EDR)	–	✓	✓

Compatibilità con altre applicazioni

Kaspersky Endpoint Security è incompatibile con alcune applicazioni Kaspersky, nonché con alcune applicazioni di terze parti. Pertanto, prima dell'installazione, dell'aggiornamento della versione dell'applicazione e della modifica dei componenti dell'applicazione, Kaspersky Endpoint Security esegue la scansione del computer per verificare la presenza di tali applicazioni.

Compatibilità con applicazioni di terzi

Kaspersky Endpoint Security è incompatibile con le applicazioni che fanno parte di sistemi di protezione degli endpoint di terze parti (Endpoint Protection Platform, PPE). Kaspersky Endpoint Security può inoltre riscontrare problemi di compatibilità con altre applicazioni. Per determinare la compatibilità, Kaspersky Endpoint Security consulta un elenco di software preparato da Kaspersky. Questo elenco è contenuto nel file incompatible.txt. Il file è incluso nel kit di distribuzione.

Kaspersky non garantisce la compatibilità di Kaspersky Endpoint Security con il software presente nell'elenco. Se viene rilevata un'applicazione nell'elenco, il programma di installazione interrompe la distribuzione di Kaspersky Endpoint Security. Il programma di installazione potrebbe eliminare automaticamente alcune applicazioni dall'elenco. Se si desidera ignorare i rischi e si desidera installare Kaspersky Endpoint Security e una parte del software nell'elenco nello stesso computer, è possibile ignorare la verifica del computer (vedere le istruzioni di seguito).

SCARICA IL FILE INCOMPATIBLE.TXT

Compatibilità con le applicazioni Kaspersky

Kaspersky Endpoint Security è incompatibile con le seguenti applicazioni Kaspersky:

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Endpoint Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Sensore Endpoint come parte delle soluzioni Kaspersky Anti Targeted Attack Platform e Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Agent come parte delle soluzioni Detection and Response di Kaspersky.

  Kaspersky sta trasferendo tutte le funzioni di Detection and Response affinché funzionino con l'agente integrato di Kaspersky Endpoint Security anziché con Kaspersky Endpoint Agent. A partire dalla versione 12.1, l'applicazione supporta tutte le soluzioni Detection and Response.

- Kaspersky Security for Virtualization Light Agent.
- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security for Windows Server

  A partire da Kaspersky Endpoint Security 12.0 è possibile eseguire la migrazione da Kaspersky Security for Windows Server a Kaspersky Endpoint Security for Windows e utilizzare un'unica soluzione per proteggere workstation e server.

- Kaspersky Embedded Systems Security.

Se le applicazioni Kaspersky presenti in questo elenco sono installate nel computer, Kaspersky Endpoint Security le rimuove. Attendere il completamento del processo prima di procedere all'installazione di Kaspersky Endpoint Security.

Ignorare il controllo della presenza di software che potrebbe causare problemi di compatibilità

Se Kaspersky Endpoint Security rileva software nell'elenco incompatible.txt, l'installazione dell'applicazione verrà terminata. Per continuare l'installazione, è necessario rimuovere l'applicazione. Tuttavia, se il produttore di software di terzi ha indicato nella documentazione che il software è compatibile con le soluzioni Endpoint Protection Platform (EPP), è possibile installare Kaspersky Endpoint Security su un computer contenente un'applicazione di questo produttore. Ad esempio, il fornitore di soluzioni Endpoint Detection and Response (EDR) può dichiarare la propria compatibilità con i sistemi EPP di terzi. In questo caso, è necessario avviare l'installazione di Kaspersky Endpoint Security senza eseguire un controllo del software installato. A tale scopo, passare i seguenti parametri al programma di installazione:

- `SKIPPRODUCTCHECK=1` Disabilitare la verifica della presenza di software installato. L'elenco del software che può causare problemi di compatibilità è disponibile nel file incompatible.txt incluso nel kit di distribuzione. Se non viene impostato alcun valore per questo parametro e viene rilevato software nell'elenco, l'installazione di Kaspersky Endpoint Security verrà terminata.

- `SKIPPRODUCTUNINSTALL=1` Disabilitare la rimozione automatica del software rilevato nell'elenco incompatible.txt. Se non viene impostato alcun valore per questo parametro, Kaspersky Endpoint Security tenta di rimuovere il software che potrebbe causare problemi di compatibilità.

- `CLEANERSIGNCHECK=0` Disabilitare la verifica della firma digitale delle applicazioni rilevate dal controllo. Se questo parametro non è impostato, la verifica delle firme digitali è disabilitata durante la distribuzione dell'applicazione tramite Kaspersky Security Center. Quando l'applicazione è installata in locale, la verifica della firma digitale è abilitata per impostazione predefinita.

È possibile passare i parametri nella riga di comando durante l'installazione dell'applicazione in locale.

Se durante il processo di installazione è stata ignorata la scansione del software che potrebbe causare problemi di compatibilità, Kaspersky Endpoint Security può eseguire nuovamente il controllo quando i componenti dell'applicazione cambiano. Per ignorare la scansione del software installato, è necessario configurare l'attività *Modifica i componenti dell'applicazione*.

Esempio:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Per installare Kaspersky Endpoint Security da remoto, è necessario aggiungere i parametri appropriati al file di generazione del pacchetto di installazione denominato `kes_win.kud` in `[Setup]` (vedere di seguito). Il file `kes_win.kud` è incluso nel kit di distribuzione.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

Installazione e rimozione dell'applicazione

Kaspersky Endpoint Security può essere installato in un computer nei seguenti modi:

- In locale, utilizzando l'Installazione guidata.
- In locale dalla riga di comando.
- Da remoto tramite Kaspersky Security Center.
- Da remoto tramite l'editor Gestione Criteri di gruppo di Microsoft Windows (per ulteriori dettagli, visitare il sito Web del supporto tecnico di Microsoft).
- In remoto, utilizzando System Center Configuration Manager.

È possibile configurare le impostazioni di installazione delle applicazioni in diversi modi. Se si utilizzano contemporaneamente più metodi per configurare le impostazioni, Kaspersky Endpoint Security applica le impostazioni con la priorità più elevata. Kaspersky Endpoint Security utilizza il seguente ordine di priorità:

1. Impostazioni ricevute dal file setup.ini.
2. Impostazioni ricevute dal file installer.ini.
3. Impostazioni ricevute dalla riga di comando.
4. Impostazioni ricevute dal file di configurazione (install.cfg).

È consigliabile chiudere tutte le applicazioni in esecuzione prima di avviare l'installazione di Kaspersky Endpoint Security (inclusa l'installazione remota).

Durante l'installazione di Kaspersky Endpoint Security, il sistema operativo potrebbe mostrare i propri messaggi. È inoltre possibile che le connessioni di rete e Internet vengano interrotte durante l'installazione dell'applicazione.

Durante l'installazione, l'aggiornamento o la disinstallazione di Kaspersky Endpoint Security, potrebbero verificarsi degli errori. Per ulteriori informazioni sulla risoluzione di questi errori, consultare la Knowledge Base dell'Assistenza tecnica.

Distribuzione tramite Kaspersky Security Center

Kaspersky Endpoint Security può essere distribuito nei computer all'interno di una rete aziendale in diversi modi. È possibile scegliere lo scenario di distribuzione più adatto all'organizzazione o combinare diversi scenari di distribuzione contemporaneamente. Prima di installare l'applicazione, è necessario assicurarsi che Kaspersky Security Center Network Agent sia installato nel computer. *Network Agent* semplifica l'interazione tra Administration Server e un computer client.

Kaspersky Security Center supporta i seguenti metodi di distribuzione principali:

- Installazione dell'applicazione utilizzando la Distribuzione guidata della protezione.

  Il metodo di installazione standard è utile se l'utente è soddisfatto delle impostazioni predefinite di Kaspersky Endpoint Security e l'organizzazione dispone di un'infrastruttura semplice che non richiede configurazioni speciali.

- Installazione dell'applicazione utilizzando l'attività di installazione remota.

  Metodo di installazione universale, che consente di configurare le impostazioni di Kaspersky Endpoint Security e gestire in modo flessibile le attività di installazione remota. L'installazione di Kaspersky Endpoint Security comprende i seguenti passaggi:

  1. Creazione di un pacchetto di installazione.
  2. Creazione di un'attività di installazione remota.

Kaspersky Security Center supporta inoltre altri metodi di installazione di Kaspersky Endpoint Security, ad esempio la distribuzione all'interno di un'immagine del sistema operativo. Per informazioni dettagliate sugli altri metodi di distribuzione, consultare la Guida di Kaspersky Security Center.

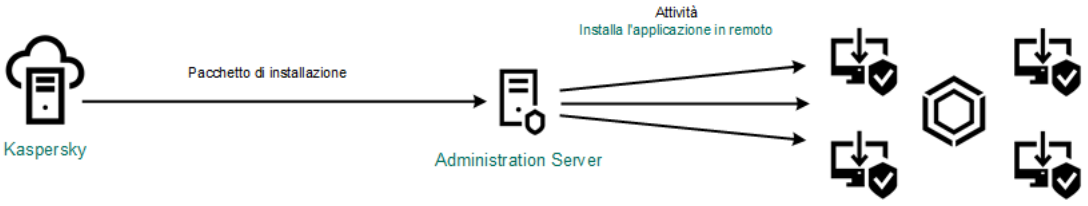
Installazione standard dell'applicazione

Kaspersky Security Center fornisce la Distribuzione guidata della protezione per installare l'applicazione nei computer aziendali. La Distribuzione guidata della protezione include le seguenti azioni principali:

1. Selezione di un pacchetto di installazione per Kaspersky Endpoint Security.

   Un *pacchetto di installazione* è un set di file creati per l'installazione remota di un'applicazione Kaspersky tramite Kaspersky Security Center. Il pacchetto di installazione contiene una serie di impostazioni necessarie per installare l'applicazione e renderla operativa subito dopo l'installazione. Il pacchetto di installazione viene creato utilizzando i file con le estensioni .kpd e. kud inclusi nel kit di distribuzione dell'applicazione. Il pacchetto di installazione di Kaspersky Endpoint Security è comune per tutte le versioni Windows supportate e i tipi di architettura del processore.

2. Creazione dell'attività *Installa l'applicazione in remoto* di Kaspersky Security Center Administration Server.



Distribuzione di Kaspersky Endpoint Security

Come eseguire la Distribuzione guidata della protezione in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Avanzate** → **Installazione remota**.
3. Fare clic sul collegamento **Distribuisci il pacchetto di installazione nei dispositivi gestiti (workstation)**.

Verrà avviata la Distribuzione guidata della protezione. Attenersi alle istruzioni della procedura guidata.

Le porte TCP 139 e 445 e le porte UDP 137 e 138 devono essere aperte in un computer client.

Passaggio 1. Selezione di un pacchetto di installazione

Selezionare il pacchetto di installazione di Kaspersky Endpoint Security dall'elenco. Se l'elenco non contiene il pacchetto di installazione per Kaspersky Endpoint Security, è possibile creare il pacchetto nella procedura guidata.

È possibile configurare le impostazioni del pacchetto di installazione in Kaspersky Security Center. È ad esempio possibile selezionare i componenti dell'applicazione che verranno installati in un computer.

Network Agent verrà inoltre installato insieme a Kaspersky Endpoint Security. *Network Agent* semplifica l'interazione tra Administration Server e un computer client. Se Network Agent è già installato nel computer, non viene installato nuovamente.

Passaggio 2. Selezione dell'origine del pacchetto di installazione

Selezionare l'origine **Distribuisci il pacchetto Kaspersky Security Center**.

Passaggio 3. Selezione dei dispositivi per l'installazione

Selezionare i computer per l'installazione di Kaspersky Endpoint Security. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. Network Agent non viene installato nei dispositivi non assegnati. In questo caso l'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 4. Definizione delle impostazioni dell'attività di installazione remota

Configurare le seguenti impostazioni aggiuntive dell'applicazione:

- **Forza il download del pacchetto di installazione**. Selezionare il metodo di installazione dell'applicazione:
  - **Utilizzando Network Agent**. Network Agent è responsabile della distribuzione del pacchetto di installazione di Kaspersky Endpoint Security ai computer client. Se Network Agent non è installato, l'attività verrà terminata con un errore. In questo caso, aggiungere il pacchetto di installazione di Network Agent all'attività *Installa l'applicazione in remoto* e abilitare l'invio dei file tramite le risorse del sistema operativo. Successivamente, Network Agent verrà installato utilizzando le risorse del sistema operativo. Kaspersky Endpoint Security verrà quindi installato dagli strumenti di Network Agent.
  - **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**. Il pacchetto di installazione viene distribuito ai computer client utilizzando le risorse del sistema operativo tramite punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete. Per informazioni dettagliate sui punti di distribuzione, consultare la Guida di Kaspersky Security Center.
  - **Utilizzando le risorse del sistema operativo tramite Administration Server**. I file verranno inviati ai computer client utilizzando le risorse del sistema operativo tramite Administration Server. È possibile selezionare questa opzione se nel computer client non è installato alcun Network Agent, ma il computer client si trova nella stessa rete di Administration Server.
- **Comportamento per i dispositivi gestiti tramite altri Administration Server**. Selezionare il metodo di installazione per Kaspersky Endpoint Security. Se nella rete è installato più di un Administration Server, questi Administration Server possono visualizzare gli stessi computer client. Ciò può ad esempio causare l'installazione in remoto di un'applicazione nello stesso computer client più volte tramite diversi Administration Server o altri conflitti.
- **Non reinstallare l'applicazione se è già installata**. Se ad esempio si desidera installare una versione precedente dell'applicazione, deselezionare la casella di controllo.
- **Assegna l'installazione di Network Agent in Criteri di gruppo di Active Directory**. Installazione manuale di Network Agent utilizzando le risorse di Active Directory. Per installare Network Agent, l'attività di installazione remota deve essere eseguita con i privilegi dell'amministratore di dominio.

Passaggio 5. Selezione di una chiave di licenza

Aggiungere una chiave al pacchetto di installazione per attivare l'applicazione. Questo passaggio è facoltativo. Se Administration Server contiene una chiave di licenza con funzionalità di distribuzione automatica, la chiave verrà aggiunta automaticamente in un secondo momento. È inoltre possibile attivare l'applicazione in un secondo momento utilizzando l'attività *Aggiungi chiave*.

Passaggio 6. Selezione dell'impostazione di riavvio del sistema operativo

Selezionare l'azione che deve essere eseguita se è richiesto il riavvio del computer. Il riavvio non è richiesto durante l'installazione di Kaspersky Endpoint Security. Il riavvio è richiesto solo se è necessario rimuovere applicazioni incompatibili prima dell'installazione. Potrebbe essere necessario il riavvio anche durante l'aggiornamento della versione dell'applicazione.

Passaggio 7. Rimozione delle applicazioni incompatibili prima di installare l'applicazione

Leggere attentamente l'elenco delle applicazioni incompatibili e consentire la rimozione di queste applicazioni. Se nel computer sono installate applicazioni incompatibili, l'installazione di Kaspersky Endpoint Security termina con un errore.

Passaggio 8. Selezione di un account per l'accesso ai dispositivi

Selezionare l'account per l'installazione di Network Agent utilizzando gli strumenti del sistema operativo. In questo caso sono richiesti i diritti di amministratore per l'accesso al computer. È possibile aggiungere più account. Se un account non dispone dei diritti sufficienti, l'Installazione guidata utilizza l'account successivo. Se si installa Kaspersky Endpoint Security utilizzando gli strumenti di Network Agent, non è necessario selezionare un account.

Passaggio 9. Avvio dell'installazione

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come avviare la Distribuzione guidata della protezione in Web Console e Cloud Console

Nella finestra principale di Web Console, fare clic su **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Distribuzione guidata della protezione**.

Verrà avviata la Distribuzione guidata della protezione. Attenersi alle istruzioni della procedura guidata.

Le porte TCP 139 e 445 e le porte UDP 137 e 138 devono essere aperte in un computer client.

Passaggio 1. Selezione di un pacchetto di installazione

Selezionare il pacchetto di installazione di Kaspersky Endpoint Security dall'elenco. Se l'elenco non contiene il pacchetto di installazione per Kaspersky Endpoint Security, è possibile creare il pacchetto nella procedura guidata. Per creare il pacchetto di installazione non è necessario cercare il pacchetto di distribuzione e salvarlo nella memoria del computer. In Kaspersky Security Center è possibile visualizzare l'elenco dei pacchetti di distribuzione che si trovano nei server Kaspersky e il pacchetto di installazione viene creato automaticamente. Kaspersky aggiorna l'elenco dopo il rilascio di nuove versioni delle applicazioni.

È possibile configurare le impostazioni del pacchetto di installazione in Kaspersky Security Center. È ad esempio possibile selezionare i componenti dell'applicazione che verranno installati in un computer.

Passaggio 2. Selezione di una chiave di licenza

Aggiungere una chiave al pacchetto di installazione per attivare l'applicazione. Questo passaggio è facoltativo. Se Administration Server contiene una chiave di licenza con funzionalità di distribuzione automatica, la chiave verrà aggiunta automaticamente in un secondo momento. È inoltre possibile attivare l'applicazione in un secondo momento utilizzando l'attività *Aggiungi chiave*.

Passaggio 3. Selezione di un Network Agent

Selezionare la versione di Network Agent che verrà installata insieme a Kaspersky Endpoint Security. *Network Agent* semplifica l'interazione tra Administration Server e un computer client. Se Network Agent è già installato nel computer, non viene installato nuovamente.

Passaggio 4. Selezione dei dispositivi per l'installazione

Selezionare i computer per l'installazione di Kaspersky Endpoint Security. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. Network Agent non viene installato nei dispositivi non assegnati. In questo caso l'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 5. Configurazione delle impostazioni avanzate

Configurare le seguenti impostazioni aggiuntive dell'applicazione:

- **Forza il download del pacchetto di installazione**. Selezionare il metodo di installazione dell'applicazione:
  - **Utilizzando Network Agent**. Network Agent è responsabile della distribuzione del pacchetto di installazione di Kaspersky Endpoint Security ai computer client. Se Network Agent non è installato, l'attività verrà terminata con un errore. In questo caso, aggiungere il pacchetto di installazione di Network Agent all'attività *Installa l'applicazione in remoto* e abilitare l'invio dei file tramite le risorse del sistema operativo. Successivamente, Network Agent verrà installato utilizzando le risorse del sistema operativo. Kaspersky Endpoint Security verrà quindi installato dagli strumenti di Network Agent.
  - **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**. Il pacchetto di installazione viene distribuito ai computer client utilizzando le risorse del sistema operativo tramite punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete. Per informazioni dettagliate sui punti di distribuzione, consultare la Guida di Kaspersky Security Center.
  - **Utilizzando le risorse del sistema operativo tramite Administration Server**. I file verranno inviati ai computer client utilizzando le risorse del sistema operativo tramite Administration Server. È possibile selezionare questa opzione se nel computer client non è installato alcun Network Agent, ma il computer client si trova nella stessa rete di Administration Server.
- **Non reinstallare l'applicazione se è già installata**. Se ad esempio si desidera installare una versione precedente dell'applicazione, deselezionare la casella di controllo.
- **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory**. Kaspersky Endpoint Security viene installato tramite Network Agent oppure manualmente tramite Active Directory. Per installare Network Agent, l'attività di installazione remota deve essere eseguita con i privilegi dell'amministratore di dominio.

Passaggio 6. Selezione dell'impostazione di riavvio del sistema operativo

Selezionare l'azione che deve essere eseguita se è richiesto il riavvio del computer. Il riavvio non è richiesto durante l'installazione di Kaspersky Endpoint Security. Il riavvio è richiesto solo se è necessario rimuovere applicazioni incompatibili prima dell'installazione. Potrebbe essere necessario il riavvio anche durante l'aggiornamento della versione dell'applicazione.

Passaggio 7. Rimozione delle applicazioni incompatibili prima di installare l'applicazione

Leggere attentamente l'elenco delle applicazioni incompatibili e consentire la rimozione di queste applicazioni. Se nel computer sono installate applicazioni incompatibili, l'installazione di Kaspersky Endpoint Security termina con un errore.

Passaggio 8. Assegnazione a un gruppo di amministrazione

Selezionare il gruppo di amministrazione in cui verranno spostati i computer dopo l'installazione di Network Agent. I computer devono essere spostati in un gruppo di amministrazione in modo che possano essere applicati criteri e attività di gruppo. Se un computer fa già parte di un gruppo di amministrazione, il computer non verrà spostato. Se non si seleziona un gruppo di amministrazione, i computer verranno aggiunti al gruppo **Dispositivi non assegnati**.

Passaggio 9. Selezione di un account per l'accesso ai dispositivi

Selezionare l'account per l'installazione di Network Agent utilizzando gli strumenti del sistema operativo. In questo caso sono richiesti i diritti di amministratore per l'accesso al computer. È possibile aggiungere più account. Se un account non dispone dei diritti sufficienti, l'Installazione guidata utilizza l'account successivo. Se si installa Kaspersky Endpoint Security utilizzando gli strumenti di Network Agent, non è necessario selezionare un account.

Passaggio 10. Avvio dell'installazione

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Creazione di un pacchetto di installazione

Un *pacchetto di installazione* è un set di file creati per l'installazione remota di un'applicazione Kaspersky tramite Kaspersky Security Center. Il pacchetto di installazione contiene una serie di impostazioni necessarie per installare l'applicazione e renderla operativa subito dopo l'installazione. Il pacchetto di installazione viene creato utilizzando i file con le estensioni .kpd e. kud inclusi nel kit di distribuzione dell'applicazione. Il pacchetto di installazione di Kaspersky Endpoint Security è comune per tutte le versioni Windows supportate e i tipi di architettura del processore.

Come creare un pacchetto di installazione in Administration Console (MMC)

1. In Administration, Console passare alla cartella **Administration Server → Avanzate → Installazione remota → Pacchetti di installazione**.

   Si aprirà un elenco di pacchetti di installazione che sono stati scaricati in Kaspersky Security Center.

2. Fare clic su **Crea pacchetto di installazione**.

Viene avviata la Creazione guidata nuovo pacchetto. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di pacchetto di installazione

Selezionare l'opzione **Creare un pacchetto di installazione per un'applicazione Kaspersky**.

Passaggio 2. Definizione del nome del pacchetto di installazione

Immettere il nome del pacchetto di installazione, ad esempio *Kaspersky Endpoint Security for Windows 14.2*.

Passaggio 3. Selezione del pacchetto di distribuzione per l'installazione

Fare clic sul pulsante **Sfoglia** e selezionare il file `kes_win.kud` incluso nel kit di distribuzione.

Se necessario, aggiornare i database anti-virus nel pacchetto di installazione utilizzando la casella di controllo **Copia aggiornamenti dall'archivio al pacchetto di installazione**.

Passaggio 4. Contratto di licenza con l'utente finale e Informativa sulla privacy

Leggere e accettare i termini del Contratto di licenza con l'utente finale e dell'Informativa sulla privacy.

Il pacchetto di installazione verrà creato e aggiunto a Kaspersky Security Center. Utilizzando il pacchetto di installazione, è possibile installare Kaspersky Endpoint Security nei computer della rete aziendale o aggiornare la versione dell'applicazione.

Nelle impostazioni del pacchetto di installazione, è possibile selezionare i componenti dell'applicazione per i diversi tipi di sistemi operativi. Ovvero, il pacchetto di installazione include due set di componenti: per le workstation e per i server. Prima di distribuire il pacchetto di installazione, il programma di installazione rileva il tipo di sistema operativo e installa solo i componenti dell'applicazione selezionati per il tipo di sistema operativo. In questo modo, è possibile utilizzare lo stesso pacchetto di installazione per le workstation e i server.

Il pacchetto di installazione contiene database anti-virus dell'archivio di Administration Server. È possibile aggiornare i database nel pacchetto di installazione per ridurre il consumo di traffico durante l'aggiornamento dei database dopo l'installazione di Kaspersky Endpoint Security.

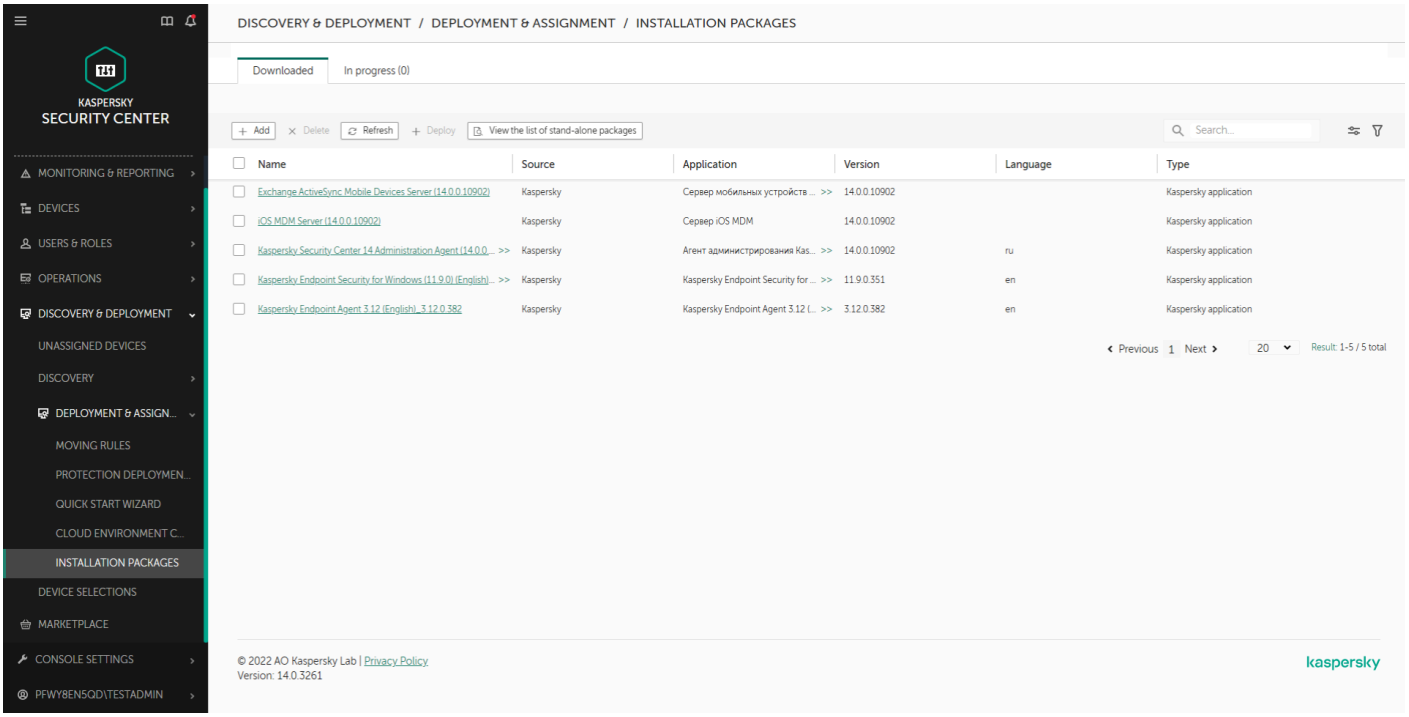
Come creare un pacchetto di installazione in Web Console

1. Nella finestra principale di Web Console, fare clic su **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

   Si aprirà un elenco di pacchetti di installazione che sono stati scaricati in Kaspersky Security Center.

2. Fare clic su **Aggiungi**.

Viene avviata la Creazione guidata nuovo pacchetto. Attenersi alle istruzioni della procedura guidata.



Elenco dei pacchetti di installazione

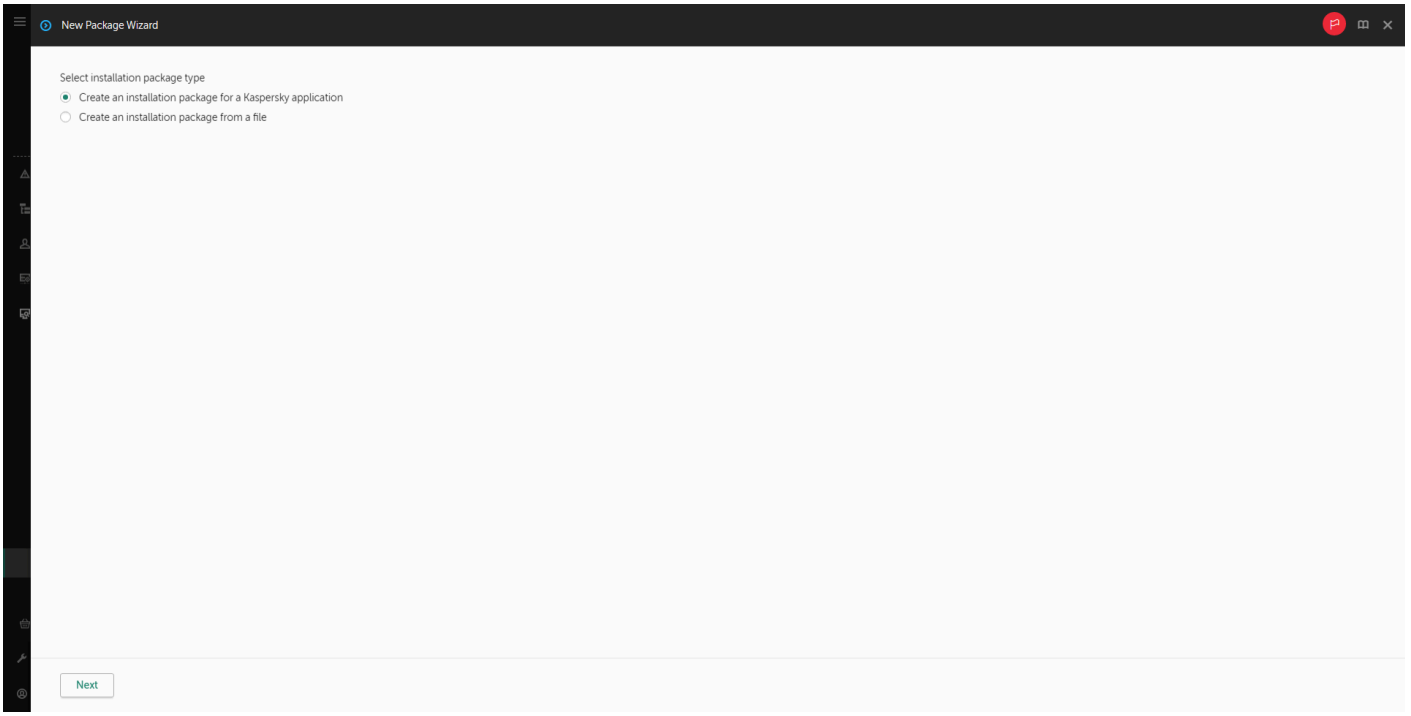
Passaggio 1. Selezione del tipo di pacchetto di installazione

Selezionare l'opzione **Crea pacchetto di installazione per un'applicazione Kaspersky**.

La procedura guidata creerà un pacchetto di installazione dal pacchetto di distribuzione presente nei server Kaspersky. L'elenco viene aggiornato automaticamente quando vengono rilasciate nuove versioni delle applicazioni. È consigliabile selezionare questa opzione per l'installazione di Kaspersky Endpoint Security.

È inoltre possibile creare un pacchetto di installazione da un file.

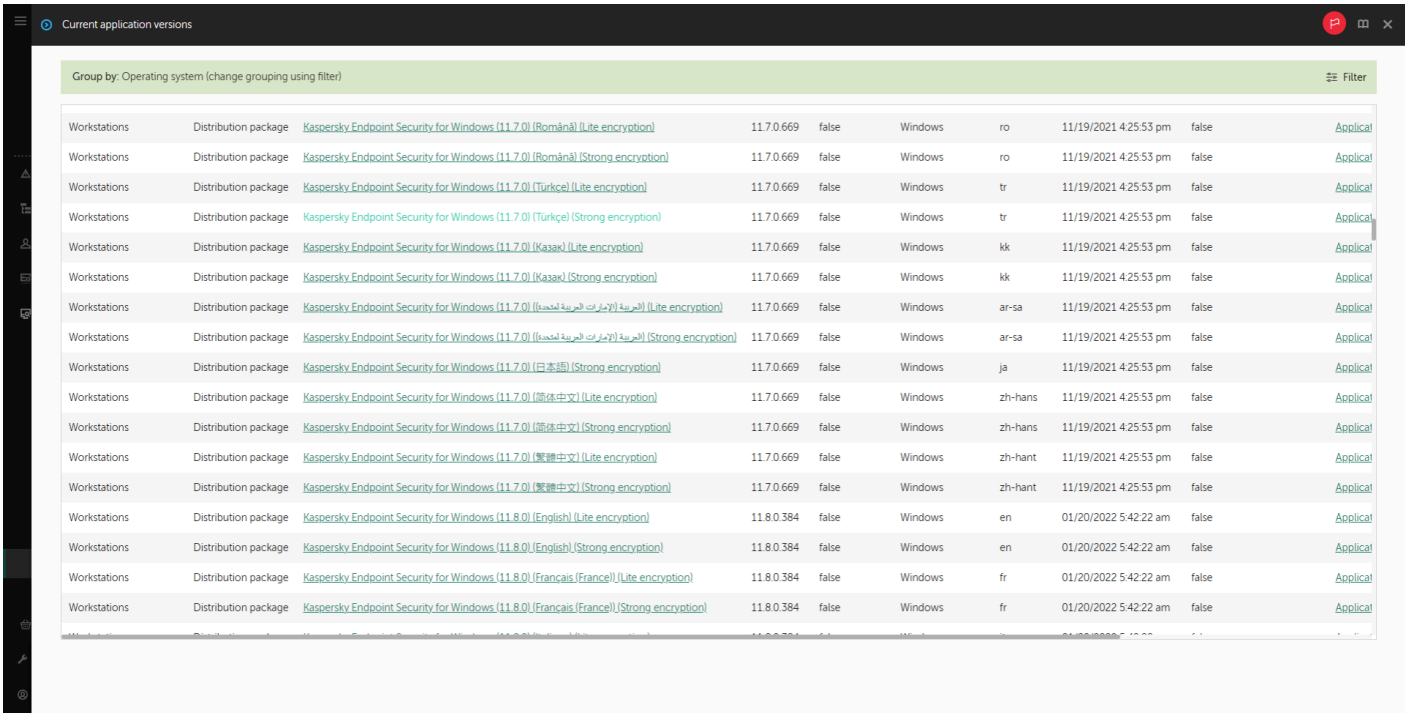
La creazione di un pacchetto di installazione per Kaspersky Endpoint Security da un file è disponibile solo in Kaspersky Security Center Web Console.



Tipi di pacchetti di installazione

Passaggio 2. Pacchetti di installazione

Selezionare il pacchetto di installazione di Kaspersky Endpoint Security for Windows. Verrà avviato il processo di creazione del pacchetto di installazione. Durante la creazione del pacchetto di installazione, è necessario accettare i termini del Contratto di licenza con l'utente finale e dell'Informativa sulla privacy.

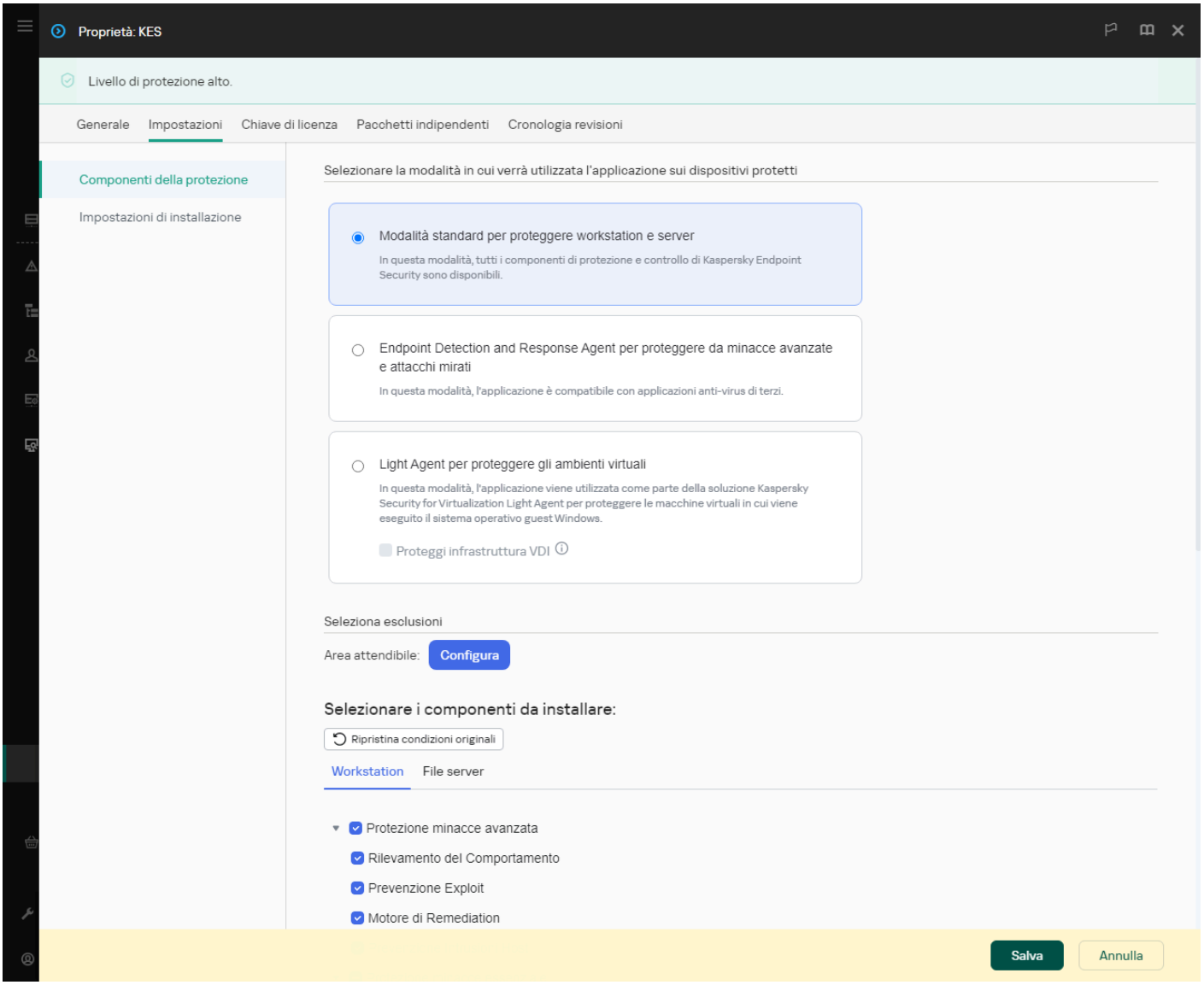


Elenco dei pacchetti di installazione nei server di Kaspersky

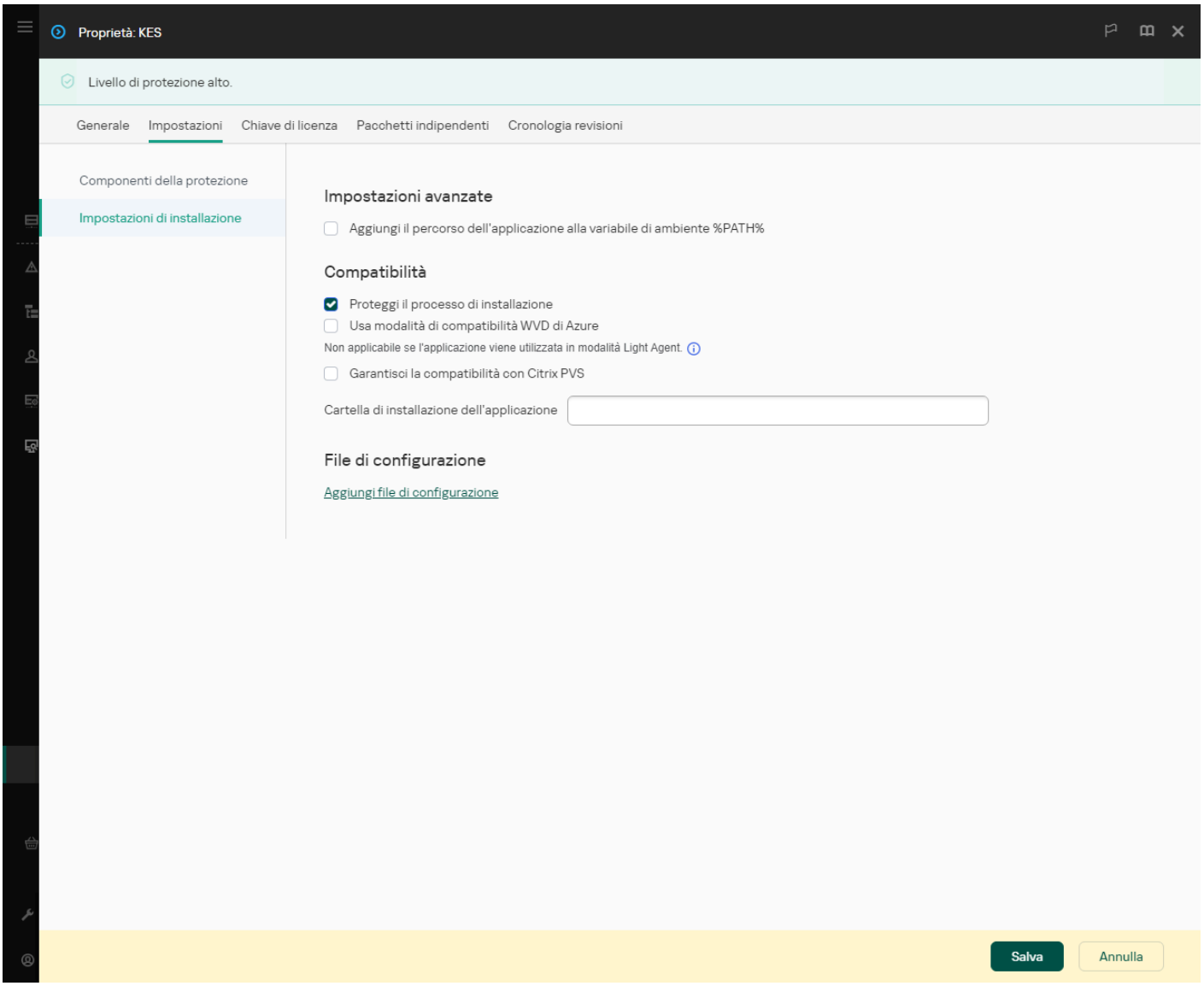
Il pacchetto di installazione verrà creato e aggiunto a Kaspersky Security Center. Utilizzando il pacchetto di installazione, è possibile installare Kaspersky Endpoint Security nei computer della rete aziendale o aggiornare la versione dell'applicazione.

Nelle impostazioni del pacchetto di installazione, è possibile selezionare i componenti dell'applicazione per i diversi tipi di sistemi operativi. Ovvero, il pacchetto di installazione include due set di componenti: per le workstation e per i server. Prima di distribuire il pacchetto di installazione, il programma di installazione rileva il tipo di sistema operativo e installa solo i componenti dell'applicazione selezionati per il tipo di sistema operativo. In questo modo, è possibile utilizzare lo stesso pacchetto di installazione per le workstation e i server.

Il pacchetto di installazione contiene database anti-virus dell'archivio di Administration Server. È possibile aggiornare i database nel pacchetto di installazione per ridurre il consumo di traffico durante l'aggiornamento dei database dopo l'installazione di Kaspersky Endpoint Security.



Componenti inclusi nel pacchetto di installazione



Impostazioni di installazione del pacchetto di installazione

Impostazioni del pacchetto di installazione

Sezione	Descrizione
Componenti della protezione	**Modalità standard**. La configurazione predefinita. Questa configurazione consente di utilizzare tutti i componenti dell'applicazione, inclusi i componenti che forniscono supporto per le soluzioni Detection and Response. Questa configurazione viene utilizzata per una protezione completa del computer da una serie di minacce, attacchi di rete e frodi. **Endpoint Detection and Response Agent**. In questa configurazione, è possibile installare solo i componenti che forniscono supporto per le soluzioni Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), così come KUMA. Questa configurazione è necessaria se nell'organizzazione viene distribuita una Endpoint Protection Platform (EPP) di terzi insieme a una soluzione Kaspersky Detection and Response. Ciò rende Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent compatibile con le applicazioni EPP di terzi. **Light Agent per proteggere gli ambienti virtuali**. Questa configurazione è destinata all'applicazione utilizzata come parte della soluzione Kaspersky Security for Virtualization Light Agent. Light Agent deve essere installato in ogni macchina virtuale da proteggere tramite la soluzione. In questa configurazione, non è possibile utilizzare i componenti di Criptaggio dati o Controllo adattivo delle anomalie. Se si installa Light Agent in un modello di macchina virtuale che verrà utilizzato per creare *macchine virtuali non persistenti*, selezionare la casella di controllo **Proteggi infrastruttura VDI** (VDI è l'acronimo di Virtual Desktop Infrastructure). La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. In questa modalità, Light Agent rifiuta gli aggiornamenti delle applicazioni che richiedono il riavvio della macchina virtuale. Quando si riceve gli aggiornamenti delle applicazioni che richiedono il riavvio, Light Agent genera un evento sulla necessità di aggiornare il modello delle macchine virtuali protette.
Esclusioni	A partire da Kaspersky Endpoint Security 12.6 for Windows, le esclusioni dalle scansioni e le applicazioni attendibili vengono aggiunte all'area attendibile. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server. A partire da Kaspersky Endpoint Security 12.8 for Windows, è possibile installare l'applicazione in modalità Light Agent per proteggere gli ambienti virtuali. Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono contribuire a configurare rapidamente Kaspersky Endpoint Security negli ambienti virtuali Citrix e VMware. È anche possibile configurare l'area attendibile in un secondo momento nelle proprietà del criterio: esclusioni dalle scansioni e applicazioni attendibili.

Sezione	Descrizione
Selezionare i componenti da installare	In questa sezione è possibile selezionare i componenti dell'applicazione che saranno disponibili. È possibile modificare il set di componenti dell'applicazione in un secondo momento utilizzando l'attività *Modifica i componenti dell'applicazione*. È possibile creare insiemi distinti di componenti per la workstation e i server. Prima di distribuire il pacchetto di installazione, il programma di installazione rileva il tipo di sistema operativo e installa solo i componenti dell'applicazione selezionati per il tipo di sistema operativo. In questo modo, è possibile utilizzare lo stesso pacchetto di installazione per le workstation e i server. L'insieme dei componenti disponibili dipende dalla configurazione dell'applicazione: **Modalità standard** Kaspersky Data Encryption, Criptaggio a livello di file e tutti gli agenti integrati, ad eccezione di EDR Optimum, non vengono installati per impostazione predefinita. Questi componenti possono essere aggiunti nelle impostazioni del pacchetto di installazione. **Endpoint Detection and Response Agent** In questa configurazione, sono disponibili solo gli agenti integrati per le soluzioni Kaspersky Detection and Response. **Light Agent per proteggere gli ambienti virtuali** In questa configurazione, è possibile utilizzare quasi tutti i componenti dell'applicazione disponibili nella configurazione **Modalità standard**, ad eccezione dei componenti di criptaggio dei dati e Controllo adattivo delle anomalie.
Chiave di licenza	In questa sezione, è possibile attivare l'applicazione. Per attivare l'applicazione, è necessario selezionare una chiave di licenza. Prima di eseguire questa operazione, è necessario aggiungere la chiave ad Administration Server. Per informazioni dettagliate sull'aggiunta di chiavi a Kaspersky Security Center Administration Server, consultare la Guida di Kaspersky Security Center.
Applicazioni incompatibili	Leggere attentamente l'elenco delle applicazioni incompatibili e consentire la rimozione di queste applicazioni. Se nel computer sono installate applicazioni incompatibili, l'installazione di Kaspersky Endpoint Security termina con un errore.
Impostazioni di installazione	**Aggiungi il percorso del file avp.com alla variabile di sistema %PATH%**. È possibile aggiungere il percorso di installazione alla variabile %PATH% per agevolare l'utilizzo dell'interfaccia della riga di comando. **Proteggi il processo di installazione**. La protezione dell'installazione include la protezione dalla sostituzione del pacchetto di distribuzione con applicazioni dannose, bloccando l'accesso alla cartella di installazione di Kaspersky Endpoint Security e bloccando l'accesso alla sezione del Registro di sistema che contiene le chiavi dell'applicazione. Se tuttavia è impossibile installare l'applicazione (ad esempio, durante l'esecuzione dell'installazione remota tramite Windows Remote Desktop), è possibile disabilitare la protezione del processo di installazione. **Garantisci la compatibilità con Citrix PVS**. È possibile abilitare il supporto di Citrix Provisioning Services per installare Kaspersky Endpoint Security in una macchina virtuale. **Usa modalità di compatibilità WVD di Azure**. Questa funzionalità garantisce la corretta visualizzazione dello stato della macchina virtuale di Azure nella console Kaspersky Anti Targeted Attack Platform. Per monitorare le prestazioni del computer, Kaspersky Endpoint Security invia dati di telemetria ai server KATA. La telemetria include un ID del computer (Sensor ID). La modalità di compatibilità Azure WVD consente di assegnare un Sensor ID univoco permanente a queste macchine virtuali. Se la modalità di compatibilità è disattivata, l'Sensor ID può cambiare dopo il riavvio del computer a causa del funzionamento delle macchine virtuali di Azure. Ciò può causare la visualizzazione di duplicati di macchine virtuali sulla console. **Cartella di installazione dell'applicazione**. È possibile modificare il percorso di installazione di Kaspersky Endpoint Security in un computer client. Per impostazione predefinita, l'applicazione viene installata nella cartella `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`. **File di configurazione**. Installazione dell'applicazione con le impostazioni predefinite. A tale scopo, è necessario caricare un file che definisca le impostazioni di Kaspersky Endpoint Security. È possibile creare un file di configurazione nell'interfaccia locale dell'applicazione. La procedura guidata Nuovo pacchetto non supporta i file di configurazione criptati. Quando si esporta il file di configurazione, omettere il passaggio relativo al criptaggio del file.

Aggiornamento dei database nel pacchetto di installazione

Il pacchetto di installazione contiene i database anti-virus dell'archivio di Administration Server aggiornati al momento della creazione del pacchetto di installazione. Dopo aver creato il pacchetto di installazione, è possibile aggiornare i database anti-virus nel pacchetto di installazione. Questo consente di ridurre il consumo di traffico durante l'aggiornamento dei database anti-virus dopo l'installazione di Kaspersky Endpoint Security.

Per aggiornare i database anti-virus nell'archivio di Administration Server, utilizzare l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* di Administration Server. Per ulteriori informazioni sull'aggiornamento dei database anti-virus nell'archivio di Administration Server, consultare la Guida di Kaspersky Security Center.

È possibile aggiornare i database nel pacchetto di installazione solo in Administration Console e Kaspersky Security Center Web Console. Non è possibile aggiornare i database nel pacchetto di installazione in Kaspersky Security Center Cloud Console.

Come aggiornare i database anti-virus nel pacchetto di installazione tramite Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare la cartella **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.

   Si aprirà un elenco di pacchetti di installazione che sono stati scaricati in Kaspersky Security Center.
3. Aprire le proprietà del pacchetto di installazione.
4. Nella sezione **Generali**, fare clic su **Aggiorna database**.

Successivamente, i database anti-virus nel pacchetto di installazione verranno aggiornati dall'archivio di Administration Server. Il file `bases.cab` incluso nel kit di distribuzione verrà sostituito dalla cartella `bases`. I file del pacchetto di aggiornamento saranno all'interno della cartella.

Come aggiornare i database anti-virus in un pacchetto di installazione tramite Web Console

1. Nella finestra principale di Web Console, fare clic su **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione scaricati in Web Console.
2. Fare clic sul nome del pacchetto di installazione di Kaspersky Endpoint Security in cui si desidera aggiornare i database anti-virus.

   Verrà visualizzata la finestra delle proprietà del pacchetto di installazione.
3. Nella scheda **Informazioni generali** fare clic sul collegamento **Aggiorna database**.

Successivamente, i database anti-virus nel pacchetto di installazione verranno aggiornati dall'archivio di Administration Server. Il file `bases.cab` incluso nel kit di distribuzione verrà sostituito dalla cartella `bases`. I file del pacchetto di aggiornamento saranno all'interno della cartella.

Creazione di un'attività di installazione remota

L'attività *Installa l'applicazione in remoto* è progettata per l'installazione remota di Kaspersky Endpoint Security. L'attività *Installa l'applicazione in remoto* consente di distribuire il pacchetto di installazione dell'applicazione in tutti i computer dell'organizzazione. Prima di distribuire il pacchetto di installazione, è possibile aggiornare i database anti-virus all'interno del pacchetto e selezionare i componenti dell'applicazione disponibili nelle proprietà del pacchetto di installazione.

Come creare un'attività di installazione remota in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.
3. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Security Center Administration Server → Installa l'applicazione in remoto**.

Passaggio 2. Selezione di un pacchetto di installazione

Selezionare il pacchetto di installazione di Kaspersky Endpoint Security dall'elenco. Se l'elenco non contiene il pacchetto di installazione per Kaspersky Endpoint Security, è possibile creare il pacchetto nella procedura guidata.

È possibile configurare le impostazioni del pacchetto di installazione in Kaspersky Security Center. È ad esempio possibile selezionare i componenti dell'applicazione che verranno installati in un computer.

Network Agent verrà inoltre installato insieme a Kaspersky Endpoint Security. *Network Agent* semplifica l'interazione tra Administration Server e un computer client. Se Network Agent è già installato nel computer, non viene installato nuovamente.

Passaggio 3. Avanzate

Selezionare il pacchetto di installazione di Network Agent. La versione selezionata di Network Agent verrà installata insieme a Kaspersky Endpoint Security.

Passaggio 4. Impostazioni

Configurare le seguenti impostazioni aggiuntive dell'applicazione:

- **Forza il download del pacchetto di installazione**. Selezionare il metodo di installazione dell'applicazione:
  - **Utilizzando Network Agent**. Network Agent è responsabile della distribuzione del pacchetto di installazione di Kaspersky Endpoint Security ai computer client. Se Network Agent non è installato, l'attività verrà terminata con un errore. In questo caso, aggiungere il pacchetto di installazione di Network Agent all'attività *Installa l'applicazione in remoto* e abilitare l'invio dei file tramite le risorse del sistema operativo. Successivamente, Network Agent verrà installato utilizzando le risorse del sistema operativo. Kaspersky Endpoint Security verrà quindi installato dagli strumenti di Network Agent.
  - **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**. Il pacchetto di installazione viene distribuito ai computer client utilizzando le risorse del sistema operativo tramite punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete. Per informazioni dettagliate sui punti di distribuzione, consultare la Guida di Kaspersky Security Center.
  - **Utilizzando le risorse del sistema operativo tramite Administration Server**. I file verranno inviati ai computer client utilizzando le risorse del sistema operativo tramite Administration Server. È possibile selezionare questa opzione se nel computer client non è installato alcun Network Agent, ma il computer client si trova nella stessa rete di Administration Server.

- **Comportamento per i dispositivi gestiti tramite altri Administration Server**. Selezionare il metodo di installazione per Kaspersky Endpoint Security. Se nella rete è installato più di un Administration Server, questi Administration Server possono visualizzare gli stessi computer client. Ciò può ad esempio causare l'installazione in remoto di un'applicazione nello stesso computer client più volte tramite diversi Administration Server o altri conflitti.

- **Non reinstallare l'applicazione se è già installata**. Se ad esempio si desidera installare una versione precedente dell'applicazione, deselezionare la casella di controllo.

Passaggio 5. Selezione dell'impostazione di riavvio del sistema operativo

Selezionare l'azione che deve essere eseguita se è richiesto il riavvio del computer. Il riavvio non è richiesto durante l'installazione di Kaspersky Endpoint Security. Il riavvio è richiesto solo se è necessario rimuovere applicazioni incompatibili prima dell'installazione. Potrebbe essere necessario il riavvio anche durante l'aggiornamento della versione dell'applicazione.

Passaggio 6. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer per l'installazione di Kaspersky Endpoint Security. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.

- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. Network Agent non viene installato nei dispositivi non assegnati. In questo caso l'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 7. Selezione dell'account per eseguire l'attività

Selezionare l'account per l'installazione di Network Agent utilizzando gli strumenti del sistema operativo. In questo caso sono richiesti i diritti di amministratore per l'accesso al computer. È possibile aggiungere più account. Se un account non dispone dei diritti sufficienti, l'Installazione guidata utilizza l'account successivo. Se si installa Kaspersky Endpoint Security utilizzando gli strumenti di Network Agent, non è necessario selezionare un account.

Passaggio 8. Configurazione di una pianificazione di avvio dell'attività

Configurare una pianificazione per l'avvio di un'attività, ad esempio manualmente o quando il computer è inattivo.

Passaggio 9. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Installa Kaspersky Endpoint Security for Windows 14.2*.

Passaggio 10. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività. L'applicazione verrà installata in modalità automatica. Dopo l'installazione, l'icona verrà aggiunta all'area di notifica del computer dell'utente. Se l'icona si presenta in questo modo , assicurarsi di avere attivato l'applicazione.

Come creare un'attività di installazione remota in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Configurazione delle impostazioni generali dell'attività

Configurare le impostazioni generali dell'attività:

1. Nell'elenco a discesa **Applicazione** selezionare **Kaspersky Security Center**.
2. Nell'elenco a discesa **Tipo di attività**, selezionare **Installa l'applicazione in remoto**.
3. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Installazione di Kaspersky Endpoint Security for Managers*.
4. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

Passaggio 2. Selezione dei computer per l'installazione

In questo passaggio selezionare i computer in cui Kaspersky Endpoint Security verrà installato in base all'opzione dell'ambito dell'attività selezionata.

Passaggio 3. Configurazione di un pacchetto di installazione

In questo passaggio, configurare il pacchetto di installazione:

1. Selezionare il pacchetto di installazione di Kaspersky Endpoint Security for Windows (14.2).

2. Selezionare il pacchetto di installazione di Network Agent.

   La versione selezionata di Network Agent verrà installata insieme a Kaspersky Endpoint Security. *Network Agent* semplifica l'interazione tra Administration Server e un computer client. Se Network Agent è già installato nel computer, non viene installato nuovamente.

3. Nel blocco **Forza il download del pacchetto di installazione**, selezionare il metodo di installazione dell'applicazione:

   - **Utilizzando Network Agent**. Network Agent è responsabile della distribuzione del pacchetto di installazione di Kaspersky Endpoint Security ai computer client. Se Network Agent non è installato, l'attività verrà terminata con un errore. In questo caso, aggiungere il pacchetto di installazione di Network Agent all'attività *Installa l'applicazione in remoto* e abilitare l'invio dei file tramite le risorse del sistema operativo. Successivamente, Network Agent verrà installato utilizzando le risorse del sistema operativo. Kaspersky Endpoint Security verrà quindi installato dagli strumenti di Network Agent.

   - **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**. Il pacchetto di installazione viene distribuito ai computer client utilizzando le risorse del sistema operativo tramite punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete. Per informazioni dettagliate sui punti di distribuzione, consultare la Guida di Kaspersky Security Center.

   - **Utilizzando le risorse del sistema operativo tramite Administration Server**. I file verranno inviati ai computer client utilizzando le risorse del sistema operativo tramite Administration Server. È possibile selezionare questa opzione se nel computer client non è installato alcun Network Agent, ma il computer client si trova nella stessa rete di Administration Server.

4. Nel campo **Numero massimo di download simultanei**, impostare un limite relativo al numero di richieste di download del pacchetto di installazione inviate ad Administration Server. Il limite relativo al numero di richieste consentirà di evitare un sovraccarico della rete.

5. Nel campo **Numero massimo di tentativi di installazione**, impostare un limite relativo al numero di tentativi di installazione dell'applicazione. Se l'installazione di Kaspersky Endpoint Security termina con un errore, l'attività avvierà automaticamente la nuova installazione.

6. Se necessario, deselezionare la casella di controllo **Non reinstallare l'applicazione se è già installata**. Consente ad esempio di installare una delle versioni precedenti dell'applicazione.

7. Se necessario, deselezionare la casella di controllo **Verifica il tipo di sistema operativo prima del download**. Questo consente di evitare di scaricare il pacchetto di distribuzione di un'applicazione se il sistema operativo del computer non soddisfa i requisiti software. Se si è certi che il sistema operativo del computer soddisfi i requisiti software, è possibile ignorare la verifica.

8. Se necessario, selezionare la casella di controllo **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory**. Kaspersky Endpoint Security viene installato tramite Network Agent oppure manualmente tramite Active Directory. Per installare Network Agent, l'attività di installazione remota deve essere eseguita con i privilegi dell'amministratore di dominio.

9. Se necessario, selezionare la casella di controllo **Chiedi agli utenti di chiudere le applicazioni in esecuzione**. L'installazione di Kaspersky Endpoint Security richiede l'impiego di risorse del computer. Per comodità dell'utente l'installazione guidata dell'applicazione richiede di chiudere le applicazioni in esecuzione prima di avviare l'installazione. Questo consente di evitare le interruzioni durante l'esecuzione di altre applicazioni e impedisce possibili malfunzionamenti del computer.

10. Nel blocco **Comportamento per i dispositivi gestiti tramite altri Administration Server**, selezionare il metodo di installazione di Kaspersky Endpoint Security. Se nella rete è installato più di un Administration Server, questi Administration Server possono visualizzare gli stessi computer client. Ciò può ad esempio causare l'installazione in remoto di un'applicazione nello stesso computer client più volte tramite diversi Administration Server o altri conflitti.

Passaggio 4. Selezione dell'account per eseguire l'attività

Selezionare l'account per l'installazione di Network Agent utilizzando gli strumenti del sistema operativo. In questo caso sono richiesti i diritti di amministratore per l'accesso al computer. È possibile aggiungere più account. Se un account non dispone dei diritti sufficienti, l'Installazione guidata utilizza l'account successivo. Se si installa Kaspersky Endpoint Security utilizzando gli strumenti di Network Agent, non è necessario selezionare un account.

Passaggio 5. Completamento della creazione dell'attività

Terminare la procedura guidata facendo clic sul pulsante **Fine**. Verrà visualizzata una nuova attività nell'elenco delle attività. Per eseguire un'attività, selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**. L'applicazione verrà installata in modalità automatica. Dopo l'installazione, l'icona verrà aggiunta all'area di notifica del computer dell'utente. Se l'icona si presenta in questo modo , assicurarsi di avere attivato l'applicazione.

Installazione dell'applicazione in locale tramite la procedura guidata

L'interfaccia dell'Installazione guidata dell'applicazione è composta da una sequenza di finestre corrispondenti ai passaggi di installazione dell'applicazione. Verificare che l'account utente con cui si esegue l'Installazione guidata appartenga al gruppo di amministratori.

Per installare l'applicazione o aggiornarla da una versione precedente utilizzando l'Installazione guidata:

1. Copiare la cartella del kit di distribuzione nel computer dell'utente.

2. Eseguire setup_kes.exe.

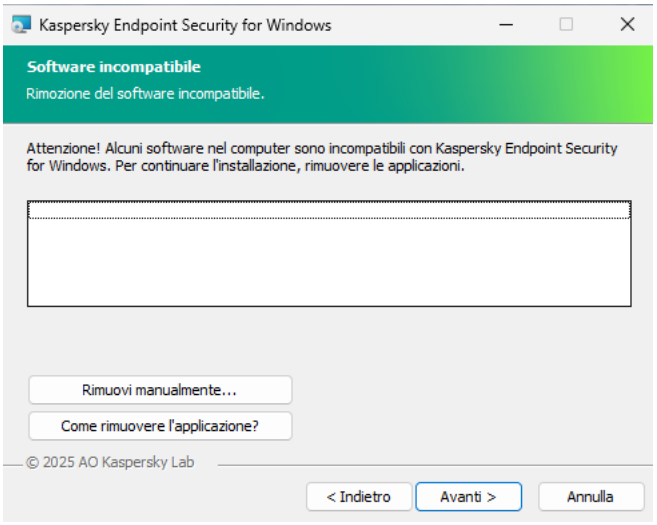
   Verrà avviata l'Installazione guidata.

Preparazione per l'installazione

Prima di installare Kaspersky Endpoint Security in un computer o di eseguire l'upgrade da una versione precedente, vengono verificate le seguenti condizioni:

- Se è installato software che potrebbe presentare problemi di compatibilità con Kaspersky Endpoint Security. (l'elenco del software è disponibile nel file incompatible.txt incluso nel kit di distribuzione).
- Se i requisiti hardware e software sono soddisfatti o meno.
- Se Microsoft .NET Framework è presente.
- Se l'utente dispone o meno dei diritti per l'installazione prodotto software.

Se uno dei precedenti requisiti non è soddisfatto, viene visualizzata una notifica sullo schermo. Ad esempio, una notifica sul software incompatibile (vedere la figura riportata di seguito).



Rimozione del software incompatibile

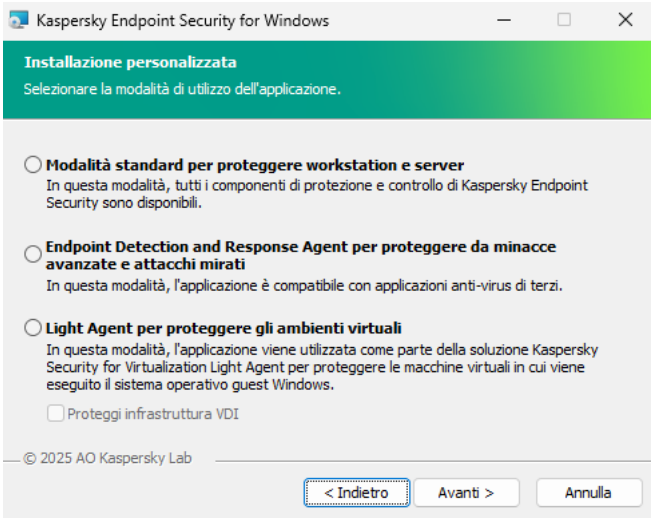
Se il computer soddisfa i requisiti elencati, l'Installazione guidata esegue una ricerca delle applicazioni Kaspersky che potrebbero generare conflitti se eseguite in combinazione con l'applicazione da installare. Se vengono rilevate applicazioni di questo tipo, viene richiesto di rimuoverle manualmente.

Se le applicazioni rilevate includono le versioni precedenti di Kaspersky Endpoint Security, tutti i dati di cui può essere eseguita la migrazione (ad esempio dati di attivazione e impostazioni dell'applicazione) vengono mantenuti e utilizzati durante l'installazione di Kaspersky Endpoint Security 14.2 for Windows e la versione precedente dell'applicazione viene rimossa automaticamente. Questo si applica alle seguenti versioni dell'applicazione:

- Kaspersky Endpoint Security 12.3 for Windows (build 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (build 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (build 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (build 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (build 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (build 12.8.0.505)

- Kaspersky Endpoint Security 12.9 for Windows (build 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (build 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (build 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (build 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (build 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (build 14.1.0.423)

Configurazione di Kaspersky Endpoint Security



Scelta della configurazione dell'applicazione

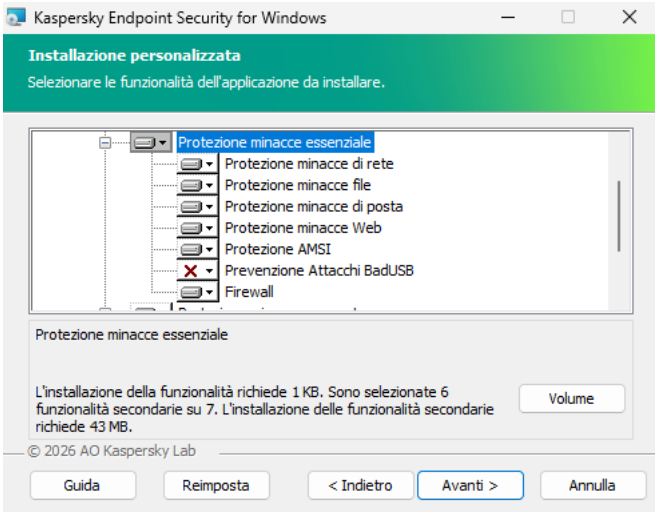
Modalità standard. La configurazione predefinita. Questa configurazione consente di utilizzare tutti i componenti dell'applicazione, inclusi i componenti che forniscono supporto per le soluzioni Detection and Response. Questa configurazione viene utilizzata per una protezione completa del computer da una serie di minacce, attacchi di rete e frodi.

Endpoint Detection and Response Agent. In questa configurazione, è possibile installare solo i componenti che forniscono supporto per le soluzioni Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), così come KUMA. Questa configurazione è necessaria se nell'organizzazione viene distribuita una Endpoint Protection Platform (EPP) di terzi insieme a una soluzione Kaspersky Detection and Response. Ciò rende Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent compatibile con le applicazioni EPP di terzi.

Light Agent per proteggere gli ambienti virtuali. Questa configurazione è destinata all'applicazione utilizzata come parte della soluzione Kaspersky Security for Virtualization Light Agent. Light Agent deve essere installato in ogni macchina virtuale da proteggere tramite la soluzione. In questa configurazione, non è possibile utilizzare i componenti di Criptaggio dati o Controllo adattivo delle anomalie. Se si installa Light Agent in un modello di macchina virtuale che verrà utilizzato per creare *macchine virtuali non persistenti*, selezionare la casella di controllo **Proteggi infrastruttura VDI** (VDI è l'acronimo di Virtual Desktop Infrastructure). La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. In questa modalità, Light Agent rifiuta gli aggiornamenti delle applicazioni che richiedono il riavvio della macchina virtuale. Quando si riceve gli aggiornamenti delle applicazioni che richiedono il riavvio, Light Agent genera un evento sulla necessità di aggiornare il modello delle macchine virtuali protette.

Componenti di Kaspersky Endpoint Security

Durante il processo di installazione, è possibile selezionare i componenti di Kaspersky Endpoint Security da installare (vedere la figura seguente). Il componente Protezione minacce file è un componente obbligatorio da installare. Non è possibile annullarne l'installazione.



Selezione dei componenti dell'applicazione da installare

Per impostazione predefinita, vengono selezionati per l'installazione tutti i componenti dell'applicazione, tranne i seguenti componenti:

- Criptaggio disco Kaspersky
- Criptaggio a livello di file
- Endpoint Detection and Response Expert (on-premises)
- Endpoint Detection and Response Expert (cloud)
- Sandbox
- Managed Detection and Response
- Network Detection and Response (KATA)
- Integrazione con KUMA

È possibile modificare i componenti dell'applicazione disponibili dopo l'installazione dell'applicazione. A tale scopo, è necessario eseguire nuovamente l'Installazione guidata e scegliere di modificare i componenti disponibili.

Se è necessario installare i componenti di Detection and Response, Kaspersky Endpoint Security supporta le seguenti configurazioni:

- Solo Endpoint Detection and Response Optimum
- Solo Endpoint Detection and Response Expert (cloud)
- Solo Endpoint Detection and Response Expert (on-premises)

- Solo Network Detection and Response (KATA)
- Solo Sandbox
- Endpoint Detection and Response Optimum e Sandbox
- Endpoint Detection and Response Expert (cloud) e Sandbox
- Endpoint Detection and Response Expert (on-premises) e Sandbox
- Network Detection and Response (KATA) e Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) e Managed Detection and Response

Kaspersky Endpoint Security verifica la selezione dei componenti prima di installare l'applicazione. Se la configurazione selezionata dei componenti di Detection and Response non è supportata, non è possibile installare Kaspersky Endpoint Security.

Selezione della cartella in cui installare l'applicazione

È possibile modificare il percorso di installazione di Kaspersky Endpoint Security in un computer client. Per impostazione predefinita, l'applicazione viene installata nella cartella `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`.

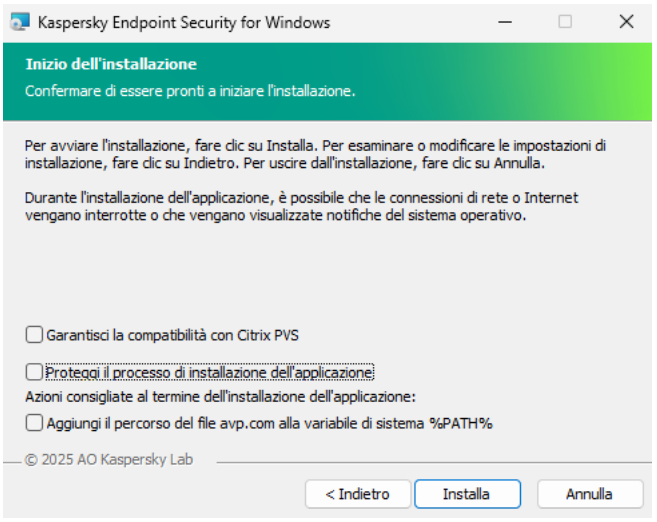
Configurazione dell'area attendibile

A partire da Kaspersky Endpoint Security 12.6 for Windows, le esclusioni dalle scansioni e le applicazioni attendibili vengono aggiunte all'area attendibile. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server.

A partire da Kaspersky Endpoint Security 12.8 for Windows, è possibile installare l'applicazione in modalità Light Agent per proteggere gli ambienti virtuali. Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono contribuire a configurare rapidamente Kaspersky Endpoint Security negli ambienti virtuali Citrix e VMware.

È anche possibile configurare l'area attendibile in un secondo momento nelle proprietà del criterio: esclusioni dalle scansioni e applicazioni attendibili.

Impostazioni avanzate



Impostazioni avanzate di installazione dell'applicazione

Proteggi il processo di installazione dell'applicazione. La protezione dell'installazione include la protezione dalla sostituzione del pacchetto di distribuzione con applicazioni dannose, bloccando l'accesso alla cartella di installazione di Kaspersky Endpoint Security e bloccando l'accesso alla sezione del Registro di sistema che contiene le chiavi dell'applicazione. Se tuttavia è impossibile installare l'applicazione (ad esempio, durante l'esecuzione dell'installazione remota tramite Windows Remote Desktop), è possibile disabilitare la protezione del processo di installazione.

Garantisci la compatibilità con Citrix PVS. È possibile abilitare il supporto di Citrix Provisioning Services per installare Kaspersky Endpoint Security in una macchina virtuale.

Aggiungi il percorso del file avp.com alla variabile di sistema %PATH%. È possibile aggiungere il percorso di installazione alla variabile %PATH% per agevolare l'utilizzo dell'interfaccia della riga di comando.

Installazione remota dell'applicazione tramite System Center Configuration Manager

Queste istruzioni si applicano a System Center Configuration Manager 2012 R2.

Per installare in remoto un'applicazione tramite System Center Configuration Manager:

1. Aprire la console di Configuration Manager.
2. Nella parte destra della console, nel blocco **Gestione applicazioni**, selezionare **Pacchetti**.
3. Nella parte superiore della console, nel pannello di controllo, fare clic sul pulsante **Crea pacchetto**.

   Verrà avviata la *Creazione guidata pacchetto e programma*.

4. Nella Creazione guidata pacchetto e programma:

   a. Nella sezione **Pacchetto**:

   - Nel campo **Nome** immettere il nome del pacchetto di installazione.
   - Nel campo **Cartella di origine** specificare il percorso della cartella che contiene il pacchetto di distribuzione di Kaspersky Endpoint Security.

   b. Nella sezione **Tipo di applicazione**, selezionare l'opzione **Programma standard**.

   c. Nella sezione **Programma standard**:

   - Nel campo **Nome** immettere il nome univoco per il pacchetto di installazione (ad esempio, il nome dell'applicazione e la versione).
   - Nel campo **Riga di comando** specificare le opzioni di installazione di Kaspersky Endpoint Security dalla riga di comando.
   - Fare clic sul pulsante **Sfoglia** per specificare il percorso del file eseguibile dell'applicazione.
   - Verificare che per l'elenco **Modalità di esecuzione** sia selezionato l'elemento **Esegui con diritti amministrativi**.

   d. Nella sezione **Requisiti**:

   - Selezionare la casella di controllo **Avvia prima un altro programma** se si desidera che venga avviata un'altra applicazione prima di installare Kaspersky Endpoint Security.

     Selezionare l'applicazione dall'elenco a discesa **Applicazione** o specificare il percorso del file eseguibile dell'applicazione facendo clic sul pulsante **Sfoglia**.

   - Selezionare l'opzione **Solo sulle piattaforme specificate** nel blocco **Requisiti di piattaforma** se si desidera che l'applicazione venga installata solo nei sistemi operativi specificati.

     Nell'elenco sottostante selezionare le caselle di controllo accanto ai sistemi operativi in cui installare Kaspersky Endpoint Security.

   Questo passaggio è facoltativo.

   e. Nella sezione **Sommario** verificare tutti i valori delle impostazioni immessi e fare clic su **Avanti**.

   Il pacchetto di installazione creato sarà visualizzato nella sezione **Pacchetti** nell'elenco dei pacchetti di installazione disponibili.

5. Dal menu di scelta rapida del pacchetto di installazione selezionare **Distribuisci**.

   Verrà avviata la *Distribuzione guidata*.

6. Nella Distribuzione guidata:

   a. Nella sezione **Generale**:

   - Nel campo **Software** immettere il nome univoco del pacchetto di installazione o selezionare il pacchetto di installazione dall'elenco facendo clic sul pulsante **Sfoglia**.
   - Nel campo **Raccolta** immettere il nome della raccolta di computer in cui installare l'applicazione o selezionare la raccolta facendo clic sul pulsante **Sfoglia**.

b. Nella sezione **Contiene** aggiungere i punti di distribuzione (per informazioni più dettagliate, fare riferimento alla Guida di System Center Configuration Manager).

c. Se necessario, specificare i valori delle altre impostazioni nella Distribuzione guidata. Queste impostazioni sono facoltative per l'installazione remota di Kaspersky Endpoint Security.

d. Nella sezione **Sommario** verificare tutti i valori delle impostazioni immessi e fare clic su **Avanti**.

Al termine della Distribuzione guidata, verrà creata un'attività per l'installazione remota di Kaspersky Endpoint Security.

Descrizione delle impostazioni di installazione del file setup.ini

Il file setup.ini è utilizzato per l'installazione dell'applicazione dalla riga di comando o quando si utilizza l'Editor Criteri di gruppo di Microsoft Windows. Per applicare le impostazioni del file setup.ini, inserire il file nella cartella contenente il pacchetto di distribuzione di Kaspersky Endpoint Security.

Utilizzare il file setup.ini solo quando l'applicazione viene installata in modalità automatica.

Non è possibile aggiungere un percorso al file di configurazione install.cfg nel file setup.ini. L'applicazione ignora anche il file di configurazione install.cfg se è posizionata nella stessa cartella con il kit di distribuzione di Kaspersky Endpoint Security. Per applicare le impostazioni dal file di configurazione install.cfg, è necessario specificare il percorso del file nel seguente comando di installazione dell'applicazione: `CONFIGPATH=<path to the configuration file>`.

SCARICA IL FILE SETUP.INI

Il file setup.ini è composto dalle seguenti sezioni:

- `[Setup]` – impostazioni generali dell'installazione dell'applicazione.
- `[Components]` – selezione dei componenti dell'applicazione da installare nella modalità Standard. Se non viene specificato alcun componente, vengono installati tutti i componenti disponibili per il sistema operativo. Protezione minacce file è un componente obbligatorio ed è installato nel computer indipendentemente dalle impostazioni indicate in questa sezione.
- `[Tasks]` – selezione di attività da includere nell'elenco delle attività di Kaspersky Endpoint Security. Se non viene specificata alcuna attività, vengono incluse tutte le attività nell'elenco di attività di Kaspersky Endpoint Security.

In alternativa al valore `1`, è possibile utilizzare i valori `yes`, `on`, `enable`, `enabled` e `true`. In alternativa al valore `0`, è possibile utilizzare i valori `no`, `off`, `disable`, `disabled` e `false`.

Sezione	Parametro	Descrizione
[Setup]	InstallDir	Percorso della cartella di installazione dell'applicazione.
	ActivationCode	Codice di attivazione di Kaspersky Endpoint Security.
	Eula	Accettazione delle condizioni del Contratto di licenza con l'utente finale. Il testo del Contratto di licenza è incluso nel kit di distribuzione di Kaspersky Endpoint Security. L'accettazione delle condizioni del Contratto di licenza con l'utente finale è necessaria per installare l'applicazione o eseguire l'aggiornamento della versione.
	PrivacyPolicy	Accettazione dell'Informativa sulla privacy. Il testo dell'Informativa sulla privacy è incluso nel kit di distribuzione di Kaspersky Endpoint Security. Per installare l'applicazione o eseguire l'upgrade della versione dell'applicazione, è necessario accettare la Informativa sulla privacy.
	KSN	Accettazione o rifiuto della partecipazione a Kaspersky Security Network (KSN). Se per questo parametro non è impostato alcun valore, Kaspersky Endpoint Security richiederà di confermare il consenso o il rifiuto di partecipare a KSN al primo avvio di Kaspersky Endpoint Security. Valori disponibili: • 1 – accettazione della partecipazione a KSN. • 0 – rifiuto della partecipazione a KSN (valore predefinito). Il pacchetto di distribuzione di Kaspersky Endpoint Security è ottimizzato per l'utilizzo con Kaspersky Security Network. Se si è scelto di non per partecipare a Kaspersky Security Network, è necessario aggiornare Kaspersky Endpoint Security subito dopo il completamento dell'installazione.
	CLEANERSIGNCHECK	Verifica delle firme digitali dei file del software rilevati nell'elenco incompatible.txt. Per rimuovere il software, Kaspersky Endpoint Security esegue il file del programma di installazione del software. Se il file del programma di installazione non dispone di una firma digitale, Kaspersky Endpoint Security considera il file non attendibile e interrompe la rimozione del software per evitare l'esecuzione di codice potenzialmente dannoso. Se l'applicazione non è in grado di verificare la firma digitale del file del software rilevato, l'installazione di Kaspersky Endpoint Security viene interrotta con un errore. Il valore predefinito è diverso a seconda del metodo di installazione del software: • 0 indica che la verifica della firma digitale è disabilitata (valore predefinito se distribuito tramite Kaspersky Security Center). • 1 indica che la verifica della firma digitale è abilitata (valore predefinito se l'applicazione viene installata in locale).
	Login	Impostare il nome utente per l'accesso alle funzionalità e alle impostazioni di Kaspersky Endpoint Security (componente Protezione tramite password). Il nome utente viene impostato insieme alle impostazioni Password e PasswordArea. Per impostazione predefinita, viene utilizzato il nome utente KLAdmin.
	Password	Specificare una password per accedere a funzionalità e impostazioni di Kaspersky Endpoint Security (la password è specificata insieme ai parametri Login e PasswordArea). Se è stata specificata una password, ma non è stato specificato un nome utente con il parametro Login, per impostazione predefinita viene utilizzato il nome utente KLAdmin.

Sezione	Parametro	Descrizione
	`PasswordArea`	Specificare l'ambito della password per accedere a Kaspersky Endpoint Security. Quando un utente tenta di eseguire un'azione inclusa in questo ambito, Kaspersky Endpoint Security richiede le credenziali dell'account utente (parametri `Login` e `Password`). Utilizzare il carattere `;` per specificare più valori. Valori disponibili: • `SET` – modifica delle impostazioni dell'applicazione. • `EXIT` – chiusura dell'applicazione. • `DISPROTECT` – disabilitazione dei componenti della protezione e arresto delle attività di scansione. • `DISPOLICY` – disabilitazione del criterio di Kaspersky Security Center. • `UNINST` – rimozione dell'applicazione dal computer. • `DISCTRL` – disabilitazione dei componenti di controllo. • `REMOVELIC` – rimozione della chiave. • `REPORTS` – visualizzazione dei rapporti. • `EXPORT` – esportazione delle impostazioni dell'applicazione. Ad esempio, `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Abilitazione o disabilitazione del meccanismo di protezione dell'installazione dell'applicazione. Valori disponibili: • `1` – il meccanismo di protezione dell'installazione dell'applicazione è abilitato (valore predefinito). • `0` – il meccanismo di protezione dell'installazione dell'applicazione è disabilitato. La protezione dell'installazione include la protezione dalla sostituzione del pacchetto di distribuzione con applicazioni dannose, bloccando l'accesso alla cartella di installazione di Kaspersky Endpoint Security e bloccando l'accesso alla sezione del Registro di sistema che contiene le chiavi dell'applicazione. Se tuttavia è impossibile installare l'applicazione (ad esempio, durante l'esecuzione dell'installazione remota tramite Windows Remote Desktop), è possibile disabilitare la protezione del processo di installazione.
	`PROTECTOSSERVICES`	Protezione della funzionalità dei servizi del sistema operativo. La protezione dei servizi del sistema operativo impedisce alle applicazioni di terze parti di interferire con il funzionamento dei servizi del sistema operativo. Tali servizi includono, ad esempio, il servizio di avvio automatico delle applicazioni. • `1` significa che la protezione dei servizi del sistema operativo è abilitata (valore predefinito). • `0` significa che la protezione dei servizi del sistema operativo è disabilitata.
	`EnableAzureSupport`	Abilitazione o disabilitazione della modalità di compatibilità di Azure WVD. Valori disponibili: • `1`: la modalità di compatibilità di Azure WVD è abilitata. • `0`: la modalità di compatibilità di Azure WVD è disabilitata (valore predefinito). Questa funzionalità garantisce la corretta visualizzazione dello stato della macchina virtuale di Azure nella console Kaspersky Anti Targeted Attack Platform. Per monitorare le prestazioni del computer, Kaspersky Endpoint Security invia dati di telemetria ai server KATA. La telemetria include un ID del computer (Sensor ID). La modalità di compatibilità Azure WVD consente di assegnare un Sensor ID univoco permanente a queste macchine virtuali. Se la modalità di compatibilità è disattivata, l'Sensor ID può cambiare dopo il riavvio del computer a causa del funzionamento delle macchine virtuali di Azure. Ciò può causare la visualizzazione di duplicati di macchine virtuali sulla console.
	`Reboot`	Riavvio automatico del computer, se necessario dopo l'installazione o l'upgrade dell'applicazione. Se non viene impostato alcun valore per questo parametro, il riavvio automatico del computer viene bloccato. Il riavvio non è richiesto durante l'installazione di Kaspersky Endpoint Security. Il riavvio è richiesto solo se è necessario rimuovere applicazioni incompatibili prima dell'installazione. Potrebbe essere necessario il riavvio anche durante l'aggiornamento della versione dell'applicazione.
	`AddEnvironment`	Nella variabile di sistema %PATH% è possibile aggiungere il percorso dei file eseguibili contenuti nella cartella di installazione di Kaspersky Endpoint Security. Valori disponibili: • `1` – alla variabile di sistema %PATH% viene aggiunto il percorso dei file eseguibili contenuti nella cartella di installazione di Kaspersky Endpoint Security. • `0` – alla variabile di sistema %PATH% non viene aggiunto il percorso dei file eseguibili contenuti nella cartella di installazione di Kaspersky Endpoint Security.

Sezione	Parametro	Descrizione
	AMPPL	Consente di abilitare o disabilitare la protezione dei processi Kaspersky Endpoint Security tramite la tecnologia AM-PPL (Antimalware Protected Process Light). Per ulteriori informazioni sulla tecnologia AM-PPL, visitare il sito Web Microsoft. La tecnologia AM-PPL è disponibile per i sistemi operativi Windows 10 versione 1703 (RS2) o successiva e Windows Server 2019. Valori disponibili: • 1 – la protezione dei processi Kaspersky Endpoint Security tramite la tecnologia AM-PPL è abilitata. • 0 – la protezione dei processi Kaspersky Endpoint Security tramite la tecnologia AM-PPL è disabilitata.
	UPGRADEMODE	Modalità di upgrade dell'applicazione: • Seamless indica l'upgrade dell'applicazione con un riavvio del computer (valore predefinito). • Force indica l'upgrade dell'applicazione senza un riavvio. È possibile eseguire l'upgrade dell'applicazione senza riavvio a partire dalla versione 11.10.0. Per eseguire l'upgrade a una versione precedente dell'applicazione, è necessario riavviare il computer. È inoltre possibile installare le patch senza riavvio a partire dalla versione 11.11.0. Il riavvio non è richiesto durante l'installazione di Kaspersky Endpoint Security. Pertanto, la modalità di upgrade dell'applicazione verrà specificata nelle impostazioni dell'applicazione. È possibile modificare questo parametro nel criterio o nelle impostazioni dell'applicazione. Quando si effettua l'upgrade di un'applicazione già installata, la priorità del parametro specificato nel file setup.ini è superiore a quella del parametro specificato nelle impostazioni dell'applicazione o nella riga di comando. Ad esempio, se la modalità di upgrade Force è specificata nel file setup.ini e la modalità Seamless è specificata nelle impostazioni dell'applicazione, l'upgrade verrà installato senza un riavvio (Force). Se si utilizza il file setup.ini, in cui il parametro UPGRADEMODE non è specificato, il programma di installazione utilizzerà un valore predefinito (Seamless) e installerà l'upgrade al riavvio del computer.
	SetupReg	Consente la scrittura delle chiavi del Registro di sistema del file setup.reg nel Registro di sistema. Valore del parametro SetupReg: setup.reg.
	EnableTraces	Abilitazione o disabilitazione del tracciamento dell'applicazione. Dopo l'avvio, Kaspersky Endpoint Security salva i file di traccia nella cartella %ProgramData%\Kaspersky Lab\KES.14.2\Traces. Valori disponibili: • 1 - il tracciamento è abilitato. • 0 - il tracciamento è disabilitato (valore predefinito).
	TracesLevel	Livello di dettaglio delle tracce. Valori disponibili: • 100 (critico). Solo messaggi sugli errori irreversibili. • 200 (alto). Messaggi su tutti gli errori, inclusi gli errori irreversibili. • 300 (diagnostico). Messaggi su tutti gli errori e avvisi. • 400 (importante). Tutti i messaggi di errore, gli avvisi e le informazioni aggiuntive. • 500 (normale). Messaggi su tutti gli errori e avvisi, nonché informazioni dettagliate sul funzionamento dell'applicazione in modalità normale (impostazione predefinita). • 600 (basso). Tutti i messaggi.
	RESTAPI	Gestione dell'applicazione tramite REST API. Per gestire l'applicazione tramite REST API, è necessario specificare il nome utente (parametro RESTAPI_User). Valori disponibili: • 1 - la gestione tramite REST API è consentita. • 0 – la gestione tramite l'API REST è bloccata (valore predefinito). Per gestire l'applicazione tramite REST API, è necessario consentire la gestione utilizzando sistemi amministrativi. A tale scopo, impostare il parametro AdminKitConnector=1. Se si gestisce l'applicazione tramite REST API, è impossibile gestire l'applicazione utilizzando i sistemi di amministrazione di Kaspersky.
	RESTAPI_User	Nome utente dell'account di dominio Windows utilizzato per la gestione dell'applicazione tramite REST API. La gestione dell'applicazione tramite REST API è disponibile solo per questo utente. Immettere il nome utente nel formato <DOMAIN>\<UserName> (ad esempio RESTAPI_User=COMPANY\Administrator). È possibile selezionare un solo utente per l'utilizzo dell'API REST. L'aggiunta di un nome utente è un prerequisito per la gestione dell'applicazione tramite REST API.
	RESTAPI_Port	Porta utilizzata per la gestione dell'applicazione tramite REST API. La porta 6782 è utilizzata per impostazione predefinita. Assicurarsi che la porta sia libera.

Sezione	Parametro	Descrizione
	`RESTAPI_Certificate`	Certificato per l'identificazione delle richieste (ad esempio, `RESTAPI_Certificate=C:\cert.pem`). L'interazione sicura di Kaspersky Endpoint Security con il client REST richiede la configurazione dell'identificazione delle richieste. A tale scopo, è necessario installare un certificato e successivamente firmare il payload di ogni richiesta.
	`StandaloneMode`	Installazione dell'applicazione in modalità Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* è un'applicazione che viene installata su singole workstation e server nell'infrastruttura IT dell'organizzazione per supportare le soluzioni Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform. EDR Agent è compatibile con le applicazioni PPE di terzi. Ciò consente di utilizzare strumenti di sicurezza dell'infrastruttura di terzi insieme a Kaspersky Detection and Response. Per installare EDR Agent, nella sezione `[Components]`, selezionare i componenti `StandaloneKATA`, `StandaloneNDR` o `StandaloneMDR`. EDR Agent non supporta altri componenti dell'applicazione. Valori disponibili: • `1` per installare l'applicazione in modalità EDR Agent. • `0` per installare l'applicazione in modalità Standard (impostazione predefinita).
	`KSVLAMode`	Installazione dell'applicazione in modalità Light Agent. Questa configurazione è destinata all'applicazione utilizzata come parte della soluzione Kaspersky Security for Virtualization Light Agent. Light Agent deve essere installato in ogni macchina virtuale da proteggere tramite la soluzione. Valori disponibili: • `1` per installare l'applicazione in modalità Light Agent. • `0` per installare l'applicazione in modalità Standard (impostazione predefinita).
	`InstallOnVDI`	Abilitazione della modalità di protezione VDI durante l'installazione dell'applicazione in modalità Light Agent (`KSVLAMode=1`). La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. In questa modalità, Light Agent rifiuta gli aggiornamenti delle applicazioni che richiedono il riavvio della macchina virtuale. Quando si riceve gli aggiornamenti delle applicazioni che richiedono il riavvio, Light Agent genera un evento sulla necessità di aggiornare il modello delle macchine virtuali protette. Valori disponibili: • `1` per abilitare la modalità di protezione VDI. • `0` per disabilitare la modalità di protezione VDI (impostazione predefinita).
	`KESExclusions`	Aggiunta di esclusioni dalla scansione e applicazioni attendibili predefinite durante l'installazione dell'applicazione nel server. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ad esempio, le esclusioni dalle scansioni predefinite per i server SQL includono i file di database MDF e LDF. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server. Valori disponibili: • `1` consente esclusioni dalla scansione e applicazioni attendibili predefinite. • `0` disabilita esclusioni dalla scansione e applicazioni attendibili predefinite (impostazione predefinita).
	`LAExclusions`	Aggiunta di esclusioni dalla scansione e applicazioni attendibili predefinite durante l'installazione dell'applicazione in una macchina virtuale (modalità Light Agent). Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono contribuire a configurare rapidamente Kaspersky Endpoint Security negli ambienti virtuali Citrix e VMware. Valori disponibili: • `1` consente esclusioni dalla scansione e applicazioni attendibili predefinite. • `0` disabilita esclusioni dalla scansione e applicazioni attendibili predefinite (impostazione predefinita).

Sezione	Parametro	Descrizione
	`EnableUniqueSensorID`	Creazione di un identificativo univoco del computer (Sensor ID) durante l'installazione o l'aggiornamento dell'applicazione. Sensor ID viene utilizzato nella soluzione Kaspersky Anti Targeted Attack Platform per identificare i computer che inviano la telemetria al server. Durante la creazione di Sensor ID, l'applicazione utilizza un algoritmo che tiene conto della configurazione del computer, ad esempio il numero di serie della scheda madre. In alcuni casi, ad esempio quando si utilizza l'applicazione in un ambiente virtuale, Sensor ID potrebbe essere duplicato. Di conseguenza, Kaspersky Anti Targeted Attack Platform non è in grado di identificare il computer da cui viene inviata la telemetria. Per creare un Sensor ID univoco, è necessario impostare il parametro `EnableUniqueSensorID=1`. In seguito a questa operazione, l'applicazione utilizzerà un algoritmo diverso per creare Sensor ID, che tiene conto degli altri dati relativi al computer. Questo garantisce un Sensor ID univoco. Per impostazione predefinita, il parametro non è impostato. L'applicazione eredita Sensor ID nei seguenti casi: • aggiornamento della versione dell'applicazione; • migrazione della configurazione [KES+KEA] alla configurazione [KES+agente integrato]. Nell'ambito della riparazione dell'applicazione, il programma di installazione tenta di ereditare l'Sensor ID. Se l'Sensor ID non può essere ripristinato, l'applicazione crea un nuovo Sensor ID.
	`CitrixCompatibility`	Abilitazione del supporto di Citrix Provisioning Services per installare Kaspersky Endpoint Security in una macchina virtuale.
`[Components]`	`ALL`	Installazione di tutti i componenti. Se è specificato il valore del parametro `1`, saranno installati tutti i componenti indipendentemente dalle impostazioni di installazione dei singoli componenti. A causa del modo in cui sono supportate le soluzioni Detection and Response, i componenti Endpoint Detection and Response Optimum e Sandbox vengono installati nel computer. Il componente Endpoint Detection and Response Expert (cloud) non è compatibile con questa configurazione.
	`MailThreatProtection`	Protezione minacce di posta.
	`WebThreatProtection`	Protezione minacce Web.
	`AMSI`	Protezione AMSI.
	`HostIntrusionPrevention`	Prevenzione Intrusioni Host.
	`BehaviorDetection`	Rilevamento del Comportamento.
	`ExploitPrevention`	Prevenzione Exploit.
	`RemediationEngine`	Motore di Remediation.
	`Firewall`	Firewall.
	`NetworkThreatProtection`	Protezione minacce di rete.
	`WebControl`	Controllo Web.
	`DeviceControl`	Controllo dispositivi.
	`ApplicationControl`	Controllo applicazioni.
	`AdaptiveAnomaliesControl`	Controllo adattivo delle anomalie.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Log Inspection
	`AntiCryptor`	Anti-Cryptor
	`FileThreatProtection`	Protezione minacce file.
	`SystemIntegrityMonitor`	Monitoraggio integrità di sistema.
	`FileEncryption`	Librerie di Criptaggio a livello di file.
	`DiskEncryption`	Librerie di Criptaggio dell'intero disco.
	`MSBitLocker`	Librerie di gestione del criptaggio BitLocker.
	`BadUSBAttackPrevention`	Prevenzione Attacchi BadUSB.

Sezione	Parametro	Descrizione
	`EDR`	Endpoint Detection and Response Optimum Il componente non è compatibile con i componenti Endpoint Detection and Response Expert (cloud) (`EDRCloud`) e Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) Il componente non è compatibile con i componenti Endpoint Detection and Response Optimum (`EDR`) e Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) Il componente non è compatibile con i componenti Endpoint Detection and Response Expert (cloud) (`EDRCloud`) e Endpoint Detection and Response Optimum (`EDR`).
	`SB`	Kaspersky Sandbox o KATA Sandbox. *Kaspersky Sandbox* è una soluzione Detection and Response indipendente di Kaspersky. *KATA Sandbox* è un componente della soluzione Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) Il componente non è compatibile con i componenti Endpoint Detection and Response Expert (cloud) (`EDRCloud`) e Endpoint Detection and Response Optimum (`EDR`).
	`AdminKitConnector`	Gestione dell'applicazione tramite sistemi di amministrazione. I sistemi di amministrazione includono ad esempio Kaspersky Security Center. Oltre ai sistemi di amministrazione di Kaspersky, è possibile utilizzare soluzioni di terzi. A tale scopo, Kaspersky Endpoint Security fornisce un'API. Valori disponibili: • `1` - la gestione dell'applicazione con l'ausilio di sistemi di amministrazione è consentita (valore predefinito). • `0` - la gestione dell'applicazione è consentita solo tramite l'interfaccia locale.
	`KUMAIntegration`	Integrazione con KUMA.
	`StandaloneKATA`	Installazione dell'applicazione in modalità Endpoint Detection and Response Agent (EDR Agent) per l'integrazione con la soluzione Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Installazione dell'applicazione in modalità Endpoint Detection and Response Agent (EDR Agent) per l'integrazione con Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Installazione dell'applicazione in modalità Endpoint Detection and Response Agent (EDR Agent) per l'integrazione con la soluzione Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Installazione dell'applicazione in modalità Endpoint Detection and Response Agent (EDR Agent) per l'integrazione con KUMA.
`[Tasks]`	`ScanMyComputer`	Attività Scansione completa. Valori disponibili: • `1` – l'attività viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security. • `0` – l'attività non viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security.
	`ScanCritical`	Attività Scansione delle aree critiche. Valori disponibili: • `1` – l'attività viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security. • `0` – l'attività non viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security.
	`Updater`	Attività di aggiornamento. Valori disponibili: • `1` – l'attività viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security. • `0` – l'attività non viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security.

Processi di Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows avvia i processi descritti nella tabella seguente.

Processi di Kaspersky Endpoint Security for Windows

Nome file	Scopo
avp.exe	Processo di lavoro di Kaspersky Endpoint Security for Windows.
avpsus.exe	Questo processo consente di installare e ripristinare le versioni precedenti degli aggiornamenti critici e approvati dei moduli dell'applicazione.

Modifica componenti dell'applicazione

Durante l'installazione dell'applicazione, è possibile selezionare i componenti che saranno disponibili. È possibile modificare i componenti dell'applicazione disponibili nei seguenti modi:

- In locale, utilizzando l'Installazione guidata.

  I componenti dell'applicazione vengono modificati utilizzando il metodo standard per un sistema operativo Windows, vale a dire tramite il Pannello di controllo. Eseguire l'Installazione guidata dell'applicazione e selezionare l'opzione per modificare i componenti dell'applicazione disponibili. Attenersi alle istruzioni visualizzate.

  > Questo metodo non è disponibile se l'applicazione è stata installata tramite Kaspersky Security Center. È possibile modificare la selezione dei componenti dell'applicazione nel Pannello di controllo solo dopo l'installazione dell'applicazione in locale.

- Da remoto tramite Kaspersky Security Center.

  L'attività *Modifica i componenti dell'applicazione* consente di modificare i componenti di Kaspersky Endpoint Security dopo l'installazione dell'applicazione.

Tenere conto delle seguenti considerazioni speciali quando si modificano i componenti dell'applicazione:

- Nei computer che eseguono Windows Server, non è possibile installare tutti i componenti di Kaspersky Endpoint Security (ad esempio il componente Controllo adattivo delle anomalie non è disponibile).
- Se i dischi rigidi nel computer sono protetti da Criptaggio dell'intero disco, non è possibile rimuovere il componente Criptaggio dell'intero disco. Per rimuovere il componente Criptaggio dell'intero disco, decriptare tutti i dischi rigidi del computer.
- Se il computer dispone di file criptati (FLE) o l'utente utilizza unità rimovibili criptate (FDE o FLE), sarà impossibile accedere ai file e alle unità rimovibili dopo aver rimosso i componenti di criptaggio dei dati. È possibile accedere ai file e alle unità rimovibili reinstallando i componenti di criptaggio dei dati.
- Se l'applicazione è installata in modalità Light Agent in un'infrastruttura VDI, la modifica dei componenti del set non è supportata.

Come aggiungere o rimuovere componenti dell'applicazione in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Selezionare i componenti da installare**.

Passaggio 2. Impostazioni dell'attività per la modifica dei componenti dell'applicazione

Selezionare la configurazione dell'applicazione:

- **Modalità standard per proteggere gli host**. La configurazione predefinita. Questa configurazione consente di utilizzare tutti i componenti dell'applicazione, inclusi i componenti che forniscono supporto per le soluzioni Detection and Response. Questa configurazione viene utilizzata per una protezione completa del computer da una serie di minacce, attacchi di rete e frodi.

- **Endpoint Detection and Response Agent per proteggere da minacce avanzate e attacchi mirati**. In questa configurazione, è possibile installare solo i componenti che forniscono supporto per le soluzioni Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), così come KUMA. Questa configurazione è necessaria se nell'organizzazione viene distribuita una Endpoint Protection Platform (EPP) di terzi insieme a una soluzione Kaspersky Detection and Response. Ciò rende Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent compatibile con le applicazioni EPP di terzi.

  Quando si modifica la configurazione dell'applicazione per fare in modo che EDR Agent funzioni con MDR, verificare che i componenti responsabili della ricezione della telemetria siano abilitati.

- **Light Agent per proteggere gli ambienti virtuali**. Questa configurazione è destinata all'applicazione utilizzata come parte della soluzione Kaspersky Security for Virtualization Light Agent. Light Agent deve essere installato in ogni macchina virtuale da proteggere tramite la soluzione. In questa configurazione, non è possibile utilizzare i componenti di Criptaggio dati o Controllo adattivo delle anomalie. Se si installa Light Agent in un modello di macchina virtuale che verrà utilizzato per creare *macchine virtuali non persistenti*, selezionare la casella di controllo **Proteggi infrastruttura VDI** (VDI è l'acronimo di Virtual Desktop Infrastructure). La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. In questa modalità, Light Agent rifiuta gli aggiornamenti delle applicazioni che richiedono il riavvio della macchina virtuale. Quando si riceve gli aggiornamenti delle applicazioni che richiedono il riavvio, Light Agent genera un evento sulla necessità di aggiornare il modello delle macchine virtuali protette.

Selezionare i componenti dell'applicazione che saranno disponibili nel computer dell'utente.

Passaggio 3. Impostazioni avanzate

Configurare le impostazioni avanzate per l'attività (vedere la tabella seguente).

Passaggio 4. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 5. Configurazione di una pianificazione di avvio dell'attività

Configurare una pianificazione per l'avvio di un'attività, ad esempio manualmente o quando il computer è inattivo.

Passaggio 6. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Aggiungi il componente Controllo applicazioni*.

Passaggio 7. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come aggiungere o rimuovere i componenti dell'applicazione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Configurazione delle impostazioni generali dell'attività

Configurare le impostazioni generali dell'attività:

1. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2.0**.
2. Nell'elenco a discesa **Tipo di attività**, selezionare **Modifica i componenti dell'applicazione**.
3. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Aggiungere il componente Controllo applicazioni*.
4. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

Passaggio 2. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Ad esempio, selezionare un gruppo di amministrazione separato o creare una selezione.

Passaggio 3. Completamento della creazione dell'attività

Selezionare la casella di controllo **Apri i dettagli dell'attività al termine della creazione** e terminare la procedura guidata.

Nelle proprietà dell'attività, selezionare la scheda **Impostazioni applicazione**. Successivamente, selezionare la configurazione dell'applicazione:

- **Modalità standard per proteggere workstation e server**. La configurazione predefinita. Questa configurazione consente di utilizzare tutti i componenti dell'applicazione, inclusi i componenti che forniscono supporto per le soluzioni Detection and Response. Questa configurazione viene utilizzata per una protezione completa del computer da una serie di minacce, attacchi di rete e frodi.

- **Endpoint Detection and Response Agent per proteggere da minacce avanzate e attacchi mirati**. In questa configurazione, è possibile installare solo i componenti che forniscono supporto per le soluzioni Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), così come KUMA. Questa configurazione è necessaria se nell'organizzazione viene distribuita una Endpoint Protection Platform (EPP) di terzi insieme a una soluzione Kaspersky Detection and Response. Ciò rende Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent compatibile con le applicazioni EPP di terzi.

  Quando si modifica la configurazione dell'applicazione per fare in modo che EDR Agent funzioni con MDR, verificare che i componenti responsabili della ricezione della telemetria siano abilitati.

- **Light Agent per proteggere gli ambienti virtuali**. Questa configurazione è destinata all'applicazione utilizzata come parte della soluzione Kaspersky Security for Virtualization Light Agent. Light Agent deve essere installato in ogni macchina virtuale da proteggere tramite la soluzione. In questa configurazione, non è possibile utilizzare i componenti di Criptaggio dati o Controllo adattivo delle anomalie. Se si installa Light Agent in un modello di macchina virtuale che verrà utilizzato per creare *macchine virtuali non persistenti*, selezionare la casella di controllo **Proteggi infrastruttura VDI** (VDI è l'acronimo di Virtual Desktop Infrastructure). La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. In questa modalità, Light Agent rifiuta gli aggiornamenti delle applicazioni che richiedono il riavvio della macchina virtuale. Quando si riceve gli aggiornamenti delle applicazioni che richiedono il riavvio, Light Agent genera un evento sulla necessità di aggiornare il modello delle macchine virtuali protette.

Selezionare i componenti dell'applicazione che saranno disponibili nel computer dell'utente. Configurare le impostazioni avanzate per l'attività (vedere la tabella seguente).

In seguito a questa operazione, il set di componenti di Kaspersky Endpoint Security nei computer degli utenti verrà modificato in modalità automatica. Le impostazioni dei componenti disponibili verranno visualizzate nell'interfaccia locale dell'applicazione. I componenti che non sono stati inclusi nell'applicazione sono disabilitati e le impostazioni di questi componenti non sono disponibili.

Durante l'installazione, l'aggiornamento o la disinstallazione di Kaspersky Endpoint Security, potrebbero verificarsi degli errori. Per ulteriori informazioni sulla risoluzione di questi errori, consultare la Knowledge Base dell'Assistenza tecnica.

Parametro	Descrizione
Impostazioni attività	**Controlla le applicazioni di terzi incompatibili**. Per impostazione predefinita, Kaspersky Endpoint Security controlla la compatibilità delle applicazioni installate. L'elenco del software che può causare problemi di compatibilità è disponibile nel file incompatible.txt. Il file è incluso nel kit di distribuzione. Se la scansione del software installato è abilitata, quando viene rilevata un'applicazione presente nell'elenco, Kaspersky Endpoint Security arresta l'attività. È possibile disabilitare la scansione del software installato se la documentazione del fornitore del software di terze parti dichiara la compatibilità con Endpoint Protection Platform (PPE). **Rimuovi le applicazioni di terzi incompatibili**. Rimozione automatica delle applicazioni elencate nel file incompatible.txt prima di modificare il set di componenti. Se questa funzionalità è abilitata, Kaspersky Endpoint Security tenta di rimuovere le applicazioni che potrebbero causare problemi di compatibilità per continuare l'attività. **Usa modalità di compatibilità WVD di Azure**. Questa funzionalità garantisce la corretta visualizzazione dello stato della macchina virtuale di Azure nella console Kaspersky Anti Targeted Attack Platform. Per monitorare le prestazioni del computer, Kaspersky Endpoint Security invia dati di telemetria ai server KATA. La telemetria include un ID del computer (Sensor ID). La modalità di compatibilità Azure WVD consente di assegnare un Sensor ID univoco permanente a queste macchine virtuali. Se la modalità di compatibilità è disattivata, l'Sensor ID può cambiare dopo il riavvio del computer a causa del funzionamento delle macchine virtuali di Azure. Ciò può causare la visualizzazione di duplicati di macchine virtuali sulla console.
Esclusioni	A partire da Kaspersky Endpoint Security 12.6 for Windows, le esclusioni dalle scansioni e le applicazioni attendibili vengono aggiunte all'area attendibile. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server. A partire da Kaspersky Endpoint Security 12.8 for Windows, è possibile installare l'applicazione in modalità Light Agent per proteggere gli ambienti virtuali. Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono contribuire a configurare rapidamente Kaspersky Endpoint Security negli ambienti virtuali Citrix e VMware. È anche possibile configurare l'area attendibile in un secondo momento nelle proprietà del criterio: esclusioni dalle scansioni e applicazioni attendibili.
Modalità separata/Modalità combinata	È possibile creare insiemi distinti di componenti per la workstation e i server: **Modalità separata**. Prima di distribuire il pacchetto di installazione, il programma di installazione rileva il tipo di sistema operativo e installa solo i componenti dell'applicazione selezionati per il tipo di sistema operativo. In questo modo, è possibile utilizzare lo stesso pacchetto di installazione per le workstation e i server. **Modalità combinata** offre un elenco comune di componenti per workstation e server. La disponibilità dei singoli componenti dipende dal tipo di sistema operativo. In questa modalità, è consigliabile creare un pacchetto di installazione separato per le workstation e un pacchetto di installazione separato per i server. È possibile configurare l'elenco comune dei componenti nel pacchetto di installazione solo in modalità Standard.
Usa password per la modifica del set di componenti dell'applicazione	In genere, gli amministratori abilitano la protezione tramite password per limitare l'accesso a Kaspersky Endpoint Security. In altre parole, per modificare la selezione dei componenti dell'applicazione, è necessario immettere le credenziali di un utente che dispone dell'autorizzazione **Rimuovi/modifica/ripristina l'applicazione**. Ad esempio, è possibile utilizzare l'account KLAdmin.
Usa la password per la disinstallazione di Kaspersky Endpoint Agent e Kaspersky Security for Windows Server	Gli amministratori in genere abilitano la protezione tramite password nelle impostazioni di queste attività per limitare l'accesso a Kaspersky Endpoint Agent (KEA) e Kaspersky Security for Windows Server (KSWS). In altre parole, se si esegue la migrazione dalla configurazione [KES KEA] a [agente integrato KES], o se si esegue la migrazione da KSWS a KES, è necessario immettere una password per rimuovere queste applicazioni.

Upgrade di una versione precedente dell'applicazione

Quando si aggiorna una versione precedente dell'applicazione a una versione più recente, considerare quanto segue:

- È consigliabile chiudere tutte le applicazioni attive prima di avviare l'aggiornamento.
- Prima dell'aggiornamento, Kaspersky Endpoint Security blocca la funzionalità Criptaggio dell'intero disco. Se non è possibile bloccare Criptaggio dell'intero disco, l'installazione dell'upgrade non verrà avviata. Dopo l'aggiornamento dell'applicazione, la funzionalità Criptaggio dell'intero disco verrà ripristinata.
- Per modificare la lingua dell'applicazione, nell'attività *Installa l'applicazione in remoto* selezionare il pacchetto di installazione con la localizzazione desiderata e aggiornare l'applicazione. La possibilità di modificare la lingua dell'applicazione è stata introdotta in Kaspersky Endpoint Security for Windows 14.2.

Kaspersky Endpoint Security supporta gli aggiornamenti per le seguenti versioni dell'applicazione:

- Kaspersky Endpoint Security 12.3 for Windows (build 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (build 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (build 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (build 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (build 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (build 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (build 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (build 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (build 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (build 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (build 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (build 14.1.0.423)

Durante l'installazione, l'aggiornamento o la disinstallazione di Kaspersky Endpoint Security, potrebbero verificarsi degli errori. Per ulteriori informazioni sulla risoluzione di questi errori, consultare la Knowledge Base dell'Assistenza tecnica.

Metodi di upgrade dell'applicazione

Kaspersky Endpoint Security può essere aggiornato nel computer nei seguenti modi:

- Tramite il servizio di aggiornamento di Kaspersky (Seamless Update - SMU).
- In locale, utilizzando l'Installazione guidata.
- In locale dalla riga di comando.
- Da remoto tramite Kaspersky Security Center.
- Da remoto tramite l'editor Gestione Criteri di gruppo di Microsoft Windows (per ulteriori dettagli, visitare il sito Web del supporto tecnico di Microsoft).
- In remoto, utilizzando System Center Configuration Manager.

Se l'applicazione distribuita nella rete aziendale presenta un set di componenti diverso da quello predefinito, l'aggiornamento dell'applicazione tramite Administration Console (MMC) è differente dall'aggiornamento dell'applicazione tramite Web Console. Durante l'aggiornamento di Kaspersky Endpoint Security, tenere presente quanto segue:

- Kaspersky Security Center Web Console.

  Se è stato creato un pacchetto di installazione per la nuova versione dell'applicazione con il set di componenti predefinito, il set di componenti nel computer di un utente non verrà modificato. Per utilizzare Kaspersky Endpoint Security con il set di componenti predefinito, è necessario aprire le proprietà del pacchetto di installazione, modificare il set di componenti, quindi ripristinare il set di componenti originale e salvare le modifiche.

- Kaspersky Security Center Administration Console.

  Il set di componenti dell'applicazione dopo l'aggiornamento corrisponderà al set di componenti nel pacchetto di installazione. In altre parole, se la nuova versione dell'applicazione dispone del set di componenti predefinito, ad esempio, l'agente MDR integrato verrà rimosso dal computer, poiché questo componente è escluso dal set predefinito. Per continuare a utilizzare l'applicazione con lo stesso set di componenti in uso prima dell'aggiornamento, selezionare i componenti richiesti nelle impostazioni del pacchetto di installazione.

Upgrade dell'applicazione senza un riavvio

L'upgrade dell'applicazione senza un riavvio garantisce il funzionamento ininterrotto del server quando viene aggiornata la versione dell'applicazione.

L'upgrade dell'applicazione senza un riavvio presenta le seguenti limitazioni:

- È possibile eseguire l'upgrade dell'applicazione senza riavvio a partire dalla versione 11.10.0. Per eseguire l'upgrade a una versione precedente dell'applicazione, è necessario riavviare il computer.
- È possibile installare le patch senza riavvio a partire dalla versione 11.11.0. Per installare le patch per le versioni precedenti dell'applicazione, potrebbe essere necessario riavviare il computer.
- L'upgrade dell'applicazione senza un riavvio non è disponibile nei computer con il criptaggio dei dati abilitato (criptaggio Kaspersky (FDE), BitLocker, criptaggio a livello di file (FLE)). Per eseguire l'upgrade dell'applicazione in computer con criptaggio dei dati abilitato, è necessario riavviare il computer.
- Non è possibile eseguire l'upgrade dell'applicazione in una macchina virtuale senza un riavvio. Per eseguire l'upgrade dell'applicazione in una macchina virtuale, è necessario riavviare la macchina virtuale.

In seguito all'upgrade dell'applicazione, all'installazione di una patch, alla modifica del set di componenti dell'applicazione o al ripristino, Kaspersky Endpoint Security si riavvia per iniziare a utilizzare la nuova versione. Il riavvio di Kaspersky Endpoint Security potrebbe richiedere fino a un minuto. Durante questo periodo di tempo, il livello di protezione del computer è ridotto. Dopo aver riavviato l'applicazione, il livello di protezione del computer verrà ripristinato.

Come selezionare la modalità di upgrade dell'applicazione in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni applicazione**.

5. Nel blocco **Impostazioni avanzate**, selezionare o deselezionare la casella di controllo **Installa aggiornamenti delle applicazioni senza riavvio** per configurare la modalità di upgrade dell'applicazione.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come selezionare la modalità di upgrade dell'applicazione in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Interazione utente**.

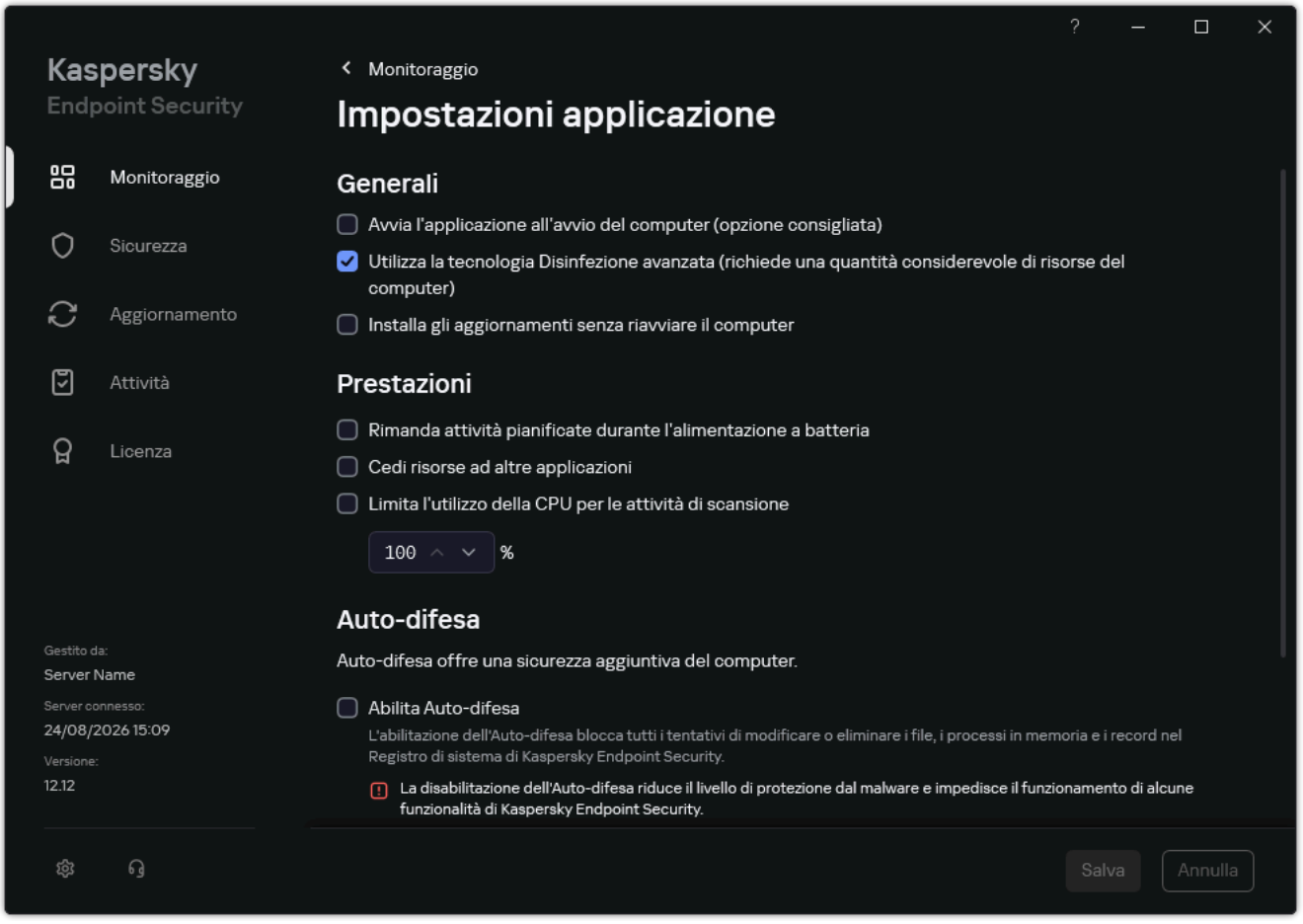
5. Nel blocco **Impostazioni di aggiornamento delle applicazioni**, selezionare o deselezionare la casella di controllo **Installa aggiornamenti delle applicazioni senza riavvio** per configurare la modalità di upgrade dell'applicazione.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come selezionare la modalità di upgrade dell'applicazione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.



Impostazioni di Kaspersky Endpoint Security for Windows

3. Nel blocco **Generali**, selezionare o deselezionare la casella di controllo **Installa gli aggiornamenti senza riavviare il computer** per configurare la modalità di upgrade dell'applicazione.

4. Salvare le modifiche.

È inoltre possibile selezionare la modalità di aggiornamento dell'applicazione durante l'installazione dell'applicazione dalla riga di comando (utilizzando l'opzione `UPGRADEMODE`).

Al termine della procedura di upgrade dell'applicazione senza riavvio, la nuova versione di Kaspersky Endpoint Security sarà stata installata nel computer. La versione precedente dell'applicazione viene eliminata automaticamente.

Non è possibile avviare l'upgrade di un'applicazione prima del termine dell'upgrade precedente.

È possibile controllare lo stato di upgrade di Kaspersky Endpoint Security utilizzando il report sulla versione dell'applicazione Kaspersky nella console di Kaspersky Security Center.

Aggiornamento SMU dell'applicazione

Per aggiornare l'applicazione utilizzando il servizio di aggiornamento Kaspersky (Seamless Update; SMU), non è necessario eseguire il programma di installazione, a differenza di altri metodi di aggiornamento. Kaspersky Endpoint Security ottiene la nuova versione dell'applicazione insieme ai database anti-virus dalla stessa sorgente.

Un aggiornamento SMU consente di aggiornare l'applicazione in tutti i computer dell'organizzazione alla versione più recente. Prima di applicare un aggiornamento SMU, si consiglia di testare la nuova versione dell'applicazione in alcuni computer. A tale scopo, è necessario aggiornare manualmente l'applicazione in questi computer (ad esempio, in locale utilizzando l'Installazione guidata). Non è possibile selezionare singoli computer durante l'esecuzione di un aggiornamento SMU.

La pianificazione degli aggiornamenti per l'applicazione è determinata dal personale di Kaspersky. Per garantire il corretto funzionamento della nuova versione dell'applicazione, Kaspersky rende disponibili gli aggiornamenti passo dopo passo. Questo significa che è possibile ricevere l'aggiornamento SMU fino a due mesi dopo il rilascio di una nuova versione.

È possibile gestire l'aggiornamento SMU dell'applicazione tramite l'attività *Aggiornamento di database e moduli dell'applicazione*. Per fare in modo che la nuova versione dell'applicazione venga inclusa nello stesso pacchetto dei database anti-virus, è necessario consentire l'aggiornamento dei *moduli dell'applicazione* nelle impostazioni dell'attività *Aggiornamento di database e moduli dell'applicazione*. Nelle impostazioni dell'attività *Aggiornamento di database e moduli dell'applicazione*, è inoltre possibile consentire l'aggiornamento dell'applicazione senza richiedere il riavvio.

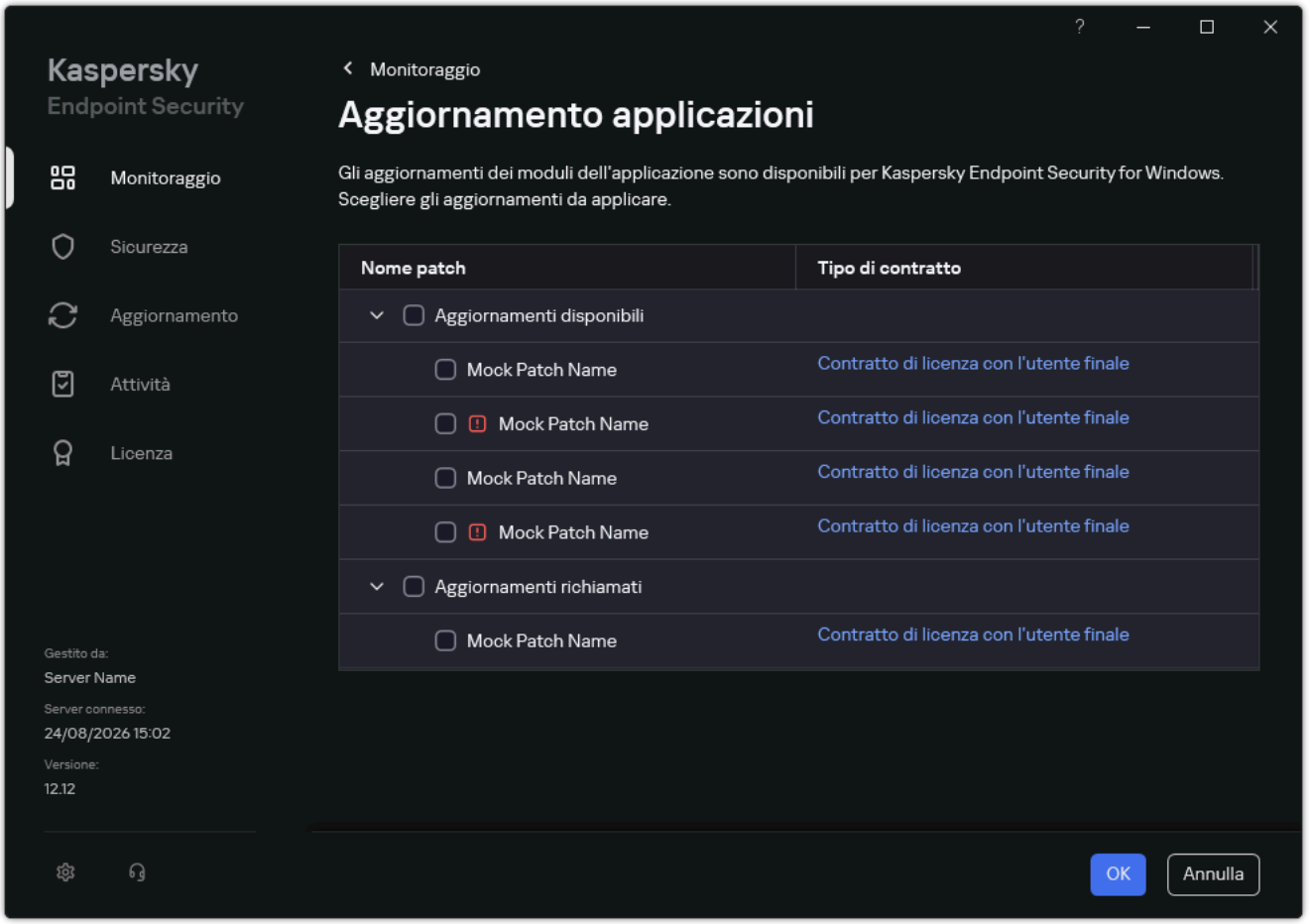
Passaggi di un aggiornamento SMU dell'applicazione

1. **Dopo il rilascio di una nuova versione dell'applicazione, Kaspersky distribuisce l'aggiornamento.**
2. **L'utente approva l'aggiornamento dell'applicazione.**

   Se il computer è connesso a Kaspersky Security Center, l'aggiornamento è disponibile in Kaspersky Security Center, nella sezione **Aggiornamento dei database Kaspersky e dei moduli dell'applicazione**. Per ulteriori dettagli sull'approvazione degli aggiornamenti, consultare la Guida di Kaspersky Security Center.

   Se il computer non è connesso a Kaspersky Security Center, l'aggiornamento è disponibile nella sezione di notifica dell'interfaccia dell'applicazione: . Per approvare l'aggiornamento, selezionare una versione dell'applicazione e accettare i termini e le condizioni degli accordi (vedere la figura seguente).
3. **Kaspersky Endpoint Security esegue l'attività *Aggiornamento di database e moduli dell'applicazione* in base alla pianificazione configurata.**

A questo punto, Kaspersky Endpoint Security aggiorna l'applicazione in modalità automatica.



Aggiornamenti delle applicazioni disponibili

Rimozione dell'applicazione

La rimozione di Kaspersky Endpoint Security lascia il computer e i dati dell'utente senza protezione dalle minacce.

Durante l'installazione, l'aggiornamento o la disinstallazione di Kaspersky Endpoint Security, potrebbero verificarsi degli errori. Per ulteriori informazioni sulla risoluzione di questi errori, consultare la Knowledge Base dell'Assistenza tecnica.

Rimozioni dell'applicazione da remoto tramite Kaspersky Security Center

È possibile disinstallare in remoto l'applicazione utilizzando l'attività *Disinstalla l'applicazione in remoto*. Quando si esegue l'attività, Kaspersky Endpoint Security scarica l'utilità di disinstallazione dell'applicazione nel computer dell'utente. Al termine della disinstallazione dell'applicazione, l'utilità verrà rimossa automaticamente.

Come rimuovere l'applicazione tramite Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Attività**.
   Viene aperto l'elenco delle attività.
3. Fare clic su **Nuova attività**.

   Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Security Center Administration Server → Avanzate → Disinstalla l'applicazione in remoto**

Passaggio 2. Selezione dell'applicazione da rimuovere

Selezionare **Disinstalla applicazione supportata da Kaspersky Security Center**.

Passaggio 3. Impostazioni dell'attività per la disinstallazione dell'applicazione

Selezionare **Kaspersky Endpoint Security for Windows (14.2)**.

Passaggio 4. Disinstallazione delle impostazioni dell'utilità

Configurare le seguenti impostazioni aggiuntive dell'applicazione:

- **Forza il download dell'utilità di disinstallazione**. Selezionare il metodo di invio dell'utilità:
  - **Utilizzando Network Agent**. Se Network Agent non è stato installato nel computer, verrà installato per prima cosa utilizzando gli strumenti del sistema operativo. Kaspersky Endpoint Security verrà quindi disinstallato dagli strumenti di Network Agent.
  - **Utilizzando le risorse del sistema operativo tramite Administration Server**. L'utilità verrà inviata ai computer client utilizzando le risorse del sistema operativo tramite Administration Server. È possibile selezionare questa opzione se nel computer client non è installato alcun Network Agent, ma il computer client si trova nella stessa rete di Administration Server.
  - **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**. L'utilità viene distribuita ai computer client utilizzando le risorse del sistema operativo tramite punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete. Per informazioni dettagliate sui punti di distribuzione, consultare la Guida di Kaspersky Security Center.
- **Verifica il tipo di sistema operativo prima del download**. Se necessario, deselezionare questa casella di controllo. Questo consente di evitare di scaricare l'utilità di disinstallazione se il sistema operativo del computer non soddisfa i requisiti software. Se si è certi che il sistema operativo del computer soddisfi i requisiti software, è possibile ignorare la verifica.

Se l'operazione di disinstallazione dell'applicazione è protetta da password, procedere come segue:

1. Selezionare la casella di controllo **Usa password di disinstallazione**.
2. Fare clic sul pulsante **Modifica**.
3. Immettere la password dell'account KLAdmin.

Passaggio 5. Selezione dell'impostazione di riavvio del sistema operativo

Dopo aver disinstallato l'applicazione, è necessario un riavvio. Selezionare l'azione che verrà eseguita per riavviare il computer.

Passaggio 6. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 7. Selezione dell'account per eseguire l'attività

Selezionare l'account per l'installazione di Network Agent utilizzando gli strumenti del sistema operativo. In questo caso sono richiesti i diritti di amministratore per l'accesso al computer. È possibile aggiungere più account. Se un account non dispone dei diritti sufficienti, l'Installazione guidata utilizza l'account successivo. Se si disinstalla Kaspersky Endpoint Security utilizzando gli strumenti di Network Agent, non è necessario selezionare un account.

Passaggio 8. Configurazione di una pianificazione di avvio dell'attività

Configurare una pianificazione per l'avvio di un'attività, ad esempio manualmente o quando il computer è inattivo.

Passaggio 9. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Rimuovi Kaspersky Endpoint Security 14.2*.

Passaggio 10. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

L'applicazione verrà disinstallata in modalità automatica.

Come rimuovere l'applicazione tramite Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Configurazione delle impostazioni generali dell'attività

Configurare le impostazioni generali dell'attività:

1. Nell'elenco a discesa **Applicazione** selezionare **Kaspersky Security Center**.
2. Nell'elenco a discesa **Tipo di attività**, selezionare **Disinstalla l'applicazione in remoto**.
3. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Disinstallare Kaspersky Endpoint Security dai computer dell'Assistenza tecnica*.
4. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

Passaggio 2. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Ad esempio, selezionare un gruppo di amministrazione separato o creare una selezione.

Passaggio 3. Configurazione delle impostazioni di disinstallazione dell'applicazione

In questo passaggio configurare le impostazioni di disinstallazione dell'applicazione:

1. Selezionare il tipo **Disinstalla l'applicazione gestita**.
2. Selezionare **Kaspersky Endpoint Security for Windows**.
3. **Forza il download dell'utilità di disinstallazione**. Selezionare il metodo di invio dell'utilità:
   - **Utilizzando Network Agent**. Se Network Agent non è stato installato nel computer, verrà installato per prima cosa utilizzando gli strumenti del sistema operativo. Kaspersky Endpoint Security verrà quindi disinstallato dagli strumenti di Network Agent.
   - **Utilizzando le risorse del sistema operativo tramite Administration Server**. L'utilità verrà inviata ai computer client utilizzando le risorse del sistema operativo tramite Administration Server. È possibile selezionare questa opzione se nel computer client non è installato alcun Network Agent, ma il computer client si trova nella stessa rete di Administration Server.
   - **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**. L'utilità viene distribuita ai computer client utilizzando le risorse del sistema operativo tramite punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete. Per informazioni dettagliate sui punti di distribuzione, consultare la Guida di Kaspersky Security Center.
4. Nel campo **Numero massimo di download simultanei**, impostare un limite per il numero di richieste inviate ad Administration Server per scaricare l'utilità di disinstallazione dell'applicazione. Il limite relativo al numero di richieste consentirà di evitare un sovraccarico della rete.

5. Nel campo **Numero massimo di tentativi di disinstallazione**, impostare un limite relativo al numero di tentativi di disinstallazione dell'applicazione. Se la disinstallazione di Kaspersky Endpoint Security termina con un errore, l'attività avvierà automaticamente la nuova disinstallazione.

6. Se necessario, deselezionare la casella di controllo **Verifica il tipo di sistema operativo prima del download**. Questo consente di evitare di scaricare l'utilità di disinstallazione se il sistema operativo del computer non soddisfa i requisiti software. Se si è certi che il sistema operativo del computer soddisfi i requisiti software, è possibile ignorare la verifica.

Passaggio 4. Selezione dell'account per eseguire l'attività

Selezionare l'account per l'installazione di Network Agent utilizzando gli strumenti del sistema operativo. In questo caso sono richiesti i diritti di amministratore per l'accesso al computer. È possibile aggiungere più account. Se un account non dispone dei diritti sufficienti, l'Installazione guidata utilizza l'account successivo. Se si disinstalla Kaspersky Endpoint Security utilizzando gli strumenti di Network Agent, non è necessario selezionare un account.

Passaggio 5. Completamento della creazione dell'attività

Terminare la procedura guidata facendo clic sul pulsante **Fine**. Verrà visualizzata una nuova attività nell'elenco delle attività.

Per eseguire un'attività, selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**. L'applicazione verrà disinstallata in modalità automatica. Al termine della disinstallazione, Kaspersky Endpoint Security visualizza la richiesta di riavvio del computer.

Se l'operazione di disinstallazione dell'applicazione è protetta tramite password, immettere la password dell'account KLAdmin nelle proprietà dell'attività *Disinstalla applicazione in remoto*. Senza la password, l'attività non verrà eseguita.

Per utilizzare la password dell'account KLAdmin nell'attività Disinstalla applicazione in remoto:

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Disinstalla l'applicazione in remoto** di Kaspersky Security Center.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Selezionare la casella di controllo **Usa password di disinstallazione**.

5. Immettere la password dell'account KLAdmin.

6. Salvare le modifiche.

Riavviare il computer per completare la disinstallazione. A tale scopo, Network Agent mostra una finestra pop-up.

Rimozione dell'applicazione da remoto tramite Active Directory

È possibile disinstallare l'applicazione da remoto utilizzando un criterio di gruppo di Microsoft Windows. Per disinstallare l'applicazione, è necessario aprire la Console Gestione Criteri di gruppo (gpmc.msc) e utilizzare Editor Criteri di gruppo per creare un'attività di rimozione delle applicazioni (per ulteriori informazioni, visitare il sito Web dell'Assistenza tecnica di Microsoft).

Se l'operazione di disinstallazione dell'applicazione è protetta da password, è necessario procedere come segue:

1. Creare un file BAT con i seguenti contenuti:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   Per `<GUID>` si intende l'ID univoco dell'applicazione. È possibile trovare il GUID dell'applicazione nella Knowledge Base dell'Assistenza tecnica oppure utilizzando il seguente comando:

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   Esempio

   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Creare un nuovo criterio di Microsoft Windows per i computer nella Console Gestione Criteri di gruppo (gpmc.msc).

3. Utilizzare il nuovo criterio per eseguire il file BAT creato sui computer.

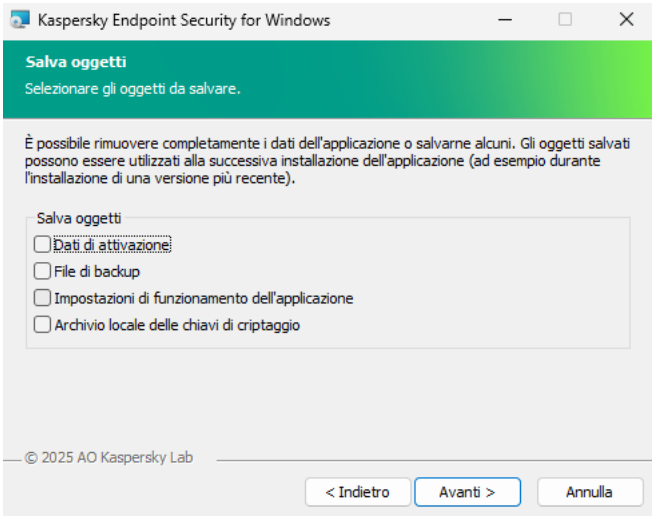
Disinstallazione dell'applicazione in locale

È inoltre possibile disinstallare l'applicazione in locale, utilizzando l'Installazione guidata. Kaspersky Endpoint Security viene rimosso utilizzando il metodo standard per un sistema operativo Windows, vale a dire tramite il Pannello di controllo. Verrà avviata l'Installazione guidata. Attenersi alle istruzioni visualizzate.



Selezione dell'operazione di rimozione dell'applicazione

È possibile specificare i dati utilizzati dall'applicazione che si desidera salvare per un utilizzo futuro, durante l'installazione successiva dell'applicazione (ad esempio durante l'upgrade a una versione più recente dell'applicazione). Se non si specificano dati, l'applicazione verrà rimossa completamente (vedere la figura riportata di seguito).



Salvataggio dei dati dopo la rimozione

È possibile salvare i seguenti dati:

- **Dati di attivazione**, per non dover attivare nuovamente l'applicazione. Kaspersky Endpoint Security aggiunge automaticamente una chiave di licenza se il periodo licenza non è scaduto prima dell'installazione.
- I **File di backup** sono file esaminati dall'applicazione e spostati in Backup.

  Ai file di backup salvati dopo la rimozione dell'applicazione è possibile accedere solo dalla stessa versione dell'applicazione utilizzata per salvarli.

  Se si prevede di utilizzare gli oggetti di backup dopo la rimozione dell'applicazione, è necessario ripristinare tali oggetti prima di rimuovere l'applicazione. Tuttavia, gli esperti di Kaspersky sconsigliano di ripristinare gli oggetti da Backup, poiché potrebbero danneggiare il computer.

- **Impostazioni di funzionamento dell'applicazione** – valori delle impostazioni dell'applicazione selezionati durante la configurazione dell'applicazione.
- **Archivio locale delle chiavi di criptaggio** – dati che consentono di accedere ai file e alle unità che sono stati criptati prima della rimozione dell'applicazione. Per garantire l'accesso alle unità e ai file criptati, assicurarsi che sia selezionata la funzionalità di criptaggio dei dati durante la reinstallazione di Kaspersky Endpoint Security. Non sono richieste ulteriori azioni per l'accesso alle unità e ai file precedentemente criptati.

Kaspersky Endpoint Security salva i rapporti nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

È inoltre possibile eliminare l'applicazione in locale tramite la riga di comando.

Licensing dell'applicazione

Questa sezione fornisce informazioni su concetti generali legati alla gestione delle licenze di Kaspersky Endpoint Security.

Informazioni sul Contratto di licenza con l'utente finale

Il *Contratto di licenza con l'utente finale* è un accordo vincolante tra l'utente e AO Kaspersky Lab, in cui sono definite le condizioni di utilizzo dell'applicazione.

Leggere attentamente le condizioni del Contratto di licenza prima di utilizzare l'applicazione.

È possibile leggere le condizioni del Contratto di licenza nei seguenti modi:

- Durante l'installazione di Kaspersky Endpoint Security in modalità interattiva.
- Consultando il file license.txt. Questo documento è incluso nel kit di distribuzione dell'applicazione e si trova anche nella cartella di installazione dell'applicazione `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

Confermando l'accettazione del Contratto di licenza con l'utente finale durante l'installazione dell'applicazione, si accettano le condizioni del Contratto di licenza con l'utente finale. Se non si accettano le condizioni del Contratto di licenza con l'utente finale, è necessario interrompere l'installazione.

Informazioni sulla licenza

Una *licenza* concede per un determinato periodo di tempo il diritto di utilizzare l'applicazione, in conformità con il Contratto di licenza con l'utente finale.

La licenza autorizza l'utente a utilizzare l'applicazione in conformità con i termini del Contratto di licenza con l'utente finale e a ricevere assistenza tecnica. L'elenco delle funzionalità disponibili e delle condizioni per l'utilizzo dell'applicazione dipendono dal tipo di licenza utilizzata per attivare l'applicazione.

Sono disponibili i seguenti tipi di licenza:

- *Di prova* - una licenza gratuita che consente di valutare l'applicazione.

  Una licenza di prova in genere è utilizzabile per un periodo di tempo limitato. Dopo la scadenza della licenza di prova, tutte le funzionalità di Kaspersky Endpoint Security vengono disabilitate. Per continuare a utilizzare l'applicazione, è necessario acquistare una licenza commerciale.

  È possibile attivare l'applicazione con una licenza di prova una sola volta. L'applicazione non può essere attivata con una licenza di prova dopo essere stata attivata con una licenza commerciale.

- *Commerciale* - una licenza a pagamento fornita al momento dell'acquisto di Kaspersky Endpoint Security.

  Le funzionalità dell'applicazione disponibili con la licenza commerciale dipendono dal prodotto scelto. Il prodotto selezionato è indicato nel Certificato di licenza. Per informazioni sui prodotti disponibili, visitare il sito Web di Kaspersky.

Quando la licenza commerciale scade, le funzionalità principali dell'applicazione vengono disabilitate. Per continuare a utilizzare l'applicazione, è necessario rinnovare la licenza commerciale. Se non si prevede di rinnovare la licenza, è necessario rimuovere l'applicazione dal computer.

Informazioni sul certificato di licenza

Un *certificato di licenza* è un documento trasferito all'utente insieme a un file chiave o a un codice di attivazione.

Il certificato di licenza contiene le seguenti informazioni di licenza:

- ID di licenza o numero dell'ordine.
- Dettagli dell'utente al quale è stata concessa la licenza.
- Dettagli dell'applicazione che può essere attivata utilizzando la licenza.
- Limitazione sul numero di unità concesse in licenza (ad esempio, il numero di dispositivi nei quali l'applicazione può essere utilizzata con la licenza).
- Data di inizio del periodo licenza.
- Data di scadenza della licenza o periodo licenza.
- Tipo di licenza.

Informazioni sull'abbonamento

Un *abbonamento per Kaspersky Endpoint Security* è un ordine di acquisto per l'applicazione con specifici parametri (ad esempio la data di scadenza dell'abbonamento e il numero di dispositivi protetti). È possibile ordinare un abbonamento per Kaspersky Endpoint Security dal fornitore del servizio (ad esempio il proprio provider di servizi Internet). Un abbonamento può essere rinnovato manualmente o automaticamente oppure è possibile annullare l'abbonamento. È possibile gestire l'abbonamento nel sito Web del fornitore del servizio.

L'abbonamento può essere limitato (ad esempio, per un anno) o illimitato (senza una data di scadenza). Per continuare a utilizzare Kaspersky Endpoint Security dopo la scadenza del periodo di validità di un abbonamento limitato, è necessario rinnovare l'abbonamento. Un abbonamento illimitato viene rinnovato automaticamente se si effettua il pagamento dei servizi del fornitore entro il termine previsto.

Allo scadere di un abbonamento limitato, è possibile usufruire di un periodo di tolleranza per il rinnovo dell'abbonamento durante il quale l'applicazione continua a funzionare. La disponibilità e la durata di tale periodo di tolleranza vengono stabilite dal provider di servizi.

Per utilizzare Kaspersky Endpoint Security con un abbonamento, è necessario applicare il codice di attivazione ricevuto dal fornitore del servizio. Una volta applicato il codice di attivazione, la chiave attiva viene aggiunta. La chiave attiva determina la licenza per l'utilizzo dell'applicazione con l'abbonamento. Non è possibile attivare l'applicazione in abbonamento utilizzando un file chiave. Il provider di servizi può fornire solo un codice di attivazione. Non è possibile aggiungere una chiave di riserva con un abbonamento.

I codici di attivazione acquistati con un abbonamento non possono essere utilizzati per attivare le versioni precedenti di Kaspersky Endpoint Security.

Informazioni sulla chiave di licenza

Una *chiave di licenza* è una sequenza di bit che è possibile utilizzare per attivare e quindi utilizzare l'applicazione in conformità con i termini del Contratto di licenza con l'utente finale.

Per una chiave aggiunta con un abbonamento non viene fornito alcun certificato di licenza.

È possibile aggiungere una chiave di licenza all'applicazione applicando un file chiave o inserendo un codice di attivazione.

La chiave può essere bloccata da Kaspersky in caso di violazione delle condizioni del Contratto di licenza con l'utente finale. Se la chiave è stata bloccata, è necessario aggiungere una chiave diversa per continuare a utilizzare l'applicazione.

Esistono due tipi di chiavi: attiva e di riserva.

Una *chiave attiva* è una chiave attualmente utilizzata dall'applicazione. Come chiave attiva può essere aggiunta una licenza di prova o commerciale. L'applicazione non può disporre di più di una chiave attiva.

Una *chiave di riserva* è una chiave che consente all'utente di utilizzare l'applicazione pur non essendo attualmente in uso. Allo scadere della chiave attiva diventa automaticamente attiva una chiave di riserva. Una chiave di riserva può essere aggiunta solo se la chiave attiva è disponibile.

Una chiave per una licenza di prova può essere aggiunta solo come chiave attiva. Non è possibile aggiungerla come chiave di riserva. La chiave di una licenza di prova non può sostituire la chiave attiva di una licenza commerciale.

Se una chiave viene aggiunta all'elenco delle chiavi vietate, la funzionalità dell'applicazione definita dalla licenza utilizzata per attivare l'applicazione rimane disponibile per otto giorni. L'applicazione informa l'utente che la chiave è stata aggiunta all'elenco delle chiavi vietate. Dopo otto giorni, le funzionalità dell'applicazione diventano limitate al livello di funzionalità disponibile dopo la scadenza della licenza. È possibile utilizzare i componenti di protezione e controllo ed eseguire una scansione utilizzando i database dell'applicazione installati prima della scadenza della licenza. L'applicazione continua inoltre a criptare i file modificati e criptati prima della scadenza della licenza, ma non cripta nuovi file. L'utilizzo di Kaspersky Security Network non è disponibile.

Informazioni sul codice di attivazione

Un *codice di attivazione* è una sequenza univoca di 20 caratteri alfanumerici. Si immette un codice di attivazione per aggiungere una chiave di licenza che attiva Kaspersky Endpoint Security. Si riceve un codice di attivazione all'indirizzo e-mail specificato dopo l'acquisto di Kaspersky Endpoint Security.

Per attivare l'applicazione con un codice di attivazione, è necessario l'accesso a Internet per eseguire la connessione ai server di attivazione di Kaspersky.

Quando l'applicazione viene attivata tramite un codice di attivazione, viene aggiunta la chiave attiva. Una chiave di riserva può essere aggiunta solo utilizzando un codice di attivazione e non può essere aggiunta utilizzando un file chiave.

Se un codice di attivazione viene smarrito dopo l'attivazione dell'applicazione, è possibile ripristinarlo. Un codice di attivazione può ad esempio essere necessario per registrare un Kaspersky CompanyAccount. Se il codice di attivazione viene smarrito dopo l'attivazione dell'applicazione, contattare il partner di Kaspersky presso cui è stata acquistata la licenza.

Informazioni sul file chiave

Un *file chiave* è un file con estensione .key che si riceve da Kaspersky. Lo scopo di un file chiave è quello di aggiungere una chiave di licenza per l'attivazione dell'applicazione.

Si riceve un file chiave all'indirizzo e-mail fornito al momento dell'acquisto di Kaspersky Endpoint Security o quando è stata ordinata la versione di prova di Kaspersky Endpoint Security.

Non è necessario connettersi ai server di attivazione di Kaspersky per attivare l'applicazione con un file chiave.

È possibile ripristinare un file chiave eliminato accidentalmente. Un file chiave potrebbe ad esempio essere necessario per eseguire la registrazione a Kaspersky CompanyAccount.

Per ripristinare un file chiave, eseguire una delle seguenti operazioni:

- Contattare il venditore della licenza.
- Ottenere un file chiave sul sito Web di Kaspersky, in base al codice di attivazione esistente.
- Ottenere un file chiave da un altro Administration Server.

Quando l'applicazione viene attivata tramite un file chiave, viene aggiunta una chiave attiva. Una chiave di riserva può essere aggiunta solo utilizzando un file chiave e non può essere aggiunta tramite un codice di attivazione.

Confronto delle funzionalità dell'applicazione in base al tipo di licenza per le workstation

La serie di funzionalità Kaspersky Endpoint Security disponibili nelle workstation dipende dal tipo di licenza (vedere la tabella seguente).

[Consultare anche il confronto delle funzionalità delle applicazioni per i server]

Confronto delle funzionalità dell'applicazione a seconda del tipo di licenza di Kaspersky Next. Vedere in Guida di Kaspersky Next.

Confronto delle funzionalità Kaspersky Endpoint Security

Funzionalità	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Protezione minacce avanzata								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Rilevamento del Comportamento	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Prevenzione Exploit	✓	✓	✓	✓	✓	✓	✓	✓
Prevenzione Intrusioni Host	✓	✓	✓	✓	✓	✓	✓	✓
Motore di Remediation	✓	✓	✓	✓	✓	✓	✓	✓
Protezione minacce essenziale								
Protezione minacce file	✓	✓	✓	✓	✓	✓	✓	✓
Protezione minacce Web	✓	✓	✓	✓	✓	✓	✓	✓
Protezione minacce di posta	✓	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Protezione minacce di rete	✓	✓	✓	✓	✓	✓	✓	✓
Prevenzione Attacchi BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Protezione AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Controlli di sicurezza								
Log Inspection	–	–	–	–	–	–	–	–
Controllo applicazioni	✓	✓	✓	✓	✓	✓	✓	✓
Controllo dispositivi	✓	✓	✓	✓	✓	✓	✓	✓
Controllo Web	✓	✓	✓	✓	✓	✓	✓	✓
Controllo adattivo delle anomalie	–	✓	✓	✓	✓	✓	–	✓
Monitoraggio integrità di sistema	–	–	–	–	–	–	–	–
Criptaggio dei dati								
Criptaggio disco Kaspersky	–	✓	✓	✓	✓	✓	–	✓

Funzionalità	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Crittografia unità BitLocker	–	✓	✓	✓	✓	✓	–	✓
Criptaggio a livello di file	–	✓	✓	✓	✓	✓	–	✓
Criptaggio unità rimovibili	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(La licenza Kaspersky Sandbox deve essere acquistata separatamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Integrazione con KUMA *(la licenza per l'integrazione di KUMA deve essere acquistata separatamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Modalità Light Agent *(per attivare l'applicazione, è necessario aggiungere una chiave di licenza alla SVM a cui è connesso Light Agent)*	–	–	–	–	–	–	✓	✓

Confronto delle funzionalità dell'applicazione in base al tipo di licenza per i server

La serie di funzionalità Kaspersky Endpoint Security disponibili nei server dipende dal tipo di licenza (vedere la tabella seguente).

Consultare anche il confronto delle funzionalità delle applicazioni per le workstation

Confronto delle funzionalità dell'applicazione a seconda del tipo di licenza di Kaspersky Next. Vedere in Guida di Kaspersky Next.

Funzionalità	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Protezione minacce avanzata								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Rilevamento del Comportamento	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
Prevenzione Exploit	✓	✓	✓	✓	✓	✓	✓	✓
Prevenzione Intrusioni Host	–	–	–	–	–	–	–	–
Motore di Remediation	✓	✓	✓	✓	✓	✓	✓	✓
Protezione minacce essenziale								
Protezione minacce file	✓	✓	✓	✓	✓	✓	✓	✓
Protezione minacce Web	–	✓	✓	✓	✓	✓	✓	✓
Protezione minacce di posta	–	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Protezione minacce di rete	✓	✓	✓	✓	✓	✓	✓	✓
Prevenzione Attacchi BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
Protezione AMSI	✓	✓	✓	✓	✓	✓	✓	✓
Controlli di sicurezza								
Log Inspection	–	–	–	–	–	–	–	✓
Controllo applicazioni	–	✓	✓	✓	✓	✓	–	✓
Controllo dispositivi	–	✓	✓	✓	✓	✓	✓	✓
Controllo Web	–	✓	✓	✓	✓	✓	✓	✓
Controllo adattivo delle anomalie	–	–	–	–	–	–	–	–
Monitoraggio integrità di sistema	–	–	–	–	–	–	–	✓
Criptaggio dei dati								
Criptaggio disco Kaspersky	–	–	–	–	–	–	–	–
Crittografia unità BitLocker	–	✓	✓	✓	✓	✓	–	✓
Criptaggio a livello di file	–	–	–	–	–	–	–	–
Criptaggio unità rimovibili	–	–	–	–	–	–	–	–

Funzionalità	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(La licenza Kaspersky Sandbox deve essere acquistata separatamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Integrazione con KUMA *(la licenza per l'integrazione di KUMA deve essere acquistata separatamente)*	✓	✓	✓	✓	✓	✓	✓	✓
Modalità Light Agent *(per attivare l'applicazione, è necessario aggiungere una chiave di licenza alla SVM a cui è connesso Light Agent)*	–	–	–	–	–	–	✓	✓

Attivazione dell'applicazione

L'*attivazione* è il processo di attivazione di una licenza che, fino alla scadenza, consente di utilizzare tutte le funzionalità dell'applicazione. L'attivazione dell'applicazione implica l'aggiunta di una chiave di licenza.

È possibile attivare l'applicazione in uno dei seguenti modi:

- Localmente dall'interfaccia dell'applicazione, utilizzando l'Attivazione guidata. In questo modo è possibile aggiungere sia la chiave attiva che la chiave di riserva.
- In remoto utilizzando il software Kaspersky Security Center.
  - Utilizzando l'attività *Aggiungi chiave*.

    Questo metodo consente di aggiungere una chiave a un computer specifico o ai computer appartenenti a un gruppo di amministrazione. In questo modo è possibile aggiungere sia la chiave attiva che la chiave di riserva.
  - Distribuendo ai computer una chiave memorizzata in Kaspersky Security Center Administration Server.

    Questo metodo consente di aggiungere automaticamente una chiave nei computer già connessi a Kaspersky Security Center e nei nuovi computer. Per utilizzare questo metodo, è prima necessario aggiungere la chiave a Kaspersky Security Center Administration Server. Per informazioni dettagliate sull'aggiunta di chiavi a Kaspersky Security Center Administration Server, consultare la Guida di Kaspersky Security Center.

Viene innanzitutto distribuito il codice di attivazione acquistato con l'abbonamento.

- Aggiungendo la chiave al pacchetto di installazione di Kaspersky Endpoint Security.

  Questo metodo consente di aggiungere la chiave nelle proprietà del pacchetto di installazione durante la distribuzione di Kaspersky Endpoint Security. L'applicazione viene attivata automaticamente dopo l'installazione.

- Utilizzando la riga di comando.

L'attivazione dell'applicazione tramite un codice di attivazione può richiedere un certo tempo, sia durante l'installazione remota che non interattiva, per via della distribuzione del carico tra i server di attivazione di Kaspersky. Se è necessario attivare immediatamente l'applicazione, è possibile interrompere il processo di attivazione in corso e avviare l'attivazione mediante l'Attivazione guidata.

Se Kaspersky Endpoint Security viene utilizzato in modalità Light Agent per proteggere gli ambienti virtuali, non è necessario attivare l'applicazione separatamente.

Attivazione dell'applicazione

Come attivare l'applicazione in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Aggiungi chiave**.

Passaggio 2. Aggiunta di una chiave

Immettere un codice di attivazione o selezionare un file chiave.

Per informazioni dettagliate sull'aggiunta di chiavi all'archivio di Kaspersky Security Center, consultare la Guida di Kaspersky Security Center.

Passaggio 3. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 4. Configurazione di una pianificazione di avvio dell'attività

Configurare una pianificazione per l'avvio di un'attività, ad esempio manualmente o quando il computer è inattivo.

Passaggio 5. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Attiva Kaspersky Endpoint Security for Windows*.

Passaggio 6. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività. In seguito a questa operazione, Kaspersky Endpoint Security verrà attivato nei computer degli utenti in modalità automatica.

Come attivare l'applicazione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Configurazione delle impostazioni generali dell'attività

Configurare le impostazioni generali dell'attività:

1. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.
2. Nell'elenco a discesa **Tipo di attività**, selezionare **Aggiungi chiave**.
3. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Attivazione di Kaspersky Endpoint Security for Windows*.
4. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività. Procedere con il passaggio successivo.

Passaggio 2. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 3. Selezione di una licenza

Selezionare la licenza che si desidera utilizzare per attivare l'applicazione. Procedere con il passaggio successivo.

È possibile aggiungere chiavi a Web Console (**Operazioni** → **Licensing**).

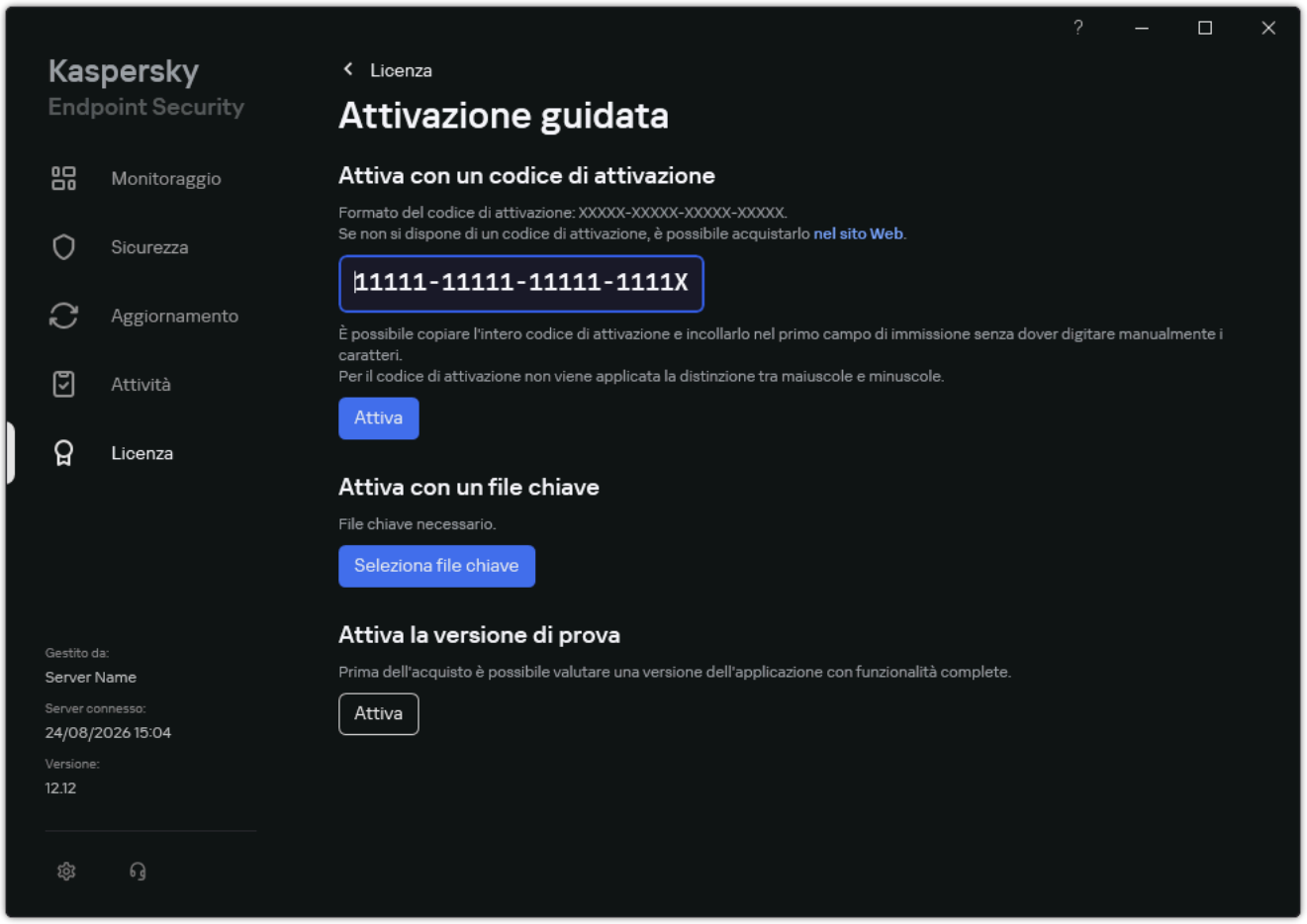
Passaggio 4. Completamento della creazione dell'attività

Terminare la procedura guidata facendo clic sul pulsante **Fine**. Verrà visualizzata una nuova attività nell'elenco delle attività. Per eseguire un'attività, selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**. In seguito a questa operazione, Kaspersky Endpoint Security verrà attivato nei computer degli utenti in modalità automatica.

Come attivare l'applicazione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Licenza**.
2. Fare clic su **Attiva l'applicazione utilizzando una nuova licenza**.

Verrà avviata l'Attivazione guidata dell'applicazione. Attenersi alle istruzioni dell'Attivazione guidata.



Attivazione dell'applicazione

Nelle proprietà dell'attività *Aggiungi chiave* è possibile aggiungere una chiave di riserva al computer. Una *chiave di riserva* diventa attiva quando la chiave attiva scade. La disponibilità di una chiave di riserva consente di evitare limitazioni delle funzionalità dell'applicazione allo scadere di una licenza.

Come aggiungere automaticamente una chiave di licenza ai computer tramite Administration Console (MMC)

1. In Administration Console, passare alla cartella **Licenze di Kaspersky**.

   Viene visualizzato un elenco di chiavi di licenza.

2. Aprire le proprietà della chiave di licenza.

3. Nella sezione **Generale**, selezionare la casella di controllo **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

4. Salvare le modifiche.

   In seguito a questa operazione, la chiave verrà distribuita automaticamente ai computer appropriati. Durante la distribuzione automatica di una chiave come chiave attiva o di riserva, viene preso in considerazione il limite di licenze relativo al numero di computer (impostato nelle proprietà della chiave). Se viene raggiunto il limite di licenze, la distribuzione di questa chiave ai computer si interrompe automaticamente. È possibile visualizzare il numero di computer in cui la chiave è stata aggiunta e altri dati nelle proprietà della chiave nella sezione **Dispositivi**.

Come aggiungere automaticamente una chiave di licenza ai computer tramite Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Operazioni → Licensing → Licenze**.

   Viene visualizzato un elenco di chiavi di licenza.

2. Aprire le proprietà della chiave di licenza.

3. Nella scheda **Generali**, abilitare l'interruttore **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

4. Salvare le modifiche.

In seguito a questa operazione, la chiave verrà distribuita automaticamente ai computer appropriati. Durante la distribuzione automatica di una chiave come chiave attiva o di riserva, viene preso in considerazione il limite di licenze relativo al numero di computer (impostato nelle proprietà della chiave). Se viene raggiunto il limite di licenze, la distribuzione di questa chiave ai computer si interrompe automaticamente. È possibile visualizzare il numero di computer in cui la chiave è stata aggiunta e altri dati nelle proprietà della chiave della scheda **Dispositivi**.

Se si attiva l'applicazione con un *codice di attivazione*, è necessario l'accesso a Internet per eseguire la connessione ai server di attivazione di Kaspersky. Se si attiva l'applicazione con un *file chiave*, l'accesso a Internet non è necessario. Se i computer si trovano in un segmento di rete isolato senza accesso a Internet, per attivare l'applicazione con un codice è necessario consentire l'utilizzo di Kaspersky Security Center Administration Server come server proxy. In altre parole, l'applicazione può ottenere l'accesso ai server di attivazione tramite l'Administration Server con accesso a Internet.

Come consentire l'utilizzo di Administration Server come server proxy per l'attivazione dell'applicazione in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Impostazioni generali → Impostazioni applicazione**.

4. Selezionare la casella di controllo **Usa Kaspersky Security Center come server proxy per l'attivazione**.

5. Salvare le modifiche.

Come consentire l'utilizzo di Administration Server come server proxy per l'attivazione dell'applicazione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali → Integrazione KSC**.

5. Selezionare la casella di controllo **Usa Kaspersky Security Center come server proxy per l'attivazione**.

6. Salvare le modifiche.

Se non è possibile attivare l'applicazione con un *codice di attivazione*, è possibile provare a ottenere un *file chiave* utilizzando la soluzione Kaspersky e tentando di attivare nuovamente l'applicazione utilizzando un metodo diverso.

Monitoraggio dell'utilizzo della licenza

È possibile monitorare l'utilizzo delle licenze nei seguenti modi:

- Visualizzare il *Rapporto sull'utilizzo delle chiavi di licenza* per l'infrastruttura dell'organizzazione (**Monitoraggio** → **Rapporti**).
- Visualizzare gli stati dei computer nella scheda **Dispositivi gestiti** → **Dispositivi**. Se l'applicazione non viene attivata, il computer avrà lo stato ⚠ *L'applicazione non è stata attivata*.
- Visualizzare le informazioni relative alla licenza nelle proprietà del computer.
- Visualizza le proprietà della chiave (**Operazioni** → **Licensing**).

Specifiche dell'attivazione dell'applicazione come parte di Kaspersky Security Center Cloud Console

Viene fornita una versione di prova per Kaspersky Security Center Cloud Console. La *versione di prova* è una versione speciale di Kaspersky Security Center Cloud Console progettata per fare in modo che un utente acquisisca familiarità con le funzionalità dell'applicazione. In questa versione è possibile eseguire azioni in un'area di lavoro per un periodo di 30 giorni. Tutte le applicazioni gestite vengono eseguite automaticamente con una licenza di prova per Kaspersky Security Center Cloud Console, tra cui Kaspersky Endpoint Security. Tuttavia, non è possibile attivare Kaspersky Endpoint Security utilizzando la propria licenza di prova allo scadere della licenza di prova per Kaspersky Security Center Cloud Console. Per informazioni dettagliate sulla gestione delle licenze di Kaspersky Security Center, consultare la Guida di Kaspersky Security Center Cloud Console.

La versione di prova di Kaspersky Security Center Cloud Console non consente di passare successivamente a una versione commerciale. Tutte le aree di lavoro di prova verranno automaticamente eliminate con i relativi contenuti allo scadere del periodo di 30 giorni.

Rimozione di una chiave di licenza

Per rimuovere una chiave di licenza, è necessario eseguire un'attività speciale nei computer. È ad esempio possibile rimuovere una chiave di licenza per riorganizzare le unità di licenza. Inoltre, quando la licenza scade, Kaspersky Endpoint Security invia una notifica. Se è stata aggiunta una chiave di licenza a breve termine per provare l'applicazione (ad esempio EDR Optimum Add-on), è possibile rimuovere questa chiave di licenza per eliminare le notifiche e correggere lo stato del computer.

L'attività *Rimuovi chiave* consente di rimuovere eventuali chiavi di licenza dal computer. È possibile rimuovere chiavi di licenza attive e chiavi di licenza di riserva. Oltre alla chiave di licenza di attivazione di Kaspersky Endpoint Security, è possibile rimuovere singole chiavi di licenza delle soluzioni Kaspersky Detection and Response (ad esempio, EDR Optimum Add-on).

Come rimuovere una chiave di licenza in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Rimuovi chiave**.

Passaggio 2. Selezione di una licenza

Selezionare la chiave di licenza che si desidera eliminare. È possibile selezionare una chiave di licenza dall'archivio di chiavi di Kaspersky Security Center o selezionare un file chiave.

Passaggio 3. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 4. Configurazione di una pianificazione di avvio dell'attività

Configurare una pianificazione per l'avvio di un'attività, ad esempio manualmente o quando il computer è inattivo.

Passaggio 5. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Rimuovi chiave per beta*.

Passaggio 6. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come rimuovere una chiave di licenza in Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Configurazione delle impostazioni generali dell'attività

Configurare le impostazioni generali dell'attività:

1. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.
2. Nell'elenco a discesa **Tipo di attività**, selezionare **Rimuovi chiave**.
3. Nel campo **Nome attività**, immettere una breve descrizione, ad esempio *Rimuovi chiave per beta*.
4. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività. Procedere con il passaggio successivo.

Passaggio 2. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 3. Selezione di una licenza

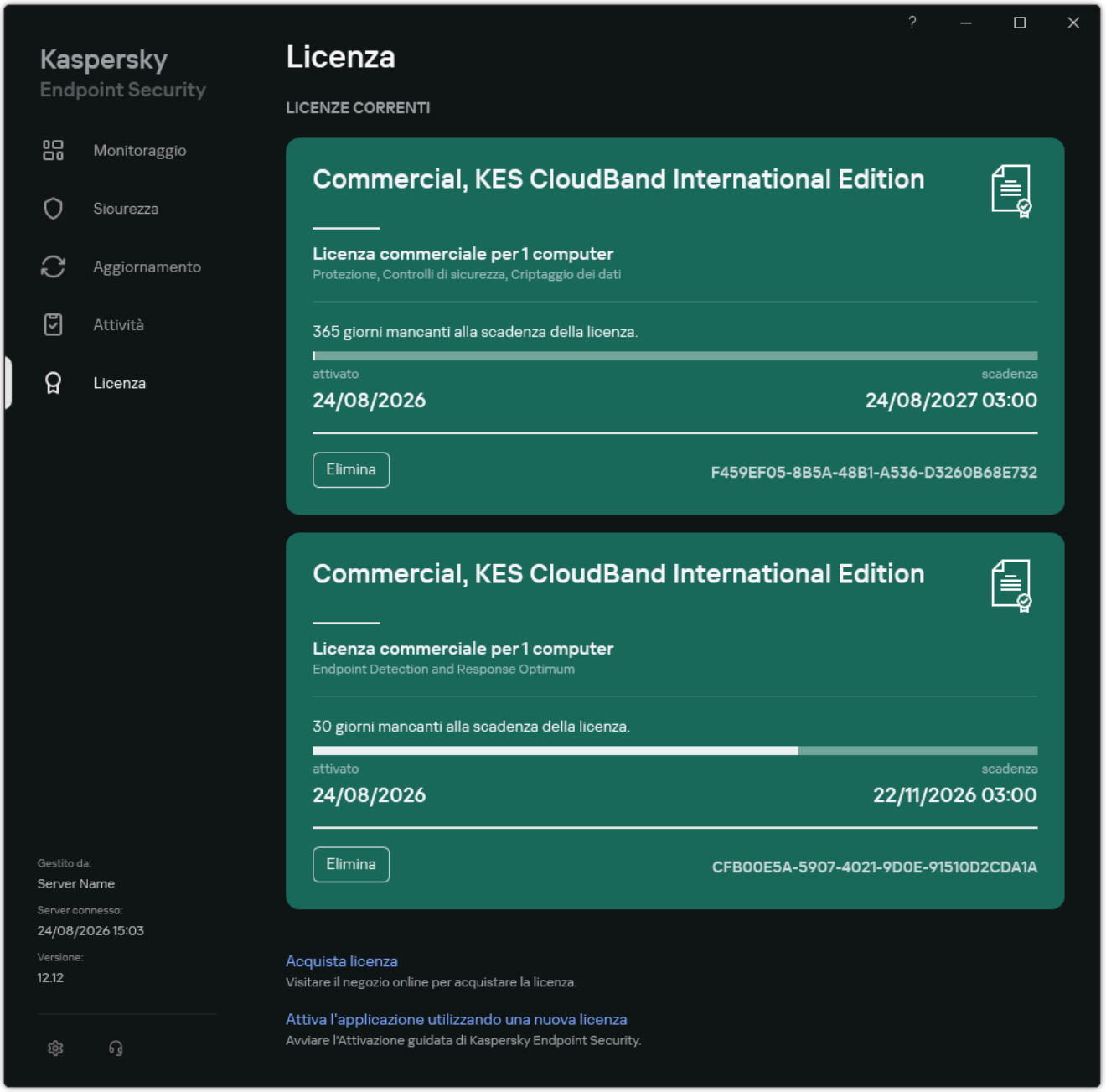
Selezionare la chiave di licenza che si desidera eliminare. È possibile selezionare una chiave di licenza dall'archivio di chiavi di Kaspersky Security Center o selezionare un file chiave. Procedere con il passaggio successivo.

Passaggio 4. Completamento della creazione dell'attività

Terminare la procedura guidata facendo clic sul pulsante **Fine**. Verrà visualizzata una nuova attività nell'elenco delle attività. Per eseguire un'attività, selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**.

Come rimuovere una chiave di licenza nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Licenza**.
2. Selezionare la chiave che si desidera eliminare e fare clic su **Elimina**.



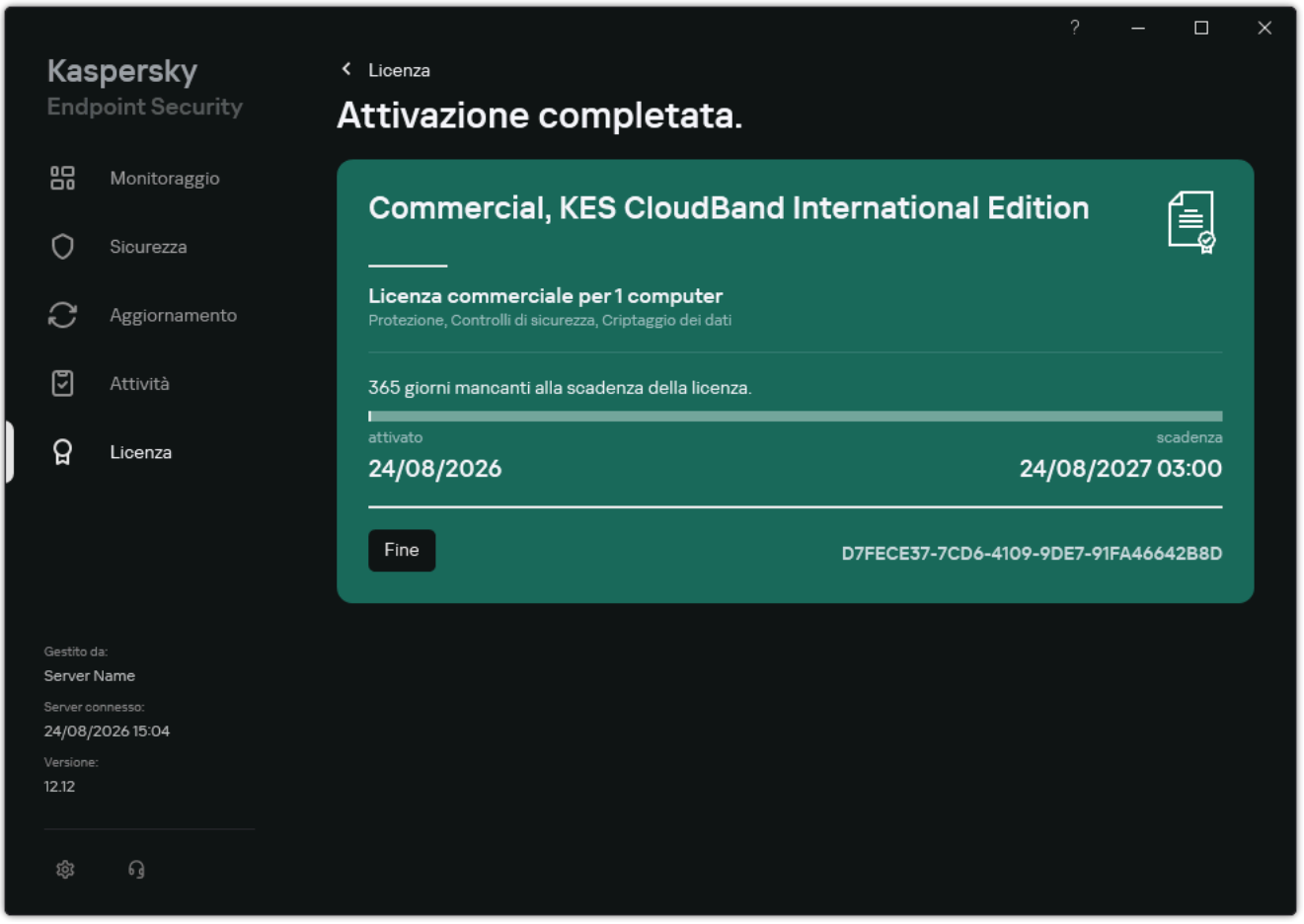
Finestra Gestione delle licenze

È inoltre possibile rimuovere una chiave di licenza dalla riga di comando.

Visualizzazione delle informazioni sulla licenza

Per visualizzare le informazioni su una licenza:

Nella finestra principale dell'applicazione, passare alla sezione **Licenza** (vedere la figura riportata di seguito).



Finestra Gestione delle licenze

La sezione mostra i seguenti dettagli:

- *Stato della chiave*. In un computer possono essere archiviati diversi tasti. Esistono due tipi di chiavi: attiva e di riserva. L'applicazione non può disporre di più di una chiave attiva. Una chiave di riserva può diventare attiva solo dopo la scadenza della chiave attiva o dopo che la chiave viene eliminata facendo clic sul pulsante **Elimina**.
- *Nome applicazione*. Nome completo dell'applicazione Kaspersky acquistata.
- *Tipo di licenza*. Sono disponibili i seguenti tipi di licenze: licenza di prova e commerciale.
- *Funzionalità*. Funzionalità dell'applicazione disponibili con la licenza. Le funzionalità possono includere Protezione, Controlli di sicurezza, Criptaggio dei dati e altro ancora. L'elenco delle funzionalità disponibili è specificato anche nel Certificato di licenza.

- *Informazioni aggiuntive sulla licenza*. Data di inizio e data di fine del periodo della licenza (solo per la chiave attiva), durata residua del termine della licenza.

  L'ora di scadenza della licenza è visualizzata in base al fuso orario configurato nel sistema operativo.

- *Chiave*. Una chiave è una sequenza alfanumerica univoca generata da un codice di attivazione o da un file chiave.

Nella finestra Gestione delle licenze è inoltre possibile eseguire una delle seguenti operazioni:

- **Acquista licenza/Rinnova la licenza**. Viene aperto il sito Web del negozio online Kaspersky in cui è possibile acquistare o rinnovare una licenza. A tale scopo, immettere le informazioni sull'azienda e pagare l'ordine.

- **Attiva l'applicazione utilizzando una nuova licenza**. Verrà avviata l'Attivazione guidata dell'applicazione. In questa procedura guidata è possibile aggiungere una chiave utilizzando un codice di attivazione o un file chiave. L'Attivazione guidata dell'applicazione consente di aggiungere una chiave attiva e solo una chiave di riserva.

Acquisto di una licenza

È possibile acquistare una licenza dopo l'installazione dell'applicazione. Al momento dell'acquisto di una licenza, l'utente riceve un codice di attivazione o un file chiave per l'attivazione dell'applicazione.

Per acquistare una licenza:

1. Nella finestra principale dell'applicazione, andare alla sezione **Licenza**.

2. Eseguire una delle seguenti operazioni:

   - Se non è stata aggiunta alcuna chiave o è stata aggiunta una chiave per una licenza di prova, fare clic sul pulsante **Acquista licenza**.

   - Se è stata aggiunta una chiave per una licenza commerciale, fare clic sul pulsante **Rinnova la licenza**.

   Verrà visualizzata una finestra con il sito Web del negozio online di Kaspersky, in cui è possibile acquistare una licenza.

Rinnovo dell'abbonamento

Quando si utilizza l'applicazione con un abbonamento, Kaspersky Endpoint Security contatta automaticamente il server di attivazione a intervalli specifici fino alla scadenza dell'abbonamento.

Se si utilizza l'applicazione con un abbonamento illimitato, Kaspersky Endpoint Security controlla automaticamente in background il server di attivazione per verificare se sono presenti chiavi rinnovate. Se è disponibile una chiave nel server di attivazione, l'applicazione la aggiunge sostituendo la chiave precedente. In questo modo, l'abbonamento illimitato per Kaspersky Endpoint Security viene rinnovato senza l'intervento dell'utente.

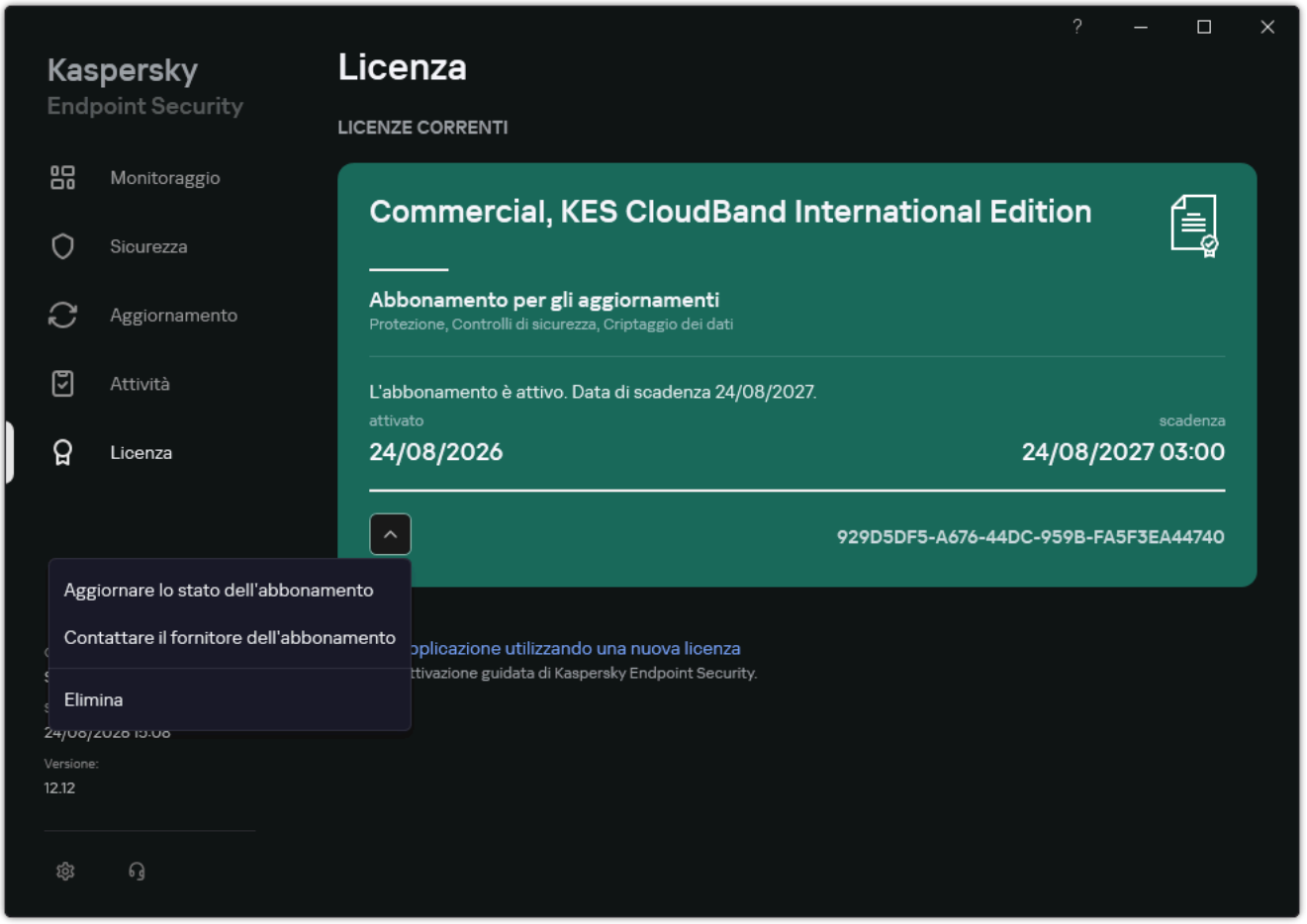
Se si utilizza l'applicazione con un abbonamento limitato, alla data di scadenza dell'abbonamento (o alla data di scadenza del periodo di tolleranza per il rinnovo dell'abbonamento), Kaspersky Endpoint Security invia una notifica in merito e interrompe i tentativi di rinnovo automatico dell'abbonamento. In questo caso, il funzionamento di Kaspersky Endpoint Security è lo stesso che si presenta in caso di scadenza della licenza commerciale per l'applicazione: l'applicazione viene eseguita senza aggiornamenti e Kaspersky Security Network non è disponibile.

È possibile rinnovare l'abbonamento nel sito Web del fornitore del servizio.

Per aprire il sito Web del fornitore del servizio dall'interfaccia dell'applicazione:

1. Nella finestra principale dell'applicazione, andare alla sezione **Licenza**.
2. Fare clic su **Contattare il fornitore dell'abbonamento**.

È possibile aggiornare lo stato dell'abbonamento manualmente. Questo può essere necessario se l'abbonamento è stato rinnovato dopo il periodo di tolleranza e l'applicazione non ha aggiornato lo stato dell'abbonamento automaticamente.



Rinnovo dell'abbonamento

Guida introduttiva

Dopo l'installazione di Kaspersky Endpoint Security, è possibile gestire l'applicazione utilizzando le seguenti interfacce:

- Interfaccia locale dell'applicazione.
- Kaspersky Security Center Administration Console.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Kaspersky Security Center Administration Console

Kaspersky Security Center consente di installare e disinstallare in remoto, avviare e interrompere Kaspersky Endpoint Security, configurare le impostazioni dell'applicazione, modificare il set di componenti dell'applicazione disponibili, aggiungere chiavi e avviare e interrompere attività di aggiornamento e scansione.

L'applicazione può essere gestita tramite Kaspersky Security Center, utilizzando il plug-in di gestione di Kaspersky Endpoint Security.

Per informazioni dettagliate sulla gestione dell'applicazione tramite Kaspersky Security Center, consultare la Guida di Kaspersky Security Center.

Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (di seguito denominata anche *Web Console*). Si tratta di un'interfaccia Web per la gestione di un sistema di protezione basato sulle applicazioni Kaspersky. È possibile utilizzare Kaspersky Security Center Web Console tramite un browser su qualsiasi dispositivo. Per informazioni dettagliate su Kaspersky Security Center Web Console, consultare la Guida di Kaspersky Security Center.

Kaspersky Security Center Cloud Console (di seguito denominato anche "*Cloud Console*") è una soluzione basata sul cloud per la protezione e la gestione della rete di un'organizzazione. Per informazioni dettagliate su Kaspersky Security Center Cloud Console, consultare la Guida di Kaspersky Security Center Cloud Console.

Web Console e Cloud Console consentono di eseguire le seguenti operazioni:

- Monitorare lo stato del sistema di sicurezza aziendale.
- Installare le applicazioni Kaspersky nei dispositivi della rete.
- Gestire le applicazioni installate.
- Visualizzare i rapporti sullo stato del sistema di sicurezza.

La gestione di Kaspersky Endpoint Security tramite Web Console, Cloud Console e Kaspersky Security Center Administration Console offre funzionalità di gestione diverse. I componenti e le attività disponibili variano anche per le diverse console.

Informazioni sul plug-in di gestione di Kaspersky Endpoint Security for Windows

Il plug-in di gestione di Kaspersky Endpoint Security for Windows consente l'interazione tra Kaspersky Endpoint Security e Kaspersky Security Center. Il plug-in di gestione consente di gestire Kaspersky Endpoint Security utilizzando criteri, attività e impostazioni locali dell'applicazione. L'interazione con Kaspersky Security Center Web Console viene consentita dal plug-in Web.

La versione del plug-in di gestione può essere diversa dalla versione dell'applicazione Kaspersky Endpoint Security installata nel computer client. Se la versione installata del plug-in di gestione ha meno funzionalità della versione installata di Kaspersky Endpoint Security, le impostazioni delle funzioni mancanti non sono gestite dal plug-in di gestione. Queste impostazioni possono essere modificate dall'utente nell'interfaccia locale di Kaspersky Endpoint Security.

Per impostazione predefinita, il plug-in Web non è installato in Kaspersky Security Center Web Console. Il plug-in Web deve essere installato in un computer in cui è installato Kaspersky Security Center Web Console. La funzionalità del plug-in Web è disponibile per tutti gli amministratori che hanno accesso a Web Console in un browser. È possibile visualizzare l'elenco dei plug-in Web installati nell'interfaccia di Web Console (**Impostazioni della console** → **Plug-in Web**).

Se si utilizza Kaspersky Endpoint Security come parte della soluzione Kaspersky Endpoint Detection and Response Optimum, è necessario installare il plug-in di gestione di Kaspersky Endpoint Detection and Response. Per visualizzare i dettagli degli avvisi, è necessario il plug-in di gestione. *Dettagli avviso* è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Pertanto, per creare attività di reazione alle minacce, è necessario il plug-in di gestione di Kaspersky Endpoint Security e per visualizzare i dettagli degli avvisi è necessario il plug-in di gestione di EDR.

Installazione del plug-in Web

È possibile installare il plug-in Web nel seguente modo:

- Installare il plug-in Web utilizzando l'Avvio rapido guidato di Kaspersky Security Center Web Console.

  Web Console richiede automaticamente di eseguire l'Avvio rapido guidato al momento della prima connessione di Web Console ad Administration Server. È inoltre possibile eseguire l'Avvio rapido guidato nell'interfaccia di Web Console (**Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Avvio rapido guidato**). L'Avvio rapido guidato può anche verificare se i plug-in Web installati sono aggiornati e scaricare gli aggiornamenti necessari. Per ulteriori dettagli sull'Avvio rapido guidato di Kaspersky Security Center Web Console, consultare la Guida di Kaspersky Security Center.

- Installare il plug-in Web dall'elenco dei pacchetti di distribuzione disponibili in Web Console.

  Per installare il plug-in Web, selezionare il pacchetto di distribuzione del plug-in Web di Kaspersky Endpoint Security nell'interfaccia di Web Console (**Impostazioni della console** → **Plug-in Web**). L'elenco dei pacchetti di distribuzione disponibili viene aggiornato automaticamente dopo il rilascio delle nuove versioni delle applicazioni Kaspersky.

- Scaricare il pacchetto di distribuzione in Web Console da una sorgente esterna.

  Per installare il plug-in Web, aggiungere l'archivio ZIP del pacchetto di distribuzione per il plug-in Web di Kaspersky Endpoint Security nell'interfaccia di Web Console (**Impostazioni della console** → **Plug-in Web**). Il pacchetto di distribuzione del plug-in Web può ad esempio essere scaricato nel sito Web di Kaspersky.

A partire da Kaspersky Endpoint Security 12.11 for Windows, la procedura di installazione del plug-in Web è stata modificata. Il pacchetto di distribuzione ora include due plug-in Web: *Kaspersky Endpoint Security for Windows 14.2.0* e *Unified Protection and Management Plug-in*. Ciò è dovuto al passaggio a un singolo plug-in Web unificato per la gestione delle applicazioni Kaspersky. Il plug-in Web unificato consente di creare un singolo criterio per gestire più applicazioni Kaspersky (ad esempio, Kaspersky Endpoint Security for Windows, macOS e Linux). La transizione al plug-in Web unificato potrebbe richiedere diversi rilasci. Al termine della transizione, il pacchetto di distribuzione includerà solo *Unified Protection and Management Plug-in*.

Aggiornamento del plug-in di gestione

Per aggiornare il plug-in di gestione di Kaspersky Endpoint Security for Windows, scaricare la versione più recente del plug-in (inclusa nel kit di distribuzione) ed eseguire l'installazione guidata del plug-in.

Se viene resa disponibile una nuova versione del plug-in Web, Web Console visualizzerà la notifica *Sono disponibili aggiornamenti per i plug-in utilizzati*. È possibile procedere all'aggiornamento della versione del plug-in Web da questa notifica di Web Console. È inoltre possibile verificare manualmente la disponibilità di nuovi aggiornamenti del plug-in Web nell'interfaccia di Web Console (**Impostazioni della console** → **Plug-in Web**). La versione precedente del plug-in Web verrà automaticamente rimossa durante l'aggiornamento.

Quando il plug-in Web viene aggiornato, gli elementi già esistenti (ad esempio, criteri o attività) vengono salvati. Le nuove impostazioni degli elementi che implementano nuove funzioni di Kaspersky Endpoint Security verranno visualizzate negli elementi esistenti e avranno i valori predefiniti.

È possibile aggiornare il plug-in Web nel seguente modo:

- Aggiornare il plug-in Web nell'elenco dei plug-in Web in modalità online.

  Per aggiornare il plug-in Web, è necessario selezionare il pacchetto di distribuzione del plug-in Web di Kaspersky Endpoint Security nell'interfaccia di Web Console: **Impostazioni della console** → **Plug-in Web**. Web Console verifica la disponibilità degli aggiornamenti nei server di Kaspersky e scarica gli aggiornamenti rilevanti.

- Aggiornare il plug-in Web da un file.

  Per aggiornare il plug-in Web, è necessario selezionare l'archivio ZIP del pacchetto di distribuzione del plug-in Web di Kaspersky Endpoint Security nell'interfaccia di Web Console (**Impostazioni della console** → **Plug-in Web**). Il pacchetto di distribuzione del plug-in Web può ad esempio essere scaricato nel sito Web di Kaspersky. È possibile aggiornare il plug-in Web di Kaspersky Endpoint Security solo a una versione più recente. Il plug-in Web non può essere aggiornato a una versione precedente.

Se viene aperto qualsiasi elemento, ad esempio un criterio o un'attività, il plug-in Web verifica le informazioni sulla relativa compatibilità. Se la versione del plug-in Web è uguale o successiva alla versione specificata nelle informazioni relative alla compatibilità, è possibile modificare le impostazioni dell'elemento. In caso contrario, non è possibile utilizzare il plug-in Web per modificare le impostazioni dell'elemento selezionato. È consigliabile aggiornare il plug-in Web.

Considerazioni speciali in caso di utilizzo di versioni diverse dei plug-in di gestione

È possibile gestire Kaspersky Endpoint Security tramite Kaspersky Security Center solo se si dispone di un plug-in di gestione la cui versione è uguale o successiva a quella specificata nelle informazioni relative alla compatibilità di Kaspersky Endpoint Security con il plug-in di gestione. È possibile visualizzare la versione minima richiesta del plug-in di gestione nel file installer.ini incluso nel kit di distribuzione.

Se viene aperto qualsiasi elemento, ad esempio un criterio o un'attività, il plug-in di gestione controlla le informazioni sulla relativa compatibilità. Se la versione del plug-in di gestione è uguale o successiva alla versione specificata nelle informazioni relative alla compatibilità, è possibile modificare le impostazioni dell'elemento. In caso contrario, non è possibile utilizzare il plug-in di gestione per modificare le impostazioni dell'elemento selezionato. È consigliabile eseguire l'upgrade del plug-in di gestione.

Se il plug-in di gestione di Kaspersky Endpoint Security è installato in Administration Console, tenere conto dei seguenti aspetti durante l'installazione di una nuova versione del plug-in di gestione:

- La versione precedente del plug-in di gestione di Kaspersky Endpoint Security verrà rimossa.
- La nuova versione del plug-in di gestione di Kaspersky Endpoint Security supporta la gestione della versione precedente di Kaspersky Endpoint Security for Windows nei computer degli utenti.
- È possibile utilizzare la nuova versione del plug-in di gestione per modificare le impostazioni in criteri, attività e altri elementi creati dalla versione precedente del plug-in di gestione.
- Per le nuove impostazioni, la nuova versione del plug-in di gestione assegna i valori predefiniti quando si salva per la prima volta un criterio, un profilo criterio o un'attività.

  Dopo l'upgrade del plug-in di gestione è consigliabile verificare e salvare i valori delle nuove impostazioni nei criteri e nei profili criterio. Se non si esegue questa operazione, i nuovi gruppi di impostazioni di Kaspersky Endpoint Security nel computer dell'utente utilizzeranno i valori predefiniti e potranno essere modificati (attributo). È consigliabile verificare le impostazioni a partire dai criteri e dai profili criterio nel livello superiore della gerarchia. È inoltre consigliabile utilizzare l'account utente che dispone dei diritti di accesso a tutte le aree funzionali di Kaspersky Security Center.

  Per informazioni sulle nuove funzionalità dell'applicazione, fare riferimento alle note sulla versione o alla guida dell'applicazione.

- Se è stato aggiunto un nuovo parametro a un gruppo di impostazioni nella nuova versione del plug-in di gestione, lo stato definito precedentemente dell'attributo / per questo gruppo di impostazioni non viene modificato.

Considerazioni speciali quando si utilizzano protocolli criptati per l'interazione con servizi esterni

Kaspersky Endpoint Security e Kaspersky Security Center utilizzano un canale di comunicazione criptato con TLS (Transport Layer Security) per il funzionamento con i servizi esterni di Kaspersky. Kaspersky Endpoint Security utilizza servizi esterni per le seguenti funzionalità:

- aggiornamento di database e moduli software dell'applicazione;
- attivazione dell'applicazione con un codice di attivazione (attivazione 2.0);
- utilizzo di Kaspersky Security Network.

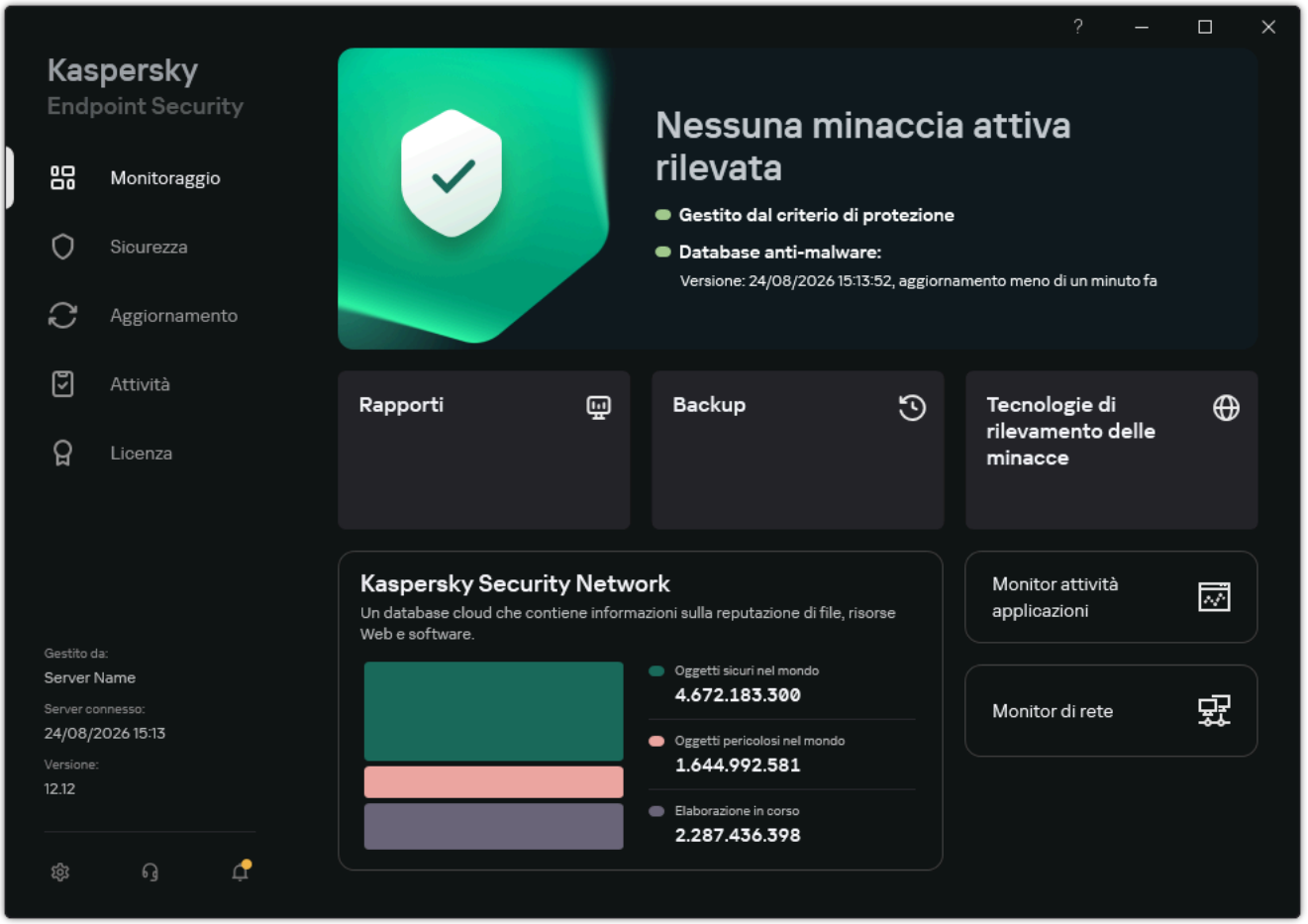
L'uso del canale TLS protegge l'applicazione fornendo le seguenti funzionalità:

- Criptaggio. I contenuti dei messaggi sono riservati e non vengono divulgati a utenti di terzi.
- Integrità. Il destinatario del messaggio è certo che il contenuto del messaggio non sia stato modificato da quando il messaggio è stato inoltrato dal mittente.
- Autenticazione. Il destinatario è certo che la comunicazione venga stabilita solo con un server Kaspersky attendibile.

Kaspersky Endpoint Security utilizza certificati a chiave pubblica per l'autenticazione del server. Per utilizzare i certificati è necessaria una PKI (Public Key Infrastructure). Un'autorità di certificazione fa parte di una PKI. Kaspersky utilizza la propria autorità di certificazione poiché i servizi Kaspersky sono altamente tecnici e non pubblici. In questo caso, quando i certificati radice di Thawte, VeriSign, GlobalTrust e altri vengono revocati, la PKI Kaspersky rimane operativa senza interruzioni.

Gli ambienti che dispongono di MITM (strumenti software e hardware che supportano l'analisi del protocollo HTTPS) sono considerati non sicuri da Kaspersky Endpoint Security. È possibile che si verifichino errori durante l'utilizzo dei servizi Kaspersky. Potrebbero ad esempio verificarsi errori relativi all'uso di Self-Signed Certificate. Questi errori potrebbero verificarsi perché uno strumento di ispezione HTTPS del proprio ambiente non riconosce la PKI Kaspersky. Per correggere questi problemi, è necessario configurare le esclusioni per l'interazione con i servizi esterni.

Interfaccia dell'applicazione



Finestra principale dell'applicazione

Monitoraggio	• **Rapporti**. Visualizzare gli eventi che si sono verificati durante il funzionamento dell'applicazione, dei singoli componenti e delle attività. • **Backup**. Visualizzare un elenco delle copie salvate dei file infetti eliminati dall'applicazione. • **Tecnologie di rilevamento delle minacce**. Visualizzare le informazioni sulle tecnologie di rilevamento delle minacce e il numero di minacce rilevate da queste tecnologie. • **Kaspersky Security Network**. Stato della connessione tra Kaspersky Endpoint Security e Kaspersky Security Network e statistiche KSN globali. *Kaspersky Security Network (KSN)* è un'infrastruttura di servizi cloud che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce risposte più rapide da parte di Kaspersky Endpoint Security alle nuove minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi positivi. Se si partecipa a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla reputazione degli indirizzi Web scansionati, nonché informazioni sulla categoria e sulla reputazione dei file scansionati. • **Monitor attività applicazioni**. Visualizzare le informazioni sul funzionamento delle applicazioni installate. Monitor attività applicazioni tiene traccia degli eventi associati all'applicazione relativi a file, registro di sistema e sistema operativo. • **Monitor di rete**. Visualizzare le informazioni sull'attività di rete del computer in tempo reale. • **Monitoraggio criptaggio**. Consente di monitorare il processo di criptaggio o decriptaggio del disco in tempo reale. Monitoraggio criptaggio è disponibile se è installato il componente Criptaggio disco Kaspersky o Crittografia unità BitLocker.
Sicurezza	Stato operativo dei componenti installati. È inoltre possibile procedere alla configurazione dei componenti o alla visualizzazione dei rapporti.
Aggiornamento	Gestire le attività di aggiornamento di Kaspersky Endpoint Security. È possibile aggiornare i database anti-virus e i moduli delle applicazioni ed eseguire il rollback dell'ultimo aggiornamento. Un amministratore può nascondere la sezione all'utente o limitare la gestione delle attività.
Attività	Gestire le attività di scansione di Kaspersky Endpoint Security. È possibile eseguire una scansione malware e un controllo dell'integrità dell'applicazione. Un amministratore può nascondere le attività a un utente o limitare la gestione delle attività.
Licenza	Licensing dell'applicazione. È possibile acquistare una licenza, attivare l'applicazione o rinnovare un abbonamento. È inoltre possibile visualizzare le informazioni sulla licenza corrente.

	Configura le impostazioni dell'applicazione. Un amministratore può vietare le modifiche delle impostazioni in Kaspersky Security Center.
	Informazioni sull'applicazione: versione corrente di Kaspersky Endpoint Security, data di rilascio dei database, chiave e altre informazioni. È inoltre possibile accedere alle risorse delle informazioni Kaspersky con informazioni utili, raccomandazioni e risposte alle domande frequenti sull'acquisto, l'installazione e l'utilizzo dell'applicazione.
	Messaggi contenenti informazioni sugli aggiornamenti disponibili e richieste di accesso a file e dispositivi criptati.

Icona dell'applicazione nell'area di notifica della barra delle applicazioni

Al termine dell'installazione di Kaspersky Endpoint Security, l'icona dell'applicazione viene visualizzata nell'area di notifica della barra delle applicazioni di Microsoft Windows.

Se l'icona dell'applicazione nell'area di notifica della barra delle applicazioni è nascosta, l'amministratore ha disabilitato la visualizzazione dell'interfaccia dell'applicazione nel criterio.

L'icona ha le seguenti funzioni:

- Indica l'attività dell'applicazione.
- Opera come collegamento per accedere al menu di scelta rapida e alla finestra principale dell'applicazione.

I seguenti stati dell'icona dell'applicazione vengono forniti per la visualizzazione delle informazioni sul funzionamento dell'applicazione:

- L'icona indica che tutti i componenti di protezione dell'applicazione di importanza critica sono abilitati. Kaspersky Endpoint Security visualizzerà un avviso se all'utente è richiesto di eseguire un'azione, ad esempio riavviare il computer dopo l'aggiornamento dell'applicazione.
- L'icona indica che tutti i componenti di protezione dell'applicazione di importanza critica sono disabilitati o non funzionano correttamente. I componenti di protezione potrebbero ad esempio non funzionare correttamente se la licenza è scaduta o a causa di un errore dell'applicazione. Kaspersky Endpoint Security visualizzerà un avviso con una descrizione del problema nella protezione del computer.

Il menu di scelta rapida dell'icona dell'applicazione contiene i seguenti elementi:

- **Kaspersky Endpoint Security for Windows**. Apre la finestra principale dell'applicazione. In questa finestra è possibile regolare il funzionamento dei componenti e delle attività dell'applicazione e visualizzare le statistiche relative ai file elaborati e alle minacce rilevate.
- **Sospendi la protezione/Ripristina protezione**. Consente di sospendere il funzionamento di tutti i componenti di protezione e controllo non contrassegnati da un lucchetto () nel criterio. Prima di eseguire questa operazione, è consigliabile disabilitare il criterio di Kaspersky Security Center.

  Prima di sospendere il funzionamento dei componenti di protezione e controllo, l'applicazione richiede la password per l'accesso a Kaspersky Endpoint Security (password dell'account o password temporanea). È quindi possibile selezionare il periodo di sospensione: per una specifica quantità di tempo, fino a un riavvio o su richiesta dell'utente.

  Questo elemento del menu di scelta rapida è disponibile se Protezione tramite password è abilitata. Per ripristinare il funzionamento dei componenti di protezione e controllo, fare clic su **Ripristina protezione** nel menu di scelta rapida dell'applicazione.

La sospensione del funzionamento dei componenti di protezione e controllo non influisce sulle prestazioni delle attività di aggiornamento e scansione malware. L'applicazione continua inoltre a utilizzare Kaspersky Security Network.

- **Disabilita criterio/Abilita criterio**. Disabilitazione di un criterio di Kaspersky Security Center nel computer. Tutte le impostazioni di Kaspersky Endpoint Security sono disponibili per la configurazione, incluse le impostazioni con un lucchetto chiuso nel criterio (). Se il criterio è disabilitato, l'applicazione richiede la password per l'accesso a Kaspersky Endpoint Security (password dell'account o password provvisoria). Questo elemento del menu di scelta rapida è disponibile se Protezione tramite password è abilitata. Per abilitare il criterio, selezionare **Abilita criterio** nel menu di scelta rapida dell'applicazione.

- **Impostazioni**. Apre la finestra delle impostazioni dell'applicazione.

- **Assistenza**. Si apre una finestra che contiene le informazioni necessarie per contattare l'Assistenza tecnica di Kaspersky.

- **Informazioni su**. Questo elemento apre una finestra di informazioni con i dettagli sull'applicazione.

- **Esci**. Questo elemento consente di uscire da Kaspersky Endpoint Security. Facendo clic su questa voce del menu di scelta rapida, l'applicazione viene scaricata dalla RAM del computer.



Menu di scelta rapida dell'icona dell'applicazione

Interfaccia dell'applicazione semplificata

Se un criterio di Kaspersky Security Center configurato per la visualizzazione dell'interfaccia dell'applicazione semplificata è applicato a un computer client in cui è installato Kaspersky Endpoint Security, la finestra principale dell'applicazione non è disponibile in tale computer client. Fare clic con il tasto destro del mouse per aprire il menu di scelta rapida dell'icona di Kaspersky Endpoint Security (vedere la figura di seguito) contenente i seguenti elementi:

- **Disabilita criterio/Abilita criterio**. Disabilitazione di un criterio di Kaspersky Security Center nel computer. Tutte le impostazioni di Kaspersky Endpoint Security sono disponibili per la configurazione, incluse le impostazioni con un lucchetto chiuso nel criterio (). Se il criterio è disabilitato, l'applicazione richiede la password per l'accesso a Kaspersky Endpoint Security (password dell'account o password provvisoria). Questo elemento del menu di scelta rapida è disponibile se Protezione tramite password è abilitata. Per abilitare il criterio, selezionare **Abilita criterio** nel menu di scelta rapida dell'applicazione.

- **Attività**. Elenco a discesa contenente i seguenti elementi:

  - **Controllo integrità applicazione**.

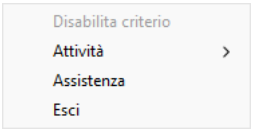
  - **Rollback alla versione precedente del database**.

  - **Scansione completa**.

  - **Scansione Personalizzata**.

- **Scansione delle aree critiche**.
- **Aggiornamento**.

- **Assistenza**. Si apre una finestra che contiene le informazioni necessarie per contattare l'Assistenza tecnica di Kaspersky.
- **Esci**. Questo elemento consente di uscire da Kaspersky Endpoint Security. Facendo clic su questa voce del menu di scelta rapida, l'applicazione viene scaricata dalla RAM del computer.



Menu di scelta rapida dell'icona dell'applicazione durante la visualizzazione dell'interfaccia semplificata

Configurazione della visualizzazione dell'interfaccia dell'applicazione

È possibile configurare la modalità di visualizzazione dell'interfaccia dell'applicazione per un utente. L'utente può interagire con l'applicazione nei seguenti modi:

- **Semplificata**. In un computer client, la finestra principale dell'applicazione non è accessibile ed è disponibile solo l'icona nell'area di notifica di Windows. Nel menu di scelta rapida dell'icona l'utente può eseguire un numero limitato di operazioni con Kaspersky Endpoint Security. Kaspersky Endpoint Security mostra inoltre solo le notifiche che richiedono l'azione dell'utente sopra l'icona dell'applicazione.
- **Completa**. In un computer client sono disponibili la finestra principale di Kaspersky Endpoint Security e l'icona nell'area di notifica Windows. Nel menu di scelta rapida dell'icona l'utente può eseguire operazioni con Kaspersky Endpoint Security. Kaspersky Endpoint Security visualizza inoltre le notifiche sopra l'icona dell'applicazione.
- **Non visualizzare l'interfaccia utente**. In un computer client non vengono visualizzati segni di esecuzione di Kaspersky Endpoint Security. L'icona nell'area di notifica di Windows e le notifiche non sono disponibili.

Come configurare la modalità di visualizzazione dell'interfaccia dell'applicazione in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Interfaccia**.

4. Nel blocco **Interazione con l'utente**, configurare il modo in cui verrà visualizzata l'interfaccia dell'applicazione:

   - **Visualizza interfaccia utente**. In un computer client sono disponibili la finestra principale di Kaspersky Endpoint Security e l'icona nell'area di notifica Windows. Nel menu di scelta rapida dell'icona l'utente può eseguire operazioni con Kaspersky Endpoint Security. Kaspersky Endpoint Security visualizza inoltre le notifiche sopra l'icona dell'applicazione. Se necessario, è possibile abilitare la funzionalità **Nascondi sezione Monitor attività applicazioni** per nascondere i dati sulle attività delle applicazioni nel computer, limitando l'accesso dell'utente allo strumento Monitoraggio attività applicazioni.

   - **Visualizza interfaccia semplificata**. In un computer client, la finestra principale dell'applicazione non è accessibile ed è disponibile solo l'icona nell'area di notifica di Windows. Nel menu di scelta rapida dell'icona l'utente può eseguire un numero limitato di operazioni con Kaspersky Endpoint Security. Kaspersky Endpoint Security mostra inoltre solo le notifiche che richiedono l'azione dell'utente sopra l'icona dell'applicazione.

   - **Non visualizzare l'interfaccia utente**. In un computer client non vengono visualizzati segni di esecuzione di Kaspersky Endpoint Security. L'icona nell'area di notifica di Windows e le notifiche non sono disponibili.

5. Salvare le modifiche.

Come configurare la modalità di visualizzazione dell'interfaccia dell'applicazione in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Interazione utente**.

5. Nel blocco **Visibilità per gli utenti**, configurare il modo in cui verrà visualizzata l'interfaccia dell'applicazione:

   - **Visualizza interfaccia utente**. Se questa funzionalità è disabilitata, nei computer client non viene visualizzato alcun segno dell'esecuzione di Kaspersky Endpoint Security. L'icona nell'area di notifica di Windows e le notifiche non sono disponibili.

   - **Semplificata**. In un computer client, la finestra principale dell'applicazione non è accessibile ed è disponibile solo l'icona nell'area di notifica di Windows. Nel menu di scelta rapida dell'icona l'utente può eseguire un numero limitato di operazioni con Kaspersky Endpoint Security. Kaspersky Endpoint Security mostra inoltre solo le notifiche che richiedono l'azione dell'utente sopra l'icona dell'applicazione.

   - **Completa**. In un computer client sono disponibili la finestra principale di Kaspersky Endpoint Security e l'icona nell'area di notifica Windows. Nel menu di scelta rapida dell'icona l'utente può eseguire operazioni con Kaspersky Endpoint Security. Kaspersky Endpoint Security visualizza inoltre le notifiche sopra l'icona dell'applicazione.

   - **Nascondi sezione Monitor attività applicazioni**. Se si desidera nascondere le informazioni sull'attività dell'applicazione sul computer dell'utente, è possibile limitare l'accesso dell'utente allo strumento Monitor attività applicazioni.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Preparazione dell'applicazione per l'utilizzo

Dopo la distribuzione dell'applicazione nei computer client, per l'utilizzo di Kaspersky Endpoint Security da Kaspersky Security Center Web Console è necessario eseguire le seguenti azioni:

- Creare e configurare un criterio.

  È possibile utilizzare i criteri per applicare le stesse impostazioni di Kaspersky Endpoint Security a tutti i computer client in un gruppo di amministrazione. L'Avvio rapido guidato di Kaspersky Security Center crea automaticamente un criterio per Kaspersky Endpoint Security.

- Creare le attività *Aggiornamento di database e moduli dell'applicazione* e *Scansione malware*.

  L'attività *Aggiornamento di database e moduli dell'applicazione* è necessaria per mantenere aggiornata la sicurezza del computer. Al momento dell'esecuzione dell'attività, Kaspersky Endpoint Security aggiorna i database anti-virus e i moduli dell'applicazione. L'attività *Aggiornamento di database e moduli dell'applicazione* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento di database e moduli dell'applicazione*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

  L'attività *Scansione malware* è necessaria per il rilevamento tempestivo di virus e altro malware. È necessario creare manualmente l'attività *Scansione malware*.

  Come creare un'attività Scansione malware in Administration Console (MMC)

  1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

     Viene aperto l'elenco delle attività.

  2. Fare clic su **Nuova attività**.

  Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Scansione malware**.

Passaggio 2. Ambito della scansione

Creare l'elenco degli oggetti per i quali Kaspersky Endpoint Security eseguirà la scansione durante l'esecuzione di un'attività di scansione.

Passaggio 3. Azione Kaspersky Endpoint Security

Scegliere l'azione da eseguire al rilevamento di una minaccia:

- **Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato.

- **Disinfetta (se la disinfezione non riesce, informa)**. Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive.

- **Informa**. Se questa opzione è selezionata, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti all'elenco delle minacce attive in caso di rilevamento di tali file.

- **Esegui immediatamente Disinfezione avanzata**. Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza la Tecnologia Avanzata di Disinfezione per trattare le minacce attive durante la scansione.

  La *Tecnologia Avanzata di Disinfezione* è progettata per eliminare dal sistema operativo le applicazioni dannose che hanno già avviato i propri processi nella RAM e che impediscono a Kaspersky Endpoint Security di rimuoverli con altri metodi. Come risultato, la minaccia viene neutralizzata. Mentre la disinfezione avanzata è in corso, è consigliabile evitare di avviare nuovi processi o modificare il registro del sistema operativo. La Tecnologia Avanzata di Disinfezione utilizza considerevoli risorse del sistema operativo, pertanto potrebbe rallentare le altre applicazioni. Al termine della disinfezione avanzata, Kaspersky Endpoint Security riavvierà il computer senza richiedere una conferma all'utente.

- **Esegui solo quando il computer è inattivo**. Avvio posticipato dell'attività quando le risorse del computer sono occupate. Kaspersky Endpoint Security avvia l'attività di scansione se il computer è bloccato o se lo screensaver è attivo. Se l'esecuzione dell'attività è stata interrotta, ad esempio sbloccando il computer, Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui era stata interrotta. Questa opzione di pianificazione consente di conservare le risorse del computer durante l'utilizzo del computer.

Passaggio 4. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.

- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 5. Selezione dell'account per eseguire l'attività

Selezione dell'account per eseguire l'attività *Scansione malware*. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale. Se l'ambito della scansione include unità di rete o altri oggetti con accesso limitato, selezionare un account utente con diritti di accesso sufficienti.

Passaggio 6. Configurazione di una pianificazione di avvio dell'attività

Configurare una pianificazione per l'avvio di un'attività, ad esempio manualmente o dopo il download dei database anti-virus nell'archivio.

Passaggio 7. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Scansione completa giornaliera*.

Passaggio 8. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività. In seguito a questa operazione, verrà eseguita l'attività Scansione malware nei computer degli utenti in base alla pianificazione specificata.

Come creare un'attività Scansione malware in Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Scansione malware**.

   c. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Scansione settimanale*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Selezione dell'account per eseguire l'attività. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.

6. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Per configurare la pianificazione delle attività, passare alle proprietà delle attività.

   Si consiglia di pianificare l'attività in modo che venga eseguita almeno una volta a settimana.

8. Selezionare la casella di controllo accanto all'attività.

9. Fare clic su **Avvia**.

   È possibile monitorare lo stato dell'attività e il numero di dispositivi in cui l'attività è stata completata o è stata completata con un errore.

In seguito a questa operazione, verrà eseguita l'attività Scansione malware nei computer degli utenti in base alla pianificazione specificata.

- Ottimizzare le prestazioni di Kaspersky Endpoint Security.

Gestione dei criteri

Un *criterio* è una raccolta di impostazioni dell'applicazione definite per un gruppo di amministrazione. È possibile configurare diversi criteri con differenti valori per un'applicazione. Un'applicazione può essere eseguita con diverse impostazioni per diversi gruppi di amministrazione. Ogni gruppo di amministrazione può avere uno specifico criterio per un'applicazione.

Ogni impostazione dei criteri ha l'attributo ("lucchetto"). Lo stato di questo attributo determina se l'impostazione verrà passata ai dispositivi gestiti nel gruppo di amministrazione:

- Se il "lucchetto" è aperto ( ), il valore di questa impostazione non verrà passato ai dispositivi gestiti. L'impostazione sarà disponibile per la modifica nell'interfaccia locale dell'applicazione. Tali impostazioni sono considerate *sbloccate*.

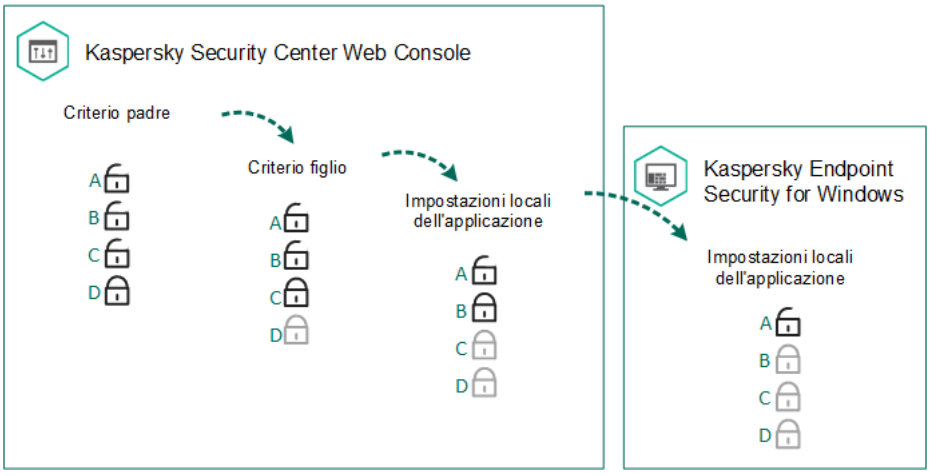
- Se il "lucchetto" è chiuso ( ), il valore di questa impostazione verrà passato e applicato ai dispositivi gestiti. Tali impostazioni sono considerate *bloccate*. Le impostazioni bloccate non possono essere modificate nell'interfaccia locale dell'applicazione.

Le impostazioni dei criteri vengono inviate ai computer client da parte di Network Agent durante la *sincronizzazione*. Per impostazione predefinita, Administration Server esegue la sincronizzazione non appena vengono modificate le impostazioni dei criteri. La porta UDP 15000 nel computer client viene utilizzata per la sincronizzazione. Administration Server esegue la sincronizzazione ogni 15 minuti per impostazione predefinita. Se la sincronizzazione non va a buon fine dopo la modifica delle impostazioni dei criteri, il successivo tentativo di sincronizzazione verrà eseguito in base alla pianificazione configurata.

Eredità impostazioni

I criteri, come i gruppi di amministrazione, sono organizzati in una gerarchia. Il *criterio figlio* è un criterio per i livelli nidificati della gerarchia, ovvero un criterio per i gruppi di amministrazione nidificati e gli Administration Server secondari.

Per impostazione predefinita, un criterio figlio eredita le impostazioni dal criterio padre. Se l'impostazione nel criterio principale ha l'attributo (lucchetto" chiuso), quindi nei criteri secondari e nelle impostazioni locali dell'applicazione, il valore di tale impostazione verrà ignorato in base al criterio principale e l'impostazione verrà bloccata. Se necessario, è possibile disabilitare l'eredità delle impostazioni dal criterio principale. I criteri fuori sede non influiscono sugli altri criteri nella gerarchia dei gruppi di amministrazione.



Eredità impostazioni

I diritti di accesso alle impostazioni dei criteri (lettura, scrittura, esecuzione) sono specificati per ogni utente che ha accesso all'Administration Server di Kaspersky Security Center e separatamente per ogni ambito funzionale di Kaspersky Endpoint Security. Per configurare i diritti di accesso alle impostazioni dei criteri, passare alla sezione **Sicurezza** della finestra delle proprietà di Kaspersky Security Center Administration Server (per impostazione predefinita, questa sezione è nascosta nell'interfaccia della console).

Revisioni dei criteri

Kaspersky Security Center monitora le modifiche ai criteri e crea le revisioni. Una *revisione* è un set di parametri modificati salvati dall'utente. Le revisioni consentono di confrontare e annullare le modifiche ai parametri del criterio. Oltre al set di parametri modificati, la revisione include informazioni sull'utente che ha apportato le modifiche, nonché l'ora, l'indirizzo IP, il commento dell'utente e altri dati pertinenti.

Per visualizzare il registro delle revisioni, aprire le proprietà del criterio e accedere alla sezione **Cronologia revisioni**. Per informazioni dettagliate sulle revisioni, consultare la Guida di Kaspersky Security Center.

Creazione di un criterio

Durante la creazione di un criterio, la procedura guidata suggerisce le impostazioni pertinenti per la modalità selezionata. Ad esempio, per la modalità Light Agent, è necessario aggiungere un server di protezione (SVM). Quando si utilizza l'applicazione per proteggere un server SQL, è necessario aggiungere esclusioni dalle scansioni predefinite per assicurarsi che il funzionamento del server non subisca interferenze. La procedura guidata suggerisce le impostazioni dei criteri pertinenti dopo aver selezionato una modalità. È quindi possibile modificare queste impostazioni nelle proprietà dei criteri.

Come creare un criterio in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, selezionare la cartella con il nome del gruppo di amministrazione a cui appartengono i computer client desiderati.
3. Nell'area di lavoro, selezionare la scheda **Criteri**.
4. Fare clic su **Nuovo criterio**.

   Verrà avviata la Creazione guidata nuovo criterio.
5. Attenersi alle istruzioni della Creazione guidata nuovo criterio.

Passaggio 1. Selezione dell'applicazione per creare il criterio di gruppo

Selezionare l'applicazione **Kaspersky Endpoint Security for Windows (14.2)**.

Passaggio 2. Denominazione del criterio di gruppo

Immettere un nome per il criterio di gruppo, ad esempio *Criterio per l'ufficio*.

È inoltre possibile creare nuovi criteri in base ai criteri esistenti utilizzando la Creazione guidata criterio. A tale scopo, quando si specifica il nome del criterio di gruppo, selezionare la casella di controllo **&Utilizza le impostazioni del criterio per una versione precedente dell'applicazione**. La procedura guidata consente inoltre di creare un criterio di Kaspersky Endpoint Security (KES) basato sul criterio di una soluzione diversa, ad esempio Kaspersky Security for Windows Server (KSWS) o Kaspersky Security for Virtualization Light Agent for Windows

Passaggio 3. Partecipazione a Kaspersky Security Network

Leggere e accettare le condizioni dell'Informativa su Kaspersky Security Network (KSN).

Passaggio 4. Selezione della modalità di utilizzo dell'applicazione nei computer

A seconda della destinazione d'uso di Kaspersky Endpoint Security, è possibile configurare un criterio per le seguenti modalità dell'applicazione:

- Modalità standard per proteggere gli host

In questa modalità, è possibile selezionare come si desidera configurare il criterio:

- **Crea un criterio con le impostazioni predefinite**. Le impostazioni predefinite sono considerate ottimali. Queste impostazioni sono consigliate dagli esperti di Kaspersky. Le impostazioni predefinite forniscono il livello di protezione consigliato e un utilizzo ottimale delle risorse.

- **Modificare le impostazioni del criterio nella procedura guidata**. Questo metodo consente di gestire dettagliatamente le impostazioni dei criteri utilizzando una procedura guidata. È inoltre possibile gestire le impostazioni dei criteri utilizzando un file di configurazione dell'applicazione (vedere il passaggio successivo).

- Endpoint Detection and Response Agent per proteggere da minacce avanzate e attacchi mirati.

  Endpoint Detection and Response Agent è un'applicazione che viene installata su singole workstation e server nell'infrastruttura IT dell'organizzazione per supportare le soluzioni Detection and Response di Kaspersky: Nel passaggio successivo, è necessario selezionare una soluzione per l'integrazione di EDR Agent.

- Light Agent per proteggere gli ambienti virtuali.

  Per utilizzare l'applicazione in modalità Light Agent, è necessario configurare una connessione con una macchina virtuale SVM. Queste impostazioni sono necessarie per il funzionamento dell'applicazione in modalità Light Agent.

Kaspersky Endpoint Security fornisce un criterio comune per tutte le modalità di applicazione e i tipi di sistemi operativi. Ciò significa che il criterio copre l'intero set di impostazioni. L'applicazione potrebbe tuttavia ignorare alcune impostazioni dei criteri poiché Kaspersky Endpoint Security viene distribuito in una modalità in cui alcune funzionalità non sono disponibili. Ad esempio, quando si utilizza l'applicazione in modalità Endpoint Detection and Response Agent, sono disponibili solo le impostazioni pertinenti per l'integrazione con le soluzioni Kaspersky Detection and Response e per l'integrazione con KUMA.

È consigliabile utilizzare criteri diversi a seconda delle modalità e dei tipi di sistemi operativi.

Passaggio 5. Importazione delle impostazioni

Questo passaggio è disponibile se si seleziona la configurazione manuale dei criteri al passaggio 4.

È possibile creare un criterio basato sulle impostazioni di Kaspersky Endpoint Security da un file di configurazione CFG. La procedura guidata Nuovo criterio non supporta i file di configurazione criptati. Quando si esporta il file di configurazione, omettere il passaggio relativo al criptaggio del file.

Quando si importa un file di configurazione CFG dell'applicazione, non tutte le impostazioni del criterio sono disponibili per la procedura guidata. Ad esempio, i profili criterio non sono presenti nelle impostazioni dell'applicazione. Se si desidera trasferire tutte le impostazioni e i profili nel criterio, è possibile importare un altro criterio da un file KLP.

Durante l'importazione di un file di configurazione, Kaspersky Endpoint Security non trasferisce le password dei contenitori crittografici. Se si utilizza l'autenticazione bidirezionale durante la connessione ai server, è necessario specificare da zero le password dei contenitori crittografici.

Passaggio 6-10. Configurazione delle impostazioni dei criteri

Questo passaggio è disponibile se si seleziona la configurazione manuale dei criteri al passaggio 4.

Seguire i passaggi per gestire le impostazioni dei criteri.

Passaggio 11. Configurazione dell'area attendibile

Configura l'area attendibile. È possibile aggiungere esclusioni dalla scansione e applicazioni attendibili predefinite. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server. Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono inoltre contribuire a configurare rapidamente Kaspersky Endpoint Security in modalità Light Agent negli ambienti virtuali Citrix e VMware.

Passaggio 12. Selezione dello stato del criterio

- **Attivo**. In seguito alla successiva sincronizzazione, il criterio verrà utilizzato come criterio attivo nel computer.

  Le impostazioni di un criterio attivo vengono salvate nei computer client durante la sincronizzazione. Non è possibile applicare più criteri contemporaneamente in un computer, quindi in ogni gruppo può essere attivo un solo criterio.

- **Inattivo**. Criterio di backup. Se necessario, un criterio inattivo può passare allo stato attivo.

  È possibile creare un numero illimitato di criteri inattivi. Un criterio inattivo non influisce sulle impostazioni dell'applicazione nei computer della rete. I criteri inattivi vengono utilizzati come strumenti preventivi per situazioni di emergenza, ad esempio un attacco virus. Se si verifica un attacco tramite unità flash, è possibile attivare un criterio che blocca l'accesso alle unità flash. In questo caso, il criterio attivo diventa automaticamente inattivo.

- **Fuori sede**. Il criterio viene attivato quando un computer esce dal perimetro di rete dell'organizzazione.

Terminare la procedura guidata.

Come creare un criterio in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuovo criterio.
3. Selezionare Kaspersky Endpoint Security e fare clic su **Avanti**.
4. Leggere e accettare le condizioni dell'Informativa su Kaspersky Security Network (KSN) e fare clic su **Avanti**.

5. Selezionare la modalità dell'applicazione:

   - Modalità standard per proteggere workstation e server
   - Endpoint Detection and Response Agent per proteggere da minacce avanzate e attacchi mirati.

     Se si seleziona questa modalità, è possibile creare un criterio per l'integrazione del computer con le soluzioni Kaspersky Detection and Response. La procedura guidata richiede di configurare l'integrazione per Kaspersky Managed Detection and Response e quindi Kaspersky Anti Targeted Attack Platform (EDR).
   - Light Agent per proteggere gli ambienti virtuali.

     Se si seleziona questa modalità, al passaggio successivo è necessario configurare la connessione al server di protezione (SVM). Queste impostazioni sono necessarie per il funzionamento dell'applicazione in modalità Light Agent.

   Kaspersky Endpoint Security fornisce un criterio comune per tutte le modalità di applicazione e i tipi di sistemi operativi. Ciò significa che il criterio copre l'intero set di impostazioni. L'applicazione potrebbe tuttavia ignorare alcune impostazioni dei criteri poiché Kaspersky Endpoint Security viene distribuito in una modalità in cui alcune funzionalità non sono disponibili. Ad esempio, quando si utilizza l'applicazione in modalità Endpoint Detection and Response Agent, sono disponibili solo le impostazioni pertinenti per l'integrazione con le soluzioni Kaspersky Detection and Response e per l'integrazione con KUMA.

   È consigliabile utilizzare criteri diversi a seconda delle modalità e dei tipi di sistemi operativi.

6. Configura l'area attendibile. È possibile aggiungere esclusioni dalla scansione e applicazioni attendibili predefinite. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server. Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono inoltre contribuire a configurare rapidamente Kaspersky Endpoint Security in modalità Light Agent negli ambienti virtuali Citrix e VMware.

7. Nella scheda **Generali** è possibile eseguire le seguenti azioni:

   - Modificare il nome del criterio.
   - Selezionare lo stato del criterio:

     - **Attivo**. In seguito alla successiva sincronizzazione, il criterio verrà utilizzato come criterio attivo nel computer.

       Le impostazioni di un criterio attivo vengono salvate nei computer client durante la sincronizzazione. Non è possibile applicare più criteri contemporaneamente in un computer, quindi in ogni gruppo può essere attivo un solo criterio.
     - **Inattivo**. Criterio di backup. Se necessario, un criterio inattivo può passare allo stato attivo.

       È possibile creare un numero illimitato di criteri inattivi. Un criterio inattivo non influisce sulle impostazioni dell'applicazione nei computer della rete. I criteri inattivi vengono utilizzati come strumenti preventivi per situazioni di emergenza, ad esempio un attacco virus. Se si verifica un attacco tramite unità flash, è possibile attivare un criterio che blocca l'accesso alle unità flash. In questo caso, il criterio attivo diventa automaticamente inattivo.
     - **Fuori sede**. Il criterio viene attivato quando un computer esce dal perimetro di rete dell'organizzazione.

- Configurare l'ereditarietà delle impostazioni:
  - **Eredita impostazioni dal criterio principale**. Se questo interruttore è attivato, i valori delle impostazioni dei criteri vengono ereditati dal criterio di livello superiore. Le impostazioni dei criteri non possono essere modificate se è impostato per il criterio padre.
  - **Forza ereditarietà impostazioni nei criteri secondari**. Se l'interruttore è attivato, i valori delle impostazioni dei criteri vengono propagati ai criteri figlio. Nelle proprietà del criterio secondario, l'interruttore **Eredita impostazioni dal criterio principale** verrà automaticamente attivato e non potrà essere disattivato. Le impostazioni del criterio figlio vengono ereditate dal criterio padre, ad eccezione delle impostazioni contrassegnate con . Le impostazioni del criterio figlio non possono essere modificate se è impostato per il criterio padre.

8. Nella scheda **Impostazioni applicazione** è possibile configurare le impostazioni dei criteri di Kaspersky Endpoint Security.
9. Terminare la procedura guidata.

In seguito a questa operazione, le impostazioni di Kaspersky Endpoint Security verranno configurate nei computer client durante la successiva sincronizzazione. È possibile visualizzare le informazioni sul criterio applicato al computer nell'interfaccia di Kaspersky Endpoint Security facendo clic sul pulsante nella schermata principale (ad esempio il nome del criterio). A tale scopo, nelle impostazioni del criterio di Network Agent, è necessario abilitare la ricezione dei dati del criterio esteso. Per informazioni dettagliate su un criterio di Network Agent, consultare la Guida di Kaspersky Security Center.

Esportazione e importazione di un criterio

Kaspersky Endpoint Security consente di esportare un criterio con le relative impostazioni e profili in un file KLP. È quindi possibile utilizzare la funzionalità di esportazione/importazione dei criteri per eseguire il backup dei criteri, eseguire la migrazione dei criteri a un altro server o, ad esempio, per la migrazione dei criteri da Kaspersky Security Center Windows a Kaspersky Security Center Linux. Per ulteriori dettagli sulla gestione dei criteri, consultare la Guida di Kaspersky Security Center.

Come esportare e importare un criterio in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, aprire la cartella con il nome del gruppo di amministrazione a cui appartengono i computer client desiderati.
3. Nell'area di lavoro, selezionare la scheda **Criteri**.
4. Per esportare un criterio:
   a. Fare clic sul criterio che si desidera esportare.
   b. Fare clic sul collegamento **Esporta criterio in un file** nella parte destra della finestra.
   c. Nella finestra visualizzata specificare il nome del file KLP in cui si desidera esportare il criterio e selezionare la cartella in cui salvare il file.
   d. Salvare il file.

5. Per importare un criterio:

    a. Fare clic su **Importa criteri da file**.

    b. Nella finestra visualizzata, selezionare il file del criterio KLP che si desidera importare.

    c. Aprire il file.

    Questo aggiunge un nuovo criterio con lo stato *Criterio inattivo*.

Come esportare e importare il criterio in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Per esportare un criterio:

    a. Selezionare la casella di controllo accanto al criterio che si desidera esportare.

    b. Fare clic sul pulsante **Esporta**.

    c. Nella finestra visualizzata specificare il nome del file KLP in cui si desidera esportare il criterio e selezionare la cartella in cui salvare il file.

    d. Salvare il file.

3. Per importare un criterio:

    a. Fare clic su **Importa**.

    b. Selezionare il file del criterio KLP che si desidera importare.

    c. Al termine dell'elaborazione del criterio, selezionare il gruppo di amministrazione a cui si desidera applicare il criterio.

    d. Fare clic sul pulsante **Completato** per terminare l'importazione del criterio.

    Questo aggiunge un nuovo criterio con lo stato *Inattivo*.

Indicatore del livello di sicurezza

L'indicatore del livello di sicurezza viene visualizzato nella parte superiore della finestra delle proprietà dei criteri. L'indicatore può avere uno dei seguenti valori:

- **Livello di protezione alto**. L'indicatore assume questo valore e diventa verde se tutti i componenti delle seguenti categorie sono abilitati:
    - **Critico**. Questa categoria include i seguenti componenti:
        - Protezione minacce file.
        - Rilevamento del Comportamento.
        - Prevenzione Exploit.

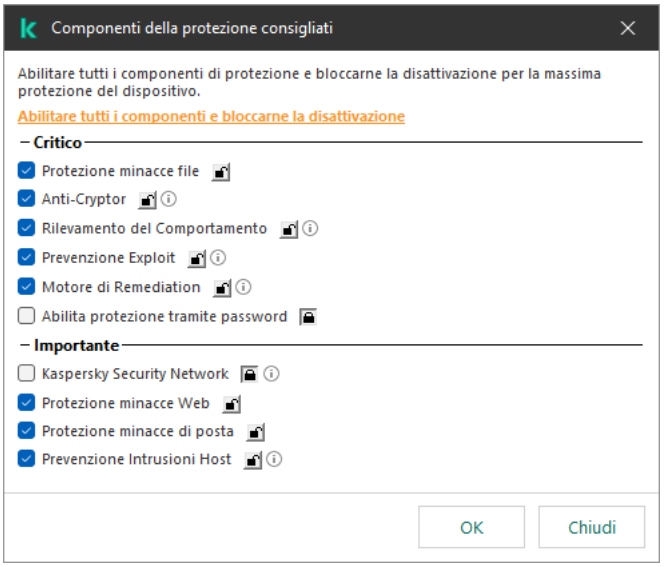
- Motore di Remediation.
- Protezione dei servizi applicativi contro la gestione esterna.

- **Importante**. Questa categoria include i seguenti componenti:
  - Kaspersky Security Network.
  - Protezione minacce Web.
  - Protezione minacce di posta.
  - Prevenzione Intrusioni Host.
  - Protezione tramite password.

- **Livello di protezione medio**. L'indicatore assume questo valore e diventa giallo se uno dei componenti importanti è disabilitato.
- **Livello di protezione basso**. L'indicatore assume questo valore e diventa rosso in uno dei seguenti casi:
  - Uno o più componenti critici sono disabilitati.
  - Due o più componenti importanti sono disabilitati.

Se l'indicatore ha il valore **Livello di protezione medio** o **Livello di protezione basso**, a destra dell'indicatore viene visualizzato un collegamento che apre la finestra **Componenti della protezione consigliati**. In questa finestra è possibile abilitare uno dei componenti della protezione consigliati.

Dopo l'aggiornamento dell'applicazione, l'indicatore del livello di protezione potrebbe indicare un livello di protezione inferiore rispetto al periodo precedente all'aggiornamento. Ciò accade perché la versione più recente dell'applicazione introduce nuovi componenti o funzionalità importanti per la protezione del computer. Dopo l'upgrade dell'applicazione, è necessario gestire le nuove impostazioni per assicurarsi che il livello di protezione rimanga elevato.



Indicatore del livello di sicurezza del criterio

Gestione attività

È possibile creare i seguenti tipi di attività per amministrare Kaspersky Endpoint Security tramite Kaspersky Security Center:

- Attività locali configurate per un singolo computer client.
- Attività di gruppo configurate per i computer client all'interno di gruppi di amministrazione.
- Attività per una selezione di computer.

È possibile creare qualsiasi numero di attività di gruppo, attività per una selezione di computer o attività locali. Per informazioni dettagliate sull'utilizzo dei gruppi di amministrazione e delle selezioni di computer, consultare la Guida di Kaspersky Security Center.

Kaspersky Endpoint Security supporta le seguenti attività:

- **Scansione malware**. Kaspersky Endpoint Security esamina le aree del computer specificate nelle impostazioni dell'attività alla ricerca di virus e altre minacce. L'attività *Scansione malware* è necessaria per l'esecuzione di Kaspersky Endpoint Security e viene creata durante l'Avvio rapido guidato. Si consiglia di pianificare l'attività in modo che venga eseguita almeno una volta a settimana.
- **Aggiungi chiave**. Kaspersky Endpoint Security aggiunge una chiave per l'attivazione delle applicazioni, compresa una chiave di riserva. Prima dell'esecuzione dell'attività, verificare che il numero di computer in cui deve essere eseguita l'attività non superi il numero di computer consentito dalla licenza.
- **Modifica i componenti dell'applicazione**. Kaspersky Endpoint Security installa o rimuove i componenti nei computer client in base all'elenco di componenti specificati nelle impostazioni dell'attività. Il componente Protezione minacce file non può essere rimosso. Il set ottimale dei componenti di Kaspersky Endpoint Security consente di ridurre l'utilizzo delle risorse del computer.
- **Inventario**. Kaspersky Endpoint Security riceve informazioni su tutti i file eseguibili delle applicazioni archiviate nei computer. L'attività *Inventario* viene eseguita dal componente Controllo applicazioni. Se il componente Controllo applicazioni non è installato, l'attività verrà terminata con un errore.
- **Aggiornamento di database e moduli dell'applicazione**. Kaspersky Endpoint Security aggiorna i database e i moduli dell'applicazione. L'attività *Aggiornamento di database e moduli dell'applicazione* è necessaria per l'esecuzione di Kaspersky Endpoint Security e viene creata durante l'Avvio rapido guidato. È consigliabile configurare una pianificazione che esegua l'attività almeno una volta al giorno.
- **Cancella dati**. Kaspersky Endpoint Security elimina i file e le cartelle dai computer degli utenti immediatamente o se la connessione a Kaspersky Security Center non è disponibile da molto tempo.
- **Rollback degli aggiornamenti**. Kaspersky Endpoint Security esegue il rollback dell'ultimo aggiornamento dei database e dei moduli dell'applicazione. Questo può essere necessario se, ad esempio, i nuovi database contengono dati errati che possono causare il blocco di un'applicazione sicura da parte di Kaspersky Endpoint Security.

- **Controllo integrità applicazione**. Kaspersky Endpoint Security analizza i file delle applicazioni, verifica la presenza di danni o modifiche nei file e le firme originali dei file delle applicazioni.

- **Gestisci account dell'Agente di Autenticazione**. Kaspersky Endpoint Security configura le impostazioni dell'account dell'Agente di Autenticazione. Per utilizzare le unità criptate è necessario un Agente di Autenticazione. Prima del caricamento del sistema operativo, l'utente deve completare l'autenticazione con l'Agente.

Se l'applicazione funziona come parte della soluzione Endpoint Detection and Response di Kaspersky, è possibile eseguire attività aggiuntive come azioni di risposta al rilevamento (responses). Ad esempio, è possibile terminare i processi da remoto tramite l'attività *Termina processo*.

Le attività vengono eseguite in un computer solo se Kaspersky Endpoint Security è in esecuzione.

Creazione di un'attività

Come creare un'attività in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Selezionare la cartella **Attività** nella struttura di Administration Console.
3. Fare clic su **Nuova attività**.

   Verrà avviata la Creazione guidata attività.
4. Attenersi alle istruzioni della Creazione guidata attività.

Come creare un'attività in Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.
3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività** selezionare l'attività da eseguire nei computer degli utenti.

   c. Nel campo **Nome attività**, immettere una breve descrizione.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.
4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Selezione dell'account per eseguire l'attività. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.

6. Terminare la procedura guidata.

Verrà visualizzata una nuova attività nell'elenco delle attività. L'attività avrà le impostazioni predefinite. Per configurare le impostazioni dell'attività, è necessario passare alle proprietà dell'attività. Per eseguire un'attività, è necessario selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**. Dopo l'avvio dell'attività, è possibile sospendere l'attività e riprenderla in un secondo momento.

Nell'elenco delle attività è possibile monitorare i risultati delle attività, tra i quali sono inclusi lo stato dell'attività e le statistiche relative alle prestazioni dell'attività nei computer. È inoltre possibile creare una selezione di eventi per monitorare il completamento delle attività (**Monitoraggio → Selezioni eventi**). Per ulteriori dettagli sulla selezione di eventi, consultare la Guida di Kaspersky Security Center. I risultati dell'esecuzione delle attività vengono salvati anche in locale nel registro eventi di Windows e nei rapporti di Kaspersky Endpoint Security.

Gestione dell'accesso alle attività

I diritti di accesso alle attività di Kaspersky Endpoint Security (lettura, scrittura, esecuzione) sono definiti per ogni utente che ha accesso a Kaspersky Security Center Administration Server, tramite le impostazioni di accesso alle aree funzionali di Kaspersky Endpoint Security. Per configurare l'accesso alle aree funzionali di Kaspersky Endpoint Security, passare alla sezione **Sicurezza** della finestra delle proprietà di Kaspersky Security Center Administration Server. Per informazioni dettagliate sulla gestione delle attività tramite Kaspersky Security Center, fare riferimento alla Guida di Kaspersky Security Center.

È possibile configurare i diritti degli utenti per l'accesso alle attività utilizzando un criterio (*modalità di gestione attività*). È ad esempio possibile nascondere le attività di gruppo nell'interfaccia di Kaspersky Endpoint Security.

Come configurare la modalità di gestione attività nell'interfaccia di Kaspersky Endpoint Security tramite Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Attività locali → Gestione attività**.

4. Configurare la modalità di gestione attività (vedere la tabella seguente).

5. Salvare le modifiche.

Come configurare la modalità di gestione attività nell'interfaccia di Kaspersky Endpoint Security tramite Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali → Interazione utente**.

5. In **Azioni consentite**, configurare la modalità di gestione attività (vedere la tabella seguente).

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Impostazioni di Gestione attività

Parametro	Descrizione
Accesso alle attività locali	Se la casella di controllo è selezionata, le attività locali vengono visualizzate nell'interfaccia locale di Kaspersky Endpoint Security. Se non sono presenti ulteriori restrizioni a livello di criterio, l'utente può configurare ed eseguire le attività. Tuttavia, la configurazione della pianificazione dell'esecuzione delle attività rimane non disponibile per l'utente. L'utente può eseguire le attività solo manualmente. Se questa casella di controllo è deselezionata, le attività locali vengono nascoste nell'interfaccia dell'applicazione. In questa modalità, le attività locali non vengono eseguite in base alla pianificazione. Non è possibile avviare o configurare le attività nell'interfaccia locale di Kaspersky Endpoint Security o durante l'utilizzo della riga di comando. Un utente può comunque avviare una scansione di un file o una cartella selezionando l'opzione **Ricerca virus** nel menu di scelta rapida del file o della cartella. L'attività di scansione viene avviata con i valori predefiniti delle impostazioni per l'attività Scansione personalizzata.
Visualizza attività di gruppo	Se la casella di controllo è selezionata, le attività di gruppo vengono visualizzate nell'interfaccia locale di Kaspersky Endpoint Security. L'utente può visualizzare l'elenco di tutte le attività nell'interfaccia dell'applicazione. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security visualizza un elenco di attività vuoto.
Gestisci attività di gruppo	Se la casella di controllo è selezionata, gli utenti possono avviare e arrestare le attività di gruppo specificate nella console di Kaspersky Security Center. Gli utenti possono avviare e arrestare le attività nell'interfaccia dell'applicazione o nell'interfaccia dell'applicazione semplificata. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security avvia automaticamente le attività pianificate oppure l'amministratore avvia le attività manualmente nella console di Kaspersky Security Center.

Configurazione delle impostazioni locali dell'applicazione

In Kaspersky Security Center è possibile configurare le impostazioni di Kaspersky Endpoint Security in un computer specifico. Si tratta delle *impostazioni locali dell'applicazione*. Alcune impostazioni possono essere inaccessibili per la modifica. Queste impostazioni sono bloccate dall'attributo nelle proprietà dei criteri.

Come configurare le impostazioni locali dell'applicazione in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, aprire la cartella con il nome del gruppo di amministrazione a cui appartengono i computer client desiderati.

3. Nell'area di lavoro, selezionare la scheda **Dispositivi**.

4. Fare doppio clic per aprire la finestra delle proprietà del computer.

5. Nella finestra delle proprietà del computer, selezionare la sezione **Applicazioni**.

6. Nell'elenco delle applicazioni Kaspersky installate nel computer selezionare **Kaspersky Endpoint Security for Windows (14.2)** e fare doppio clic per aprire le proprietà dell'applicazione.

7. Nella sezione **Impostazioni generali**, configurare Kaspersky Endpoint Security e Rapporti e archivi.

   Le altre sezioni nella finestra delle proprietà dell'applicazione sono standard per Kaspersky Security Center. Una descrizione di queste sezioni è disponibile nella Guida di Kaspersky Security Center.

Se un'applicazione è sottoposta a un criterio che impedisce la modifica di specifiche impostazioni, non sarà possibile modificarle durante la configurazione delle impostazioni dell'applicazione nella sezione **Impostazioni generali**.

8. Salvare le modifiche.

Come configurare le impostazioni locali dell'applicazione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Selezionare il computer per cui si desidera configurare le impostazioni locali dell'applicazione.

   Verranno visualizzate le proprietà del computer.
3. Selezionare la scheda **Applicazioni**.
4. Fare clic su **Kaspersky Endpoint Security for Windows 14.2**.

   Verranno visualizzate le impostazioni locali dell'applicazione.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Configurare le impostazioni locali dell'applicazione.
7. Salvare le modifiche.

Le impostazioni locali dell'applicazione sono uguali alle impostazioni dei criteri, ad eccezione delle impostazioni di criptaggio.

Avvio e arresto di Kaspersky Endpoint Security

Dopo aver installato Kaspersky Endpoint Security nel computer di un utente, l'applicazione viene avviata automaticamente. Per impostazione predefinita, Kaspersky Endpoint Security viene avviato all'avvio del sistema operativo. Non è possibile configurare l'avvio automatico dell'applicazione nelle impostazioni del sistema operativo.

Il download dei database anti-virus di Kaspersky Endpoint Security dopo l'avvio del sistema operativo può richiedere fino a due minuti, in base alle funzionalità del computer. Durante questo periodo di tempo, il livello di protezione del computer è ridotto. Il download dei database anti-virus mentre Kaspersky Endpoint Security è avviato in un sistema operativo già avviato non determina una riduzione del livello di protezione del computer.

Come configurare l'avvio di Kaspersky Endpoint Security in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
4. Utilizzare la casella di controllo **Avvia l'applicazione all'avvio del computer (consigliato)** per configurare l'avvio dell'applicazione.
5. Salvare le modifiche.

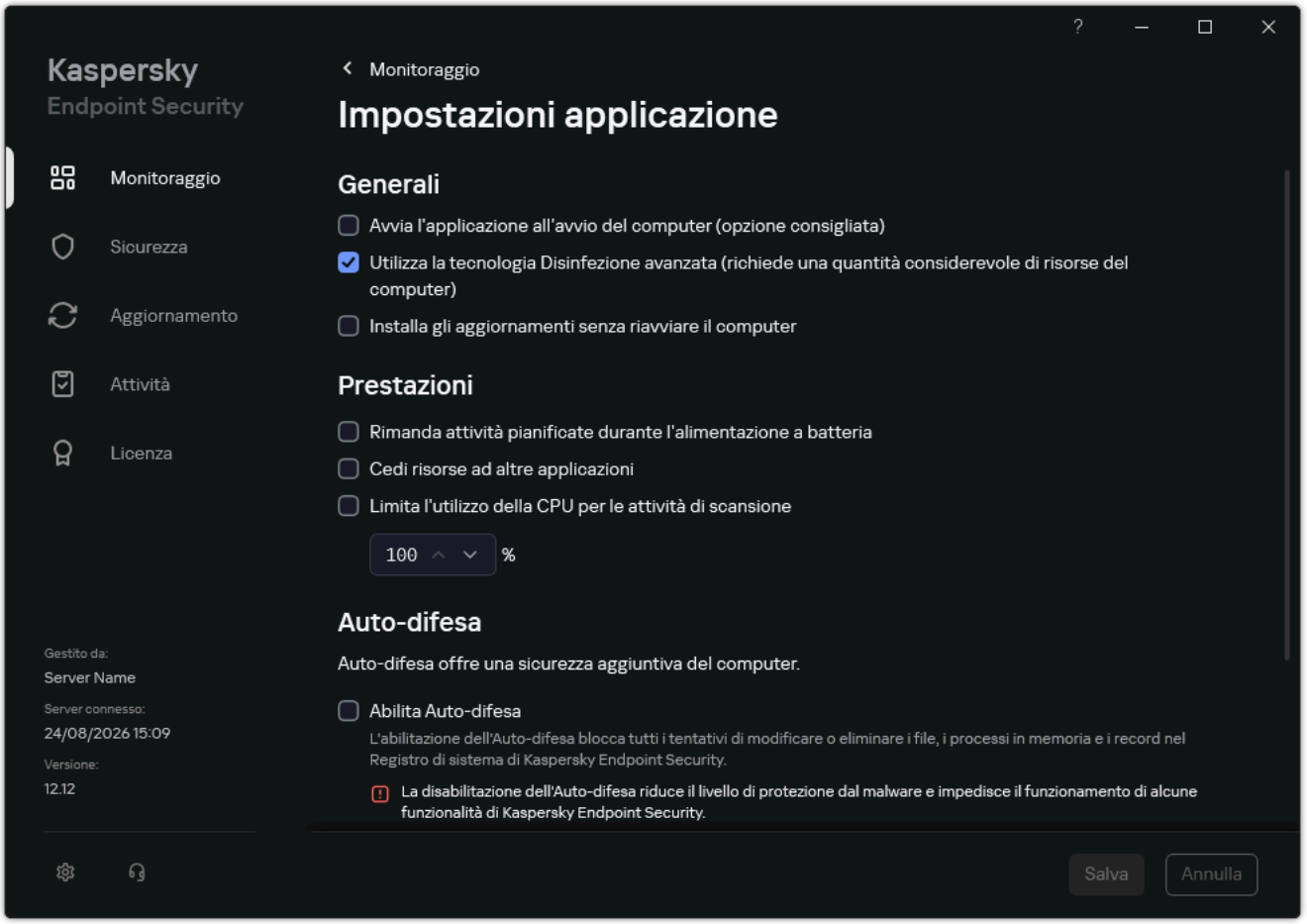
Come configurare l'avvio di Kaspersky Endpoint Security in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Interazione utente**.
5. Utilizzare la casella di controllo **Avvia Kaspersky Endpoint Security all'avvio del computer (consigliato)** per configurare l'avvio dell'applicazione.
6. Salvare le modifiche.

Come configurare l'avvio di Kaspersky Endpoint Security nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.



Impostazioni di Kaspersky Endpoint Security for Windows

3. Utilizzare la casella di controllo **Avvia l'applicazione all'avvio del computer (consigliato)** per configurare l'avvio dell'applicazione.

4. Salvare le modifiche.

Gli esperti di Kaspersky consigliano di non chiudere manualmente Kaspersky Endpoint Security, perché questo può mettere a rischio la protezione del computer e dei dati personali. Se necessario, è possibile sospendere la protezione del computer per il tempo necessario, senza arrestare l'applicazione.

È possibile monitorare lo stato dell'applicazione utilizzando il widget **Stato protezione**.

Come avviare o arrestare Kaspersky Endpoint Security in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, aprire la cartella con il nome del gruppo di amministrazione a cui appartengono i computer client desiderati.

3. Nell'area di lavoro, selezionare la scheda **Dispositivi**.

4. Fare doppio clic per aprire la finestra delle proprietà del computer.

5. Nella finestra delle proprietà del computer, selezionare la sezione **Applicazioni**.

6. Nell'elenco delle applicazioni Kaspersky installate nel computer selezionare **Kaspersky Endpoint Security for Windows (14.2)** e fare doppio clic per aprire le proprietà dell'applicazione.

7. Eseguire una delle seguenti operazioni:

   - Per avviare l'applicazione, fare clic sul pulsante  a destra dell'elenco delle applicazioni Kaspersky.
   - Per arrestare l'applicazione, fare clic sul pulsante  a destra dell'elenco delle applicazioni Kaspersky.

Come avviare o arrestare Kaspersky Endpoint Security in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.

2. Fare clic sul nome del computer in cui si desidera avviare o arrestare Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del computer.

3. Selezionare la scheda **Applicazioni**.

4. Selezionare la casella di controllo accanto a **Kaspersky Endpoint Security for Windows**.

5. Fare clic sul pulsante **Avvia** o **Arresta**.

Come avviare o arrestare Kaspersky Endpoint Security dalla riga di comando

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.

2. Accedere alla cartella in cui si trova il file eseguibile klpsm.exe.

3. Per avviare l'applicazione dalla riga di comando, immettere `klpsm.exe start_avp_service`.

4. Per arrestare l'applicazione dalla riga di comando, immettere `klpsm.exe stop_avp_service`.

Per arrestare l'applicazione dalla riga di comando, abilitare la gestione esterna dei servizi di sistema.



Avvio e arresto dell'applicazione dalla riga di comando

Sospensione e ripresa della protezione e del controllo del computer

Sospendere la protezione e il controllo del computer significa disabilitare tutti i componenti della protezione e di controllo di Kaspersky Endpoint Security per un determinato periodo.

Lo stato dell'applicazione è indicato dall'icona dell'applicazione nell'area di notifica della barra delle applicazioni.

- L'icona indica che la protezione e il controllo del computer sono sospesi.
- L'icona indica che la protezione e il controllo del computer sono abilitati.

La sospensione o la ripresa della protezione e del controllo del computer non influisce sulle attività di scansione e di aggiornamento.

Se sono già state stabilite connessioni di rete quando si sospendono o si riprendono la protezione e il controllo del computer, viene visualizzata una notifica dell'interruzione di tali connessioni di rete.

Per sospendere la protezione e il controllo del computer:

1. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni.
2. Nel menu di scelta rapida selezionare **Sospendi la protezione** (vedere la figura riportata di seguito).

   Questo elemento del menu di scelta rapida è disponibile se Protezione tramite password è abilitata.

3. Selezionare una delle seguenti opzioni:

   - **Sospendi per <periodo di tempo>** – la protezione e il controllo del computer verranno ripristinati al termine del periodo di tempo specificato nell'elenco a discesa di seguito.
   - **Sospendi fino al riavvio dell'applicazione** - la protezione e il controllo del computer verranno ripristinati dopo il riavvio dell'applicazione o del sistema operativo. Per utilizzare questa opzione, deve essere abilitato l'avvio automatico dell'applicazione.
   - **Sospendi** - la protezione e il controllo del computer verranno ripresi quando l'utente decide di abilitarli nuovamente.

4. Fare clic su **Sospendi la protezione**.

   Kaspersky Endpoint Security sospenderà il funzionamento di tutti i componenti di protezione e controllo non contrassegnati da un lucchetto (🔒) nel criterio. Prima di eseguire questa operazione, è consigliabile disabilitare il criterio di Kaspersky Security Center.



Menu di scelta rapida dell'icona dell'applicazione

Per riprendere la protezione e il controllo del computer:

1. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni.
2. Nel menu di scelta rapida, selezionare **Ripristina protezione**.

È possibile riprendere la protezione e il controllo del computer in qualsiasi momento, indipendentemente dall'opzione selezionata in precedenza per la sospensione della protezione e del controllo del computer.

Creazione e utilizzo di un file di configurazione

Un file di configurazione con le impostazioni di Kaspersky Endpoint Security consente di eseguire le seguenti attività:

- Eseguire l'installazione locale di Kaspersky Endpoint Security tramite la riga di comando con le impostazioni predefinite.
- Eseguire l'installazione remota di Kaspersky Endpoint Security tramite Kaspersky Security Center con le impostazioni predefinite.
- Trasferire le impostazioni dell'applicazione in un criterio.
- Eseguire la migrazione delle impostazioni di Kaspersky Endpoint Security da un computer a un altro (vedere le istruzioni riportate di seguito).

Esportazione un file di configurazione

A partire da Kaspersky Endpoint Security 14.2, il file di configurazione esportato può essere criptato. Poiché il file di configurazione può contenere credenziali, è consigliabile criptarlo. Non è possibile modificare un file criptato. Qualsiasi tentativo di modificare un file di configurazione lo danneggia.

Il criptaggio dei file di configurazione presenta le seguenti caratteristiche speciali:

- Kaspersky Endpoint Security consente di importare i file criptati solo tramite l'interfaccia utente dell'applicazione o la riga di comando. Non è possibile utilizzare un file di questo tipo in una console di Kaspersky Security Center per configurare un criterio o installare l'applicazione in remoto. Se si intende aggiungere il file a un criterio o a un pacchetto di installazione, saltare il passaggio relativo al criptaggio del file.
- Non è possibile recuperare la password di un file criptato.
- Le versioni di Kaspersky Endpoint Security precedenti alla 14.1 non supportano l'importazione di file di configurazione criptati. Se si intende importare il file in una versione precedente dell'applicazione, saltare il passaggio relativo al criptaggio del file.

Per creare un file di configurazione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Gestione impostazioni**.
3. Fare clic su **Esporta**.
4. Per salvare il file di configurazione, la protezione tramite password deve essere abilitata. L'utente deve avere l'autorizzazione **Esporta impostazioni**.
5. Nella finestra visualizzata specificare il percorso in cui si desidera salvare il file di configurazione e immettere il nome del file.

   Per utilizzare il file di configurazione per l'installazione locale o remota di Kaspersky Endpoint Security, è necessario denominarlo install.cfg.

6. Se necessario, attivare l'interruttore **Cripta il file esportato** e immettere la password di criptaggio del file di configurazione.

   Salvare la password in un archivio sicuro. Non è possibile recuperare questa password.

7. Salvare il file.

In seguito a questa operazione, l'applicazione crea un file di configurazione.

Importazione di un file di configurazione

Durante l'importazione di un file di configurazione, Kaspersky Endpoint Security non trasferisce le password dei contenitori crittografici. Se si utilizza l'autenticazione bidirezionale durante la connessione ai server, è necessario specificare da zero le password dei contenitori crittografici.

Per importare le impostazioni di Kaspersky Endpoint Security da un file di configurazione:

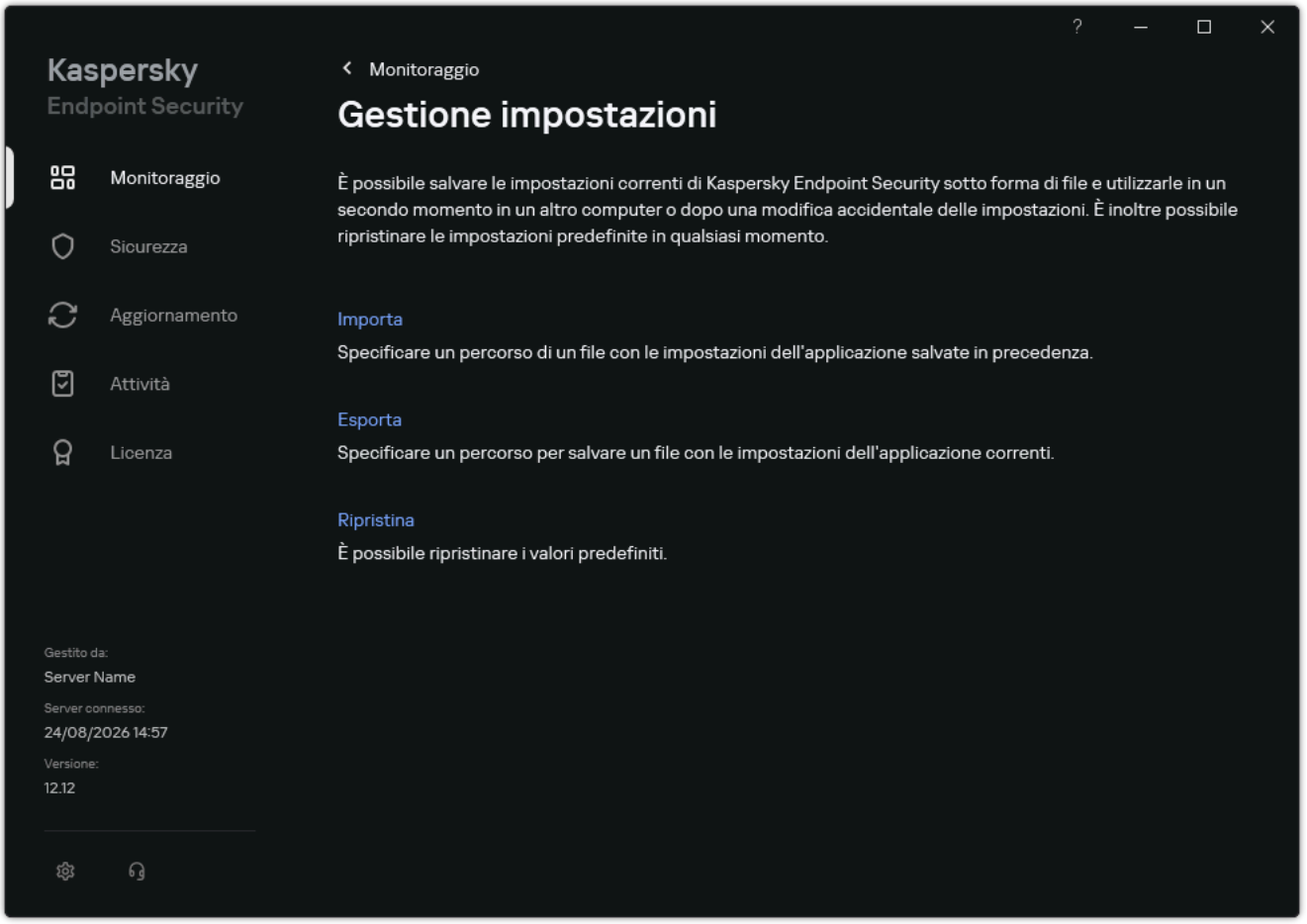
1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Gestione impostazioni**.
3. Fare clic su **Importa**.
4. Nella finestra visualizzata immettere il percorso del file di configurazione.

5. Se il file di configurazione è criptato, immettere la password specificata durante l'esportazione.

> Se si è dimenticata la password di criptaggio del file di configurazione, non è possibile recuperarla. In questo caso, è necessario ripetere i passaggi per l'esportazione del file di configurazione.

6. Aprire il file.

Tutti i valori delle impostazioni di Kaspersky Endpoint Security saranno configurati in base al file di configurazione selezionato.



Gestione delle le impostazioni dell'applicazione

Ripristino delle impostazioni predefinite dell'applicazione

È possibile ripristinare le impostazioni dell'applicazione consigliate da Kaspersky in qualsiasi momento. Quando le impostazioni sono state ripristinate, viene impostato il livello di sicurezza **Consigliato** per tutti i componenti di protezione.

Per ripristinare le impostazioni predefinite dell'applicazione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Gestione impostazioni**.
3. Fare clic su **Ripristina**.

4. Salvare le modifiche.



Gestione delle le impostazioni dell'applicazione

Prestazioni di Kaspersky Endpoint Security e compatibilità con altre applicazioni

Le prestazioni di Kaspersky Endpoint Security si riferiscono al numero di tipi di oggetti dannosi rilevabili, nonché al consumo di energia e all'utilizzo delle risorse del computer.

Selezione dei tipi di oggetti rilevabili

Kaspersky Endpoint Security consente di ottimizzare la protezione del computer e di selezionare i tipi di oggetti rilevati dall'applicazione durante l'esecuzione. Kaspersky Endpoint Security esegue sempre la scansione del sistema operativo alla ricerca di virus, worm e Trojan. Non è possibile disabilitare la scansione di questi tipi di oggetti. Il malware di questo tipo può danneggiare in modo significativo il computer. Per una maggiore protezione del computer, è possibile espandere i tipi di oggetti rilevabili abilitando il monitoraggio del software legittimo che potrebbe essere utilizzato da utenti malintenzionati per danneggiare il computer o i dati personali.

Utilizzo della modalità di risparmio energetico

Il consumo di energia da parte delle applicazioni è un aspetto essenziale per i computer portatili. Le attività pianificate di Kaspersky Endpoint Security in genere richiedono una quantità considerevole di risorse. Quando il computer è alimentato a batteria, è possibile utilizzare la modalità di risparmio energetico per ridurre il consumo di energia.

Nella modalità di risparmio energetico le seguenti attività pianificate vengono automaticamente rimandate:

- Attività Scansione completa;
- Attività Scansione delle aree critiche;
- Attività Scansione personalizzata;
- Attività Controllo integrità.

Indipendentemente dal fatto che la modalità di risparmio energetico sia abilitata o meno, Kaspersky Endpoint Security sospende le attività di criptaggio quando un computer portatile passa all'alimentazione a batteria. L'applicazione riprende le attività di criptaggio quando il computer portatile viene nuovamente alimentato dalla rete.

Concessione delle risorse del computer ad altre applicazioni

Il consumo di risorse del computer durante la scansione del computer può aumentare il carico sui sottosistemi della CPU e del disco rigido. Per risolvere il problema dell'esecuzione simultanea che determina un aumento del carico sulla CPU e sui sottosistemi del disco, Kaspersky Endpoint Security può concedere risorse ad altre applicazioni.

Utilizzo di Tecnologia Avanzata di Disinfezione

Le attuali applicazioni dannose possono penetrare nei livelli più bassi di un sistema operativo, rendendone praticamente impossibile l'eliminazione. Se vengono rilevate attività dannose nel sistema operativo, Kaspersky Endpoint Security esegue una procedura di disinfezione approfondita utilizzando una speciale Tecnologia Avanzata di Disinfezione. La *Tecnologia Avanzata di Disinfezione* è progettata per eliminare dal sistema operativo le applicazioni dannose che hanno già avviato i propri processi nella RAM e che impediscono a Kaspersky Endpoint Security di rimuoverli con altri metodi. Come risultato, la minaccia viene neutralizzata. Mentre la disinfezione avanzata è in corso, è consigliabile evitare di avviare nuovi processi o modificare il registro del sistema operativo. La Tecnologia Avanzata di Disinfezione utilizza considerevoli risorse del sistema operativo, pertanto potrebbe rallentare le altre applicazioni.

Al termine del processo di disinfezione avanzata in un computer con un sistema operativo Microsoft Windows per workstation, Kaspersky Endpoint Security richiede all'utente di consentire il riavvio del computer. Dopo il riavvio del sistema, Kaspersky Endpoint Security elimina i file del malware e avvia una scansione completa "non approfondita" del computer.

La richiesta di riavvio è impossibile in un computer con un sistema operativo Microsoft Windows per server a causa delle specifiche di Kaspersky Endpoint Security. Un riavvio non pianificato di un file server può comportare problemi di temporanea non disponibilità dei dati del file server o di perdita dei dati non salvati. È consigliabile riavviare un file server solo in base alla pianificazione. Per questo motivo, la Tecnologia Avanzata di Disinfezione è disabilitata per impostazione predefinita per i file server.

Se viene rilevata un'infezione attiva in un file server, viene inviato un evento a Kaspersky Security Center che indica che è necessaria la Disinfezione avanzata. Per disinfettare l'infezione attiva di un server, abilitare la tecnologia Disinfezione avanzata per i server e avviare un'attività di gruppo *Scansione malware* in un momento appropriato per gli utenti del server.

Abilitazione o disabilitazione della modalità di risparmio energetico

Modalità di risparmio energetico è una funzionalità che riduce il carico sulle risorse del laptop e prolunga la durata della batteria senza compromettere in modo significativo il livello di sicurezza. In modalità di risparmio energetico, l'applicazione limita l'avvio delle attività pianificate. In questo modo, la modalità di risparmio energetico garantisce l'equilibrio tra il livello di protezione e la durata della batteria del laptop.

Quando è abilitata la modalità di risparmio energetico e il computer è alimentato a batteria, le attività seguenti non vengono eseguite anche se sono pianificate:

- *Scansione completa*.
- *Scansione delle aree critiche*.
- *Scansione personalizzata*.
- *Controllo integrità applicazione*.
- *Scansione IOC*.
- *Aggiornamento di database e moduli dell'applicazione* (solo patch)

L'applicazione ignora gli aggiornamenti pianificati del database solo quando il laptop è alimentato a batteria e il livello della batteria è inferiore al 30% (valore predefinito). È possibile modificare il livello minimo di carica della batteria a partire dal quale l'applicazione inizia a ignorare gli aggiornamenti pianificati dei database antivirus modificando il Registro di sistema (vedere le istruzioni di seguito). In tutti gli altri casi, Kaspersky Endpoint Security aggiorna i database in base alla pianificazione, indipendentemente dal fatto che il laptop sia collegato o alimentato a batteria oppure che l'applicazione sia in modalità di risparmio energetico.

Come abilitare o disabilitare la modalità di risparmio energetico in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni applicazione**.

5. Nel blocco **Prestazioni**, utilizzare la casella di controllo **Rimanda attività pianificate durante l'alimentazione a batteria** per abilitare o disabilitare la modalità di risparmio batteria.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare la modalità di risparmio energetico in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Prestazioni**.

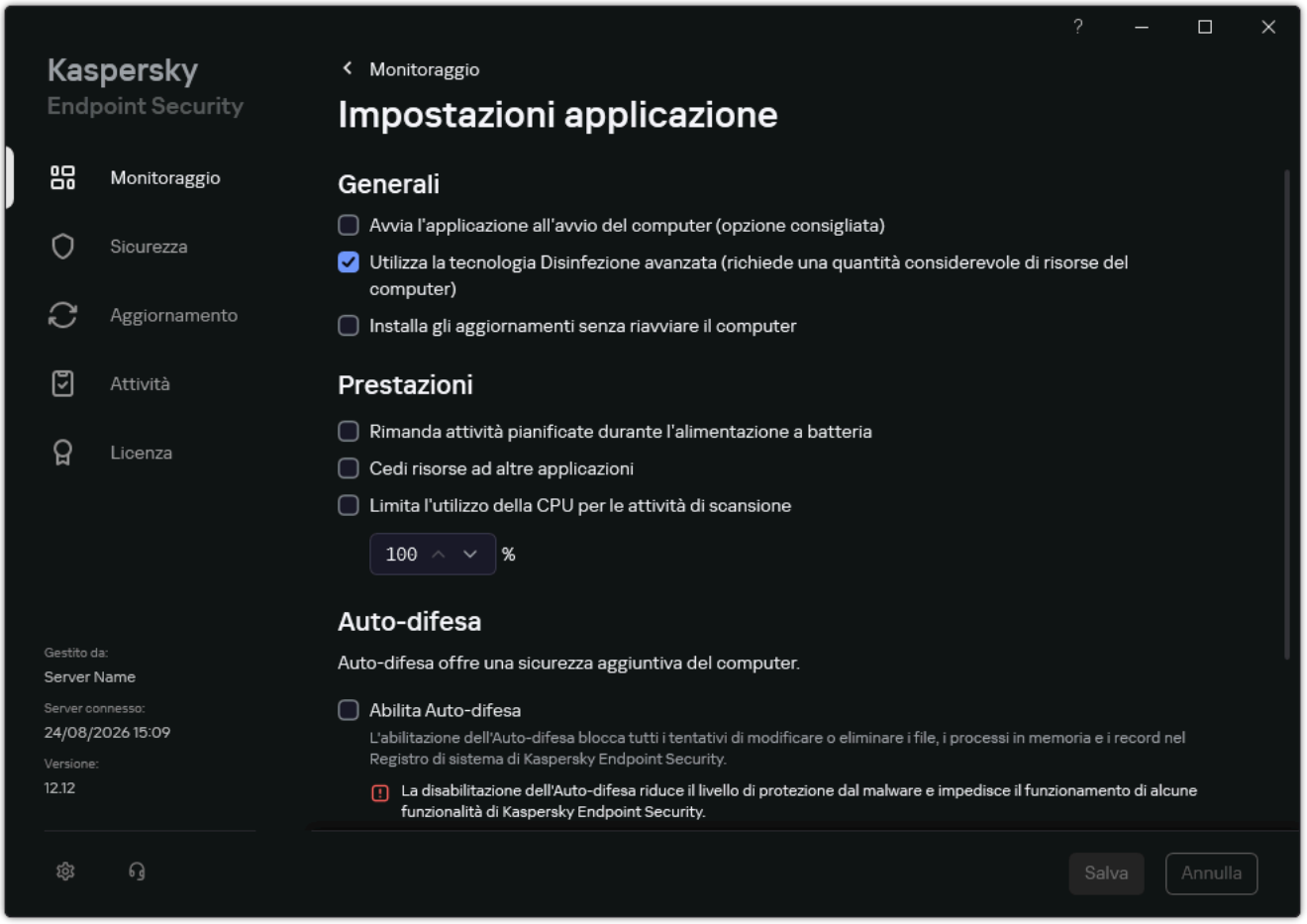
5. Nel blocco **Rimanda o ignora attività pianificate durante l'alimentazione a batteria**, utilizzare la casella di controllo **Rimanda o ignora attività pianificate durante l'alimentazione a batteria (in base al sistema operativo)** per abilitare o disabilitare la modalità di risparmio batteria.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare la modalità di risparmio energetico nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.



Impostazioni di Kaspersky Endpoint Security for Windows

3. Nel blocco **Prestazioni**, utilizzare la casella di controllo **Rimanda attività pianificate durante l'alimentazione a batteria** per abilitare o disabilitare la modalità di risparmio batteria.

4. Salvare le modifiche.

Come modificare il livello minimo di carica a partire dal quale l'applicazione inizia a ignorare gli aggiornamenti pianificati dei database antivirus

1. Aprire l'editor del Registro di sistema nel computer.

2. Nell'editor del Registro di sistema passare alla sezione seguente:

   - Per i sistemi operativi a 64 bit:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`

   - Per i sistemi operativi a 32 bit:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`

3. Aprire `UpdaterAccumulatorThreshold` per la modifica.

4. Specificare il livello minimo di carica a partire dal quale l'applicazione inizia a ignorare gli aggiornamenti pianificati dei database antivirus.

Abilitazione o disabilitazione della concessione di risorse ad altre applicazioni

Il consumo di risorse del computer da parte di Kaspersky Endpoint Security durante la scansione del computer può aumentare il carico sui sottosistemi della CPU e del disco rigido. Ciò potrebbe rallentare altre applicazioni. Per ottimizzare le prestazioni, Kaspersky Endpoint Security fornisce una *modalità per trasferire le risorse ad altre applicazioni*. In questa modalità, il sistema operativo può ridurre la priorità dei thread delle attività di scansione di Kaspersky Endpoint Security quando il carico della CPU è elevato. In questo modo, è possibile ridistribuire le risorse del sistema operativo ad altre applicazioni. Pertanto, le attività di scansione riceveranno meno tempo di CPU. Di conseguenza, Kaspersky Endpoint Security impiegherà più tempo per eseguire la scansione del computer. Per impostazione predefinita, l'applicazione è configurata in modo da cedere risorse ad altre applicazioni.

Come abilitare o disabilitare la concessione di risorse ad altre applicazioni in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni applicazione**.

4. Nel blocco **Prestazioni**, utilizzare la casella di controllo **Cedi risorse ad altre applicazioni** per abilitare o disabilitare la concessione di risorse ad altre applicazioni.

5. Salvare le modifiche.

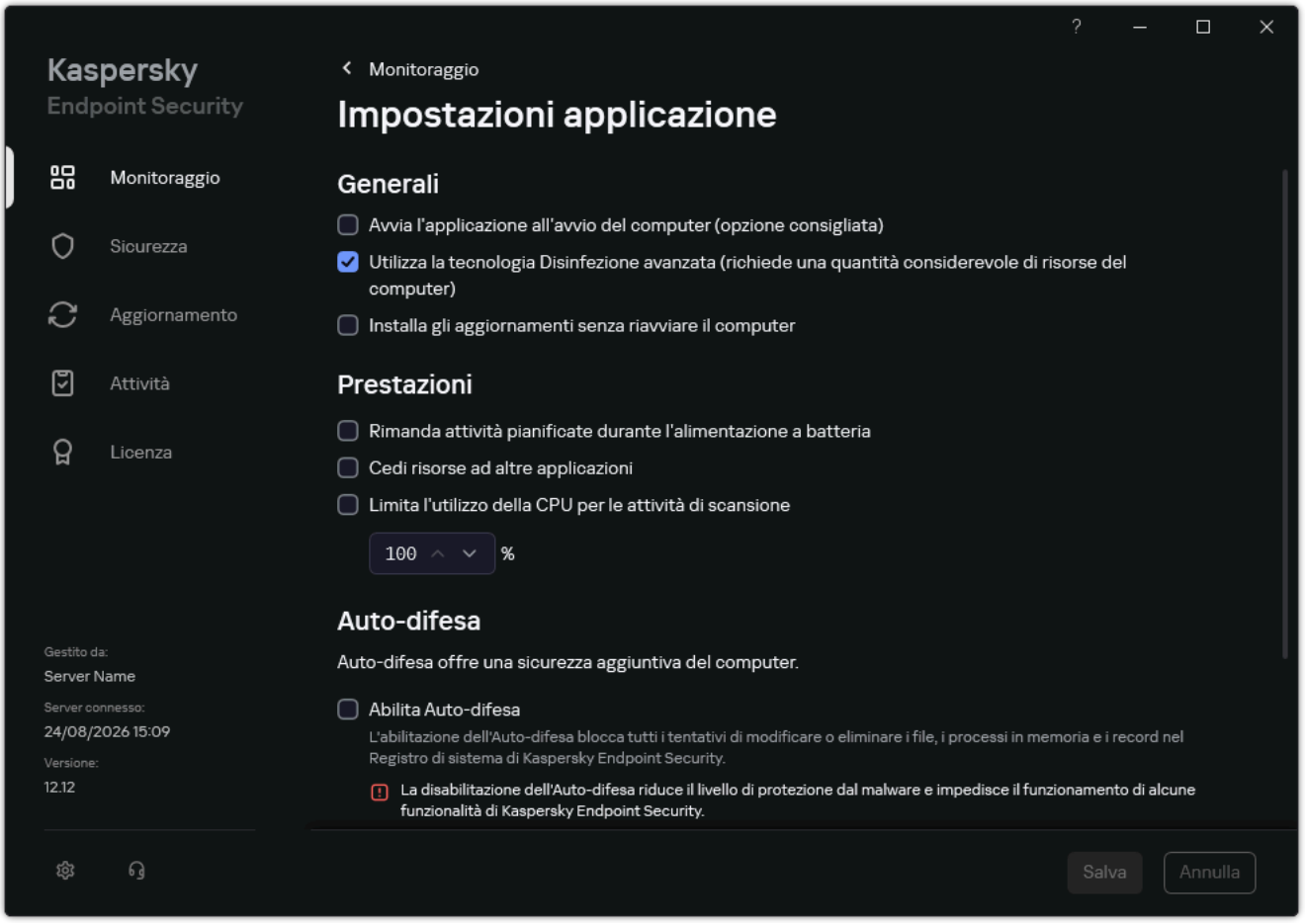
Come abilitare o disabilitare la concessione di risorse ad altre applicazioni in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Prestazioni**.
5. Nel blocco **Cedi risorse ad altre applicazioni**, utilizzare l'interruttore **Cedi risorse ad altre applicazioni** per abilitare o disabilitare la concessione di risorse ad altre applicazioni.
6. Salvare le modifiche.

Come abilitare o disabilitare la concessione di risorse ad altre applicazioni nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.



Impostazioni di Kaspersky Endpoint Security for Windows

3. Nel blocco **Prestazioni**, utilizzare la casella di controllo **Cedi risorse ad altre applicazioni** per abilitare o disabilitare la concessione di risorse ad altre applicazioni.
4. Salvare le modifiche.

Best practice per l'ottimizzazione delle prestazioni di Kaspersky Endpoint Security

Durante la distribuzione di Kaspersky Endpoint Security for Windows, è possibile attenersi ai seguenti suggerimenti per configurare la protezione del computer e ottimizzare le prestazioni. Per ulteriori informazioni su come gestire i problemi di prestazioni del computer, consultare la Knowledge Base dell'Assistenza tecnica.

Generale

Configurare le impostazioni generali dell'applicazione in base ai seguenti suggerimenti:

1. Effettuare l'upgrade di Kaspersky Endpoint Security all'ultima versione.

   Nelle versioni più recenti dell'applicazione sono stati risolti alcuni errori, la stabilità è stata migliorata e le prestazioni sono state ottimizzate.

2. Abilitare i componenti della protezione con le impostazioni predefinite.

   Le impostazioni predefinite sono considerate ottimali. Queste impostazioni sono consigliate dagli esperti di Kaspersky. Le impostazioni predefinite forniscono il livello di protezione consigliato e un utilizzo ottimale delle risorse. Se necessario, è possibile ripristinare le impostazioni predefinite dell'applicazione.

3. Abilitare le funzionalità di ottimizzazione delle prestazioni dell'applicazione.

   L'applicazione è dotata di funzionalità di ottimizzazione delle prestazioni: modalità di risparmio energetico e concessione di risorse ad altre applicazioni. Accertarsi che tali opzioni siano abilitate.

Scansione malware sulle workstation

Si consiglia di abilitare Scansione in background per la scansione malware delle workstation. *Scansione in background* è una modalità di scansione di Kaspersky Endpoint Security che non mostra notifiche per l'utente. La scansione in background richiede meno risorse del computer rispetto ad altri tipi di scansioni (ad esempio la scansione completa). In questa modalità, Kaspersky Endpoint Security esegue la scansione degli oggetti di avvio, del settore di avvio, della memoria di sistema e della partizione di sistema. Le impostazioni di scansione in background sono considerate ottimali. Queste impostazioni sono consigliate dagli esperti di Kaspersky. Pertanto, per eseguire una scansione malware del computer, è possibile utilizzare solo la modalità di scansione in background senza utilizzare altre attività di scansione.

Se la scansione in background non soddisfa le proprie esigenze, configurare l'attività *Scansione malware* in base ai seguenti suggerimenti:

1. Impostare un limite per il consumo di risorse CPU durante la scansione del computer.

   È possibile limitare l'utilizzo della CPU durante l'esecuzione dell'attività *Scansione malware*. A tale scopo, nelle impostazioni dell'applicazione, specificare la percentuale di carico CPU massima per tutti i core che è possibile utilizzare durante la scansione del computer. Questo potrebbe aumentare il tempo necessario per eseguire la scansione del computer.

2. Configurare la pianificazione della scansione del computer ottimale.

È possibile configurare l'operazione in modo che venga eseguita quando il computer funziona con carico minimo. Ad esempio, è possibile configurare l'esecuzione dell'attività di notte o nei fine settimana.

Se gli utenti spengono il computer al di fuori dell'orario di lavoro, è possibile abilitare la funzione Riattivazione LAN. La funzionalità Wake-on-LAN consente di accendere il computer da remoto inviando un segnale speciale sulla rete locale. Per utilizzare questa funzionalità, è necessario abilitare Wake-on-LAN nelle impostazioni BIOS. È inoltre possibile spegnere automaticamente il computer al termine della scansione.

Se non è possibile configurare una pianificazione di scansione ottimale, impostare le attività in modo che vengano eseguite solo quando il computer è inattivo. Kaspersky Endpoint Security avvia l'attività di scansione se il computer è bloccato o se lo screensaver è attivo. Se l'esecuzione dell'attività è stata interrotta, ad esempio sbloccando il computer, Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui era stata interrotta.

3. Definire un ambito di scansione.

   Selezionare i seguenti oggetti per la scansione (set minimo di ambiti di scansione):

   - Memoria del kernel
   - Processi in esecuzione e oggetti di avvio
   - Settori di avvio
   - %systemroot% (escluse le sottocartelle)
   - %systemroot%\System (escluse le sottocartelle)
   - %systemroot%\System32 (escluse le sottocartelle)
   - %systemroot%\System32\drivers (escluse le sottocartelle)
   - %systemroot%\SysWOW64 (escluse le sottocartelle)
   - %systemroot%\SysWOW64\drivers (escluse le sottocartelle)

4. Attivare le tecnologie iSwift e iChecker.

   - Tecnologia iSwift.

     Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.

   - Tecnologia iChecker.

     Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

   È possibile attivare le tecnologie iSwift e iChecker solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security. Non è possibile attivare queste tecnologie in Kaspersky Security Center Web Console.

5. Disabilitare la scansione degli archivi protetti da password.

   Se la scansione degli archivi protetti da password è abilitata, viene visualizzata una richiesta di password prima di eseguire la scansione dell'archivio. Poiché si consiglia di pianificare l'attività durante le ore di inattività, l'utente non può immettere la password. È possibile esaminare manualmente gli archivi protetti da password.

6. Disabilitare l'avvio simultaneo di diverse attività di scansione.

   Kaspersky Endpoint Security accoderà le nuove attività di scansione se la scansione corrente continua. In questo modo, è possibile ottimizzare il carico sul computer.

Scansione malware nei server

Configurare l'attività *Scansione malware* in base ai seguenti suggerimenti:

1. Impostare un limite per il consumo di risorse CPU durante la scansione del computer.

   È possibile limitare l'utilizzo della CPU durante l'esecuzione dell'attività *Scansione malware*. A tale scopo, nelle impostazioni dell'applicazione, specificare la percentuale di carico CPU massima per tutti i core che è possibile utilizzare durante la scansione del computer. Questo potrebbe aumentare il tempo necessario per eseguire la scansione del computer.

2. Configurare la pianificazione della scansione del computer ottimale.

   È possibile configurare l'operazione in modo che venga eseguita quando il computer funziona con carico minimo. Ad esempio, è possibile configurare l'esecuzione dell'attività di notte o nei fine settimana.

3. Attivare le tecnologie iSwift e iChecker.

   - Tecnologia iSwift.

     Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.

   - Tecnologia iChecker.

     Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

   È possibile attivare le tecnologie iSwift e iChecker solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security. Non è possibile attivare queste tecnologie in Kaspersky Security Center Web Console.

4. Disabilitare la scansione degli archivi protetti da password.

   Se la scansione degli archivi protetti da password è abilitata, viene visualizzata una richiesta di password prima di eseguire la scansione dell'archivio. Poiché si consiglia di pianificare l'attività durante le ore di inattività, l'utente non può immettere la password. È possibile esaminare manualmente gli archivi protetti da password.

5. Disabilitare l'avvio simultaneo di diverse attività di scansione.

   Kaspersky Endpoint Security accoderà le nuove attività di scansione se la scansione corrente continua. In questo modo, è possibile ottimizzare il carico sul computer.

Kaspersky Security Network

Per proteggere il computer in modo più efficace, Kaspersky Endpoint Security utilizza dati ricevuti dagli utenti di tutto il mondo. L'acquisizione di questi dati viene eseguita tramite Kaspersky Security Network.

Kaspersky Security Network (KSN) è un'infrastruttura di servizi cloud che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce risposte più rapide da parte di Kaspersky Endpoint Security alle nuove minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi positivi. Se si partecipa a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla reputazione degli indirizzi Web scansionati, nonché informazioni sulla categoria e sulla reputazione dei file scansionati.

Modificare le impostazioni di Kaspersky Security Network in base ai seguenti suggerimenti:

1. Disabilitare la modalità KSN estesa.

   Modalità KSN estesa è una modalità in cui Kaspersky Endpoint Security invia dati aggiuntivi a Kaspersky.

2. Configurare Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN) è una soluzione che consente agli utenti di computer che ospitano Kaspersky Endpoint Security o altre applicazioni Kaspersky di ottenere l'accesso ai database di reputazione di Kaspersky e ad altri dati statistici senza inviare dati a Kaspersky dai propri computer.

3. Abilitare la modalità cloud.

   La *Modalità cloud* fa riferimento alla modalità operativa dell'applicazione in cui Kaspersky Endpoint Security utilizza una versione leggera dei database anti-virus. Kaspersky Security Network supporta il funzionamento dell'applicazione con l'utilizzato dei database anti-virus leggeri. La versione leggera dei database anti-virus consente di utilizzare circa la metà della RAM del computer che altrimenti verrebbe utilizzata con i database standard. Se non si partecipa a Kaspersky Security Network o se la modalità cloud è disabilitata, Kaspersky Endpoint Security scarica la versione completa dei database anti-virus dai server di Kaspersky.

Scansione malware

Una scansione malware è essenziale per la sicurezza del computer. L'esecuzione periodica delle scansioni malware consente di eliminare la possibilità che si diffondano malware non rilevati dai componenti della protezione, perché è stato impostato un livello di protezione basso o per altri motivi.

Kaspersky Endpoint Security non esegue la scansione dei file i cui contenuti si trovano nell'archivio cloud OneDrive e crea voci di registro indicanti che i file non sono stati esaminati.

Scansione completa

Una scansione approfondita dell'intero computer. Kaspersky Endpoint Security esamina i seguenti oggetti:

- Memoria del kernel
- Oggetti caricati all'avvio del sistema operativo
- Settori di avvio
- Backup del sistema operativo
- Tutti i dischi rigidi e le unità rimovibili

Gli esperti di Kaspersky consigliano di non modificare l'ambito della scansione delle attività *Scansione completa*.

Per ridurre l'utilizzo delle risorse del computer, è consigliabile utilizzare un'attività di scansione in background anziché un'attività di scansione completa. Questo non influenzerà il livello di sicurezza del computer.

Scansione delle aree critiche

Per impostazione predefinita, Kaspersky Endpoint Security esamina la memoria del kernel, i processi in esecuzione e i settori di avvio del disco.

Gli esperti di Kaspersky consigliano di non modificare l'ambito della scansione delle attività *Scansione delle aree critiche*.

Scansione personalizzata

Kaspersky Endpoint Security esegue la scansione degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi dei seguenti oggetti:

- Memoria del sistema
- Oggetti caricati all'avvio del sistema operativo
- Backup del sistema operativo
- Dischi rigidi, unità rimovibili e di rete
- Qualsiasi file selezionato

Scansione in background

Scansione in background è una modalità di scansione di Kaspersky Endpoint Security che non mostra notifiche per l'utente. La scansione in background richiede meno risorse del computer rispetto ad altri tipi di scansioni (ad esempio la scansione completa). In questa modalità, Kaspersky Endpoint Security esegue la scansione degli oggetti di avvio, del settore di avvio, della memoria di sistema e della partizione di sistema.

Controllo integrità applicazione

Kaspersky Endpoint Security verifica se i moduli dell'applicazione risultano danneggiati o modificati.

Scansione del computer

Una scansione è essenziale per la sicurezza del computer. L'esecuzione periodica delle scansioni malware consente di eliminare la possibilità che si diffondano malware non rilevati dai componenti della protezione, perché è stato impostato un livello di protezione basso o per altri motivi. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica.

Kaspersky Endpoint Security dispone delle seguenti attività standard predefinite: *Scansione completa*, *Scansione delle aree critiche*, *Scansione personalizzata*. Se l'organizzazione ha distribuito il sistema di amministrazione di Kaspersky Security Center, è possibile creare un'attività *Scansione malware* e configurare la scansione.

Come eseguire un'attività di scansione in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Attività**.

3. Selezionare l'attività di scansione e fare doppio clic per aprire le proprietà dell'attività.

   Se necessario, creare l'attività *Scansione malware*.

4. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.

5. Configurare l'attività di scansione (vedere la tabella riportata di seguito).

   Se necessario, configurare la pianificazione dell'attività di scansione.

6. Salvare le modifiche.

7. Eseguire l'attività di scansione.

Kaspersky Endpoint Security avvierà la scansione del computer. Se l'utente ha interrotto l'esecuzione dell'attività (ad esempio spegnendo il computer), Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui la scansione era stata interrotta.

Come eseguire un'attività di scansione in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività di scansione.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Configurare l'attività di scansione (vedere la tabella riportata di seguito).

   Se necessario, configurare la pianificazione dell'attività di scansione.

5. Salvare le modifiche.

6. Eseguire l'attività di scansione.

Kaspersky Endpoint Security avvierà la scansione del computer. Se l'utente ha interrotto l'esecuzione dell'attività (ad esempio spegnendo il computer), Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui la scansione era stata interrotta.

Come eseguire un'attività di scansione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.

2. Nell'elenco delle attività, selezionare l'attività di scansione e fare clic su ⚙.

> Se l'attività di scansione non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

> Nell'interfaccia dell'applicazione è possibile configurare solo le attività di scansione locali: *Scansione completa*, *Scansione delle aree critiche*, *Scansione personalizzata*. Non è possibile configurare nell'interfaccia dell'applicazione le attività di gruppo aggiunte tramite la Console di Kaspersky Security Center. Il pulsante ⚙ non viene visualizzato per le attività di gruppo.

3. Configurare l'attività di scansione (vedere la tabella riportata di seguito).

   Se necessario, configurare la pianificazione dell'attività di scansione.

4. Salvare le modifiche.

5. Eseguire l'attività di scansione.

   Kaspersky Endpoint Security avvierà la scansione del computer. L'applicazione mostrerà l'avanzamento della scansione, il numero di file esaminati e il tempo di scansione rimanente. È possibile interrompere l'attività in qualsiasi momento facendo clic sul pulsante **Interrompi**.

Per ottimizzare le prestazioni di Kaspersky Endpoint Security durante la scansione del computer, è possibile gestire le impostazioni avanzate dell'attività *Scansione completa* e limitare l'utilizzo delle risorse della CPU.

In Kaspersky Security Center, è inoltre possibile utilizzare l'attività *Scansione in background* anziché l'attività *Scansione completa* per ottimizzare le prestazioni dell'applicazione. Questo non influenzerà il livello di sicurezza del computer. La scansione in background non può essere configurata.

Di conseguenza, Kaspersky Endpoint Security esegue la scansione del computer e, se viene rilevata una minaccia, esegue l'azione configurata nelle impostazioni dell'applicazione. In genere, l'applicazione tenta di disinfettare i file infetti. Di conseguenza, i file infetti possono ricevere i seguenti stati:

- **Rimandato**. Non è stato possibile disinfettare il file infetto. L'applicazione elimina il file infetto dopo il riavvio del computer.
- **Registrato**. Non è stato possibile disinfettare il file infetto. L'applicazione aggiunge informazioni sui file infetti rilevati all'elenco delle minacce attive.
- **Scrittura non supportata** o **Errore di scrittura**. Non è stato possibile disinfettare il file infetto. L'applicazione non ha accesso in scrittura.
- **Già elaborato**. L'applicazione ha rilevato un file infetto in precedenza. L'applicazione disinfetta o elimina il file infetto dopo il riavvio del computer.

Impostazioni di scansione

Parametro	Descrizione
Livello di sicurezza	Kaspersky Endpoint Security può utilizzare diversi gruppi di impostazioni per eseguire una scansione. I gruppi di impostazioni archiviate nell'applicazione sono denominati *livelli di protezione*: • **Alto**. Kaspersky Endpoint Security esegue la scansione di tutti i tipi di file. Durante la scansione dei file compositi, l'applicazione esegue la scansione di archivi, pacchetti di distribuzione, file dei formati Office, ma non degli archivi protetti da password. Quando è impostato questo livello di protezione, l'applicazione utilizza l'analisi euristica con il livello di dettaglio **Approfondita**. • **Consigliato**. Kaspersky Endpoint Security esegue la scansione di tutti i tipi di file. Durante la scansione dei file compositi, l'applicazione esegue la scansione di archivi, pacchetti di distribuzione, file dei formati Office, ma non degli archivi protetti da password. Quando è impostato questo livello di protezione, l'applicazione utilizza l'analisi euristica con il livello di dettaglio **Media**. • **Basso**. Kaspersky Endpoint Security esegue la scansione solo dei formati file specificati. Durante la scansione dei file compositi, l'applicazione esegue la scansione di archivi, pacchetti di distribuzione, file dei formati Office, ma non degli archivi protetti da password. Quando è impostato questo livello di protezione, l'applicazione utilizza l'analisi euristica con il livello di dettaglio **Superficiale**. È possibile selezionare uno dei livelli di protezione preimpostati o configurare manualmente le impostazioni del livello di protezione. Se si modificano le impostazioni del livello di sicurezza dei file, è possibile ripristinare in qualsiasi momento le impostazioni consigliate.

Parametro	Descrizione
Azione se viene rilevata una minaccia	**Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato. **Disinfetta (se la disinfezione non riesce, informa)**. Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive. **Informa**. Se questa opzione è selezionata, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti all'elenco delle minacce attive in caso di rilevamento di tali file. Prima di tentare di disinfettare o eliminare un file infetto, l'applicazione crea una copia di backup del file nel caso in cui sia necessario ripristinare il file o se può essere disinfettato in futuro. Se vengono rilevati file infetti che fanno parte dell'applicazione Windows Store, Kaspersky Endpoint Security tenta di eliminare il file.
Esegui immediatamente Disinfezione avanzata *(disponibile solo in Kaspersky Security Center Console)*	La disinfezione avanzata durante un'attività di scansione virus in un computer viene eseguita solo se la funzionalità Disinfezione avanzata è abilitata nelle proprietà del criterio applicato al computer. Se la casella di controllo è selezionata, Kaspersky Endpoint Security rimuove l'infezione attiva immediatamente dopo che è stata rilevata durante l'esecuzione dell'attività di scansione virus. Una volta rimossa l'infezione attiva, Kaspersky Endpoint Security riavvia il computer senza chiedere conferma all'utente. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non rimuovere l'infezione attiva immediatamente dopo che è stata rilevata durante l'esecuzione dell'attività di scansione virus. Kaspersky Endpoint Security genera eventi di infezione attivi nei rapporti delle applicazioni locali e sul lato Kaspersky Security Center. L'infezione attiva può essere rimossa quando l'attività di scansione virus viene rieseguita con la funzionalità Disinfezione avanzata attivata. In questo modo, l'amministratore di sistema può scegliere l'ora appropriata per eseguire la disinfezione avanzata e successivamente riavviare automaticamente i computer.
Ambito della scansione	Elenco di oggetti esaminati da Kaspersky Endpoint Security durante l'esecuzione di un'attività di scansione. Gli oggetti nell'ambito della scansione possono includere memoria kernel, processi in esecuzione, settori di avvio, archivio di backup di sistema, disco rigido, unità rimovibile o unità di rete, cartelle o file. In Kaspersky Endpoint Security for Windows 12.12, l'e-mail è esclusa dall'ambito della scansione dell'applicazione. La scansione dei messaggi e-mail in entrata e in uscita viene eseguita dal componente Protezione minacce di posta. Se si utilizza una versione precedente del plug-in di gestione, l'applicazione esclude la posta elettronica dall'ambito di scansione, anche se il criterio la include.
Pianificazione scansione	**Manualmente**. Modalità di esecuzione in cui è possibile avviare la scansione manualmente nel momento più opportuno. **In base alla pianificazione**. In questa modalità di esecuzione dell'attività di scansione, l'applicazione avvia l'attività di scansione in base alla pianificazione creata dall'utente. Se si seleziona questa modalità di esecuzione dell'attività di scansione, è anche possibile avviare l'attività di scansione manualmente.
Rimanda l'esecuzione dopo l'avvio dell'applicazione di N minuti	Avvio rimandato dell'attività di scansione dopo l'avvio dell'applicazione. All'avvio del sistema operativo, molti processi sono in esecuzione, pertanto è preferibile rimandare l'attività di scansione anziché eseguirla immediatamente dopo l'avvio di Kaspersky Endpoint Security.
Esegui attività ignorate	Se la casella di controllo è selezionata, Kaspersky Endpoint Security avvia l'attività ignorata appena possibile. L'attività può ad esempio essere ignorata se il computer è spento all'orario impostato per l'avvio dell'attività pianificata. Quando l'applicazione ha l'opportunità di eseguire le attività non effettuate, esegue le attività in modo casuale entro un determinato intervallo di tempo per distribuire il carico sul computer. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non esegue le attività ignorate. Viene invece eseguita l'attività successiva, in base alla pianificazione corrente.
Esegui solo quando il computer è inattivo	Avvio posticipato dell'attività quando le risorse del computer sono occupate. Kaspersky Endpoint Security avvia l'attività di scansione se il computer è bloccato o se lo screensaver è attivo. Se l'esecuzione dell'attività è stata interrotta, ad esempio sbloccando il computer, Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui era stata interrotta. Questa opzione di pianificazione consente di conservare le risorse del computer durante l'utilizzo del computer.

Parametro	Descrizione
Esegui scansione come	Per impostazione predefinita, l'attività di scansione viene eseguita per conto dell'utente i cui diritti sono registrati nel sistema operativo. L'ambito della protezione può includere unità di rete o altri oggetti che richiedono diritti di accesso speciali. È possibile specificare un utente che dispone dei diritti appropriati nelle impostazioni dell'applicazione ed eseguire l'attività di scansione tramite l'account di questo utente.
Tipi di file	Kaspersky Endpoint Security considera i file privi di estensione come eseguibili. I file eseguibili vengono sempre esaminati, indipendentemente dai tipi di file selezionati per la scansione. **Tutti i file**. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina tutti i file senza eccezioni (tutti i formati e le estensioni). **File esaminati per formato**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Prima di esaminare un file alla ricerca di codice dannoso, viene analizzata l'intestazione interna del file per determinarne il formato (ad esempio, .txt, .doc o .exe). La scansione cerca inoltre i file con estensioni file particolari. **File esaminati per estensione**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Il formato del file viene quindi determinato in base all'estensione. Per impostazione predefinita, Kaspersky Endpoint Security esegue la scansione dei file in base al loro formato. La scansione dei file per estensione è meno sicura perché un file dannoso può avere un'estensione che non è nell'elenco dei file potenzialmente infettabili (ad esempio, `.123`).
Esamina solo i file nuovi e modificati	Esamina solo i nuovi file e i file che sono stati modificati dopo l'ultima scansione. Questo consente di ridurre la durata di una scansione. Questa modalità si applica sia ai file semplici che compositi.
Ignora i file esaminati per più di N secondi	Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione.
Non eseguire più attività di scansione contemporaneamente	Ritardare le attività di scansione pianificata se una scansione pianificata avviata in precedenza è ancora in esecuzione. Kaspersky Endpoint Security metterà in coda le attività di scansione pianificata se la scansione corrente è ancora in esecuzione. In questo modo, è possibile ottimizzare il carico sul computer. Ad esempio, sono state pianificate attività di scansione da eseguire alle 18:00 e alle 20:00. Kaspersky Endpoint Security rinvierà l'attività di scansione delle 20:00 se l'attività di scansione pianificata per le 18:00 è ancora in esecuzione. L'applicazione eseguirà una scansione al termine dell'attività avviata alle 18:00. Tuttavia, Kaspersky Endpoint Security avvia immediatamente un'attività di scansione anche se è in esecuzione una delle seguenti attività di scansione: • Scansione delle unità rimovibili al momento della connessione. • Scansione dal menu di scelta rapida. • Scansione delle aree critiche avviata quando viene rilevato un indicatore di compromissione (IoC). Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security consente di eseguire più attività di scansione contemporaneamente. L'esecuzione di più attività di scansione richiede più risorse di elaborazione.
Esamina gli archivi	Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio).
Esamina i pacchetti di distribuzione	Scansione dei pacchetti di distribuzione delle applicazioni di terze parti.
Esamina i file nei formati Microsoft Office	Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE. L'applicazione analizza i file in formato Office di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.

Parametro	Descrizione
Esamina i file in formato e-mail	Scansione dei file in formato e-mail e del database delle e-mail. L'applicazione esamina i file PST e OST utilizzati dai client di posta MS Outlook e Windows Mail, nonché i file EML. Kaspersky Endpoint Security non supporta la versione a 64 bit del client di posta Microsoft Outlook. Di conseguenza, Kaspersky Endpoint Security non esegue la scansione dei file Microsoft Outlook (file PST e OST) se nel computer è installata una versione a 64 bit di Microsoft Outlook, anche se la posta è inclusa nell'ambito della scansione. Se la casella di controllo è selezionata, Kaspersky Endpoint Security suddivide il file in formato e-mail nei relativi componenti (intestazione, corpo e allegati) e li analizza alla ricerca di potenziali minacce. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security analizza il file in formato e-mail come un singolo file. Quando un oggetto dannoso viene individuato nei file PST o OST, Kaspersky Endpoint Security lo rende innocuo in base all'azione selezionata (ad esempio, la disinfezione o l'eliminazione del file). Se vengono rilevati oggetti dannosi nei file di altri client e-mail, ad esempio Mozilla Thunderbird, Kaspersky Endpoint Security non disinfetta né elimina tali file per evitare l'eliminazione indesiderata dei messaggi e-mail. Kaspersky Endpoint Security aggiunge solo le informazioni sugli oggetti rilevati all'elenco delle minacce attive. È necessario eliminare le e-mail contenenti file dannosi negli allegati tramite l'interfaccia utente del client di posta. Se per qualsiasi motivo non è possibile eliminare i messaggi contenenti oggetti dannosi, è possibile gestire tali minacce nell'interfaccia utente di Kaspersky Endpoint Security aggiungendo gli oggetti rilevati all'elenco delle esclusioni dalla scansione.
Esamina gli archivi protetti da password	Se la casella di controllo è selezionata, l'applicazione esamina gli archivi protetti tramite password. Prima di eseguire la scansione dei file in un archivio, viene richiesto di immettere la password. Se la casella di controllo è deselezionata, l'applicazione ignora la scansione degli archivi protetti tramite password.
Non decomprimere i file compositi di grandi dimensioni	Se la casella di controllo è selezionata, l'applicazione non esegue la scansione dei file compositi se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, l'applicazione esamina i file compositi di qualsiasi dimensione. L'applicazione esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Machine Learning e analisi delle firme	Il metodo Machine Learning e analisi delle firme utilizza i database di Kaspersky Endpoint Security, che contengono le descrizioni delle minacce conosciute, nonché i metodi per neutralizzarle. La protezione che utilizza questo metodo fornisce il livello di sicurezza minimo accettabile. In base ai suggerimenti degli esperti Kaspersky, il metodo Machine Learning e analisi delle firme è sempre abilitato.
Analisi euristica	Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto. Durante la scansione dei file alla ricerca di codice dannoso, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.
Tecnologia iSwift *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.
Tecnologia iChecker *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

Scansione delle unità rimovibili quando vengono connesse al computer

Kaspersky Endpoint Security esamina tutti i file eseguiti o copiati, anche se il file si trova in un'unità rimovibile (componente Protezione minacce file). Per evitare la diffusione di virus e altro malware, è possibile configurare scansioni automatiche delle unità rimovibili quando sono collegate al computer. Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati. Il componente protegge costantemente un computer eseguendo scansioni che implementano machine learning, analisi euristica (alto livello) e analisi delle firme. Kaspersky Endpoint Security utilizza anche le tecnologie di ottimizzazione delle scansioni iSwift e iChecker. Le tecnologie sono sempre disponibili e non possono essere disattivate.

Come configurare l'esecuzione di Scansione unità rimovibili in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Attività locali** → **Scansione unità rimovibili**.
4. Nell'elenco a discesa **Azione alla connessione di un'unità rimovibile**, selezionare **Scansione dettagliata** o **Scansione rapida**.
5. Configurare le opzioni avanzate per Scansione unità rimovibili (vedere la tabella riportata di seguito).
6. Salvare le modifiche.

Come configurare l'esecuzione di Scansione unità rimovibili in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Scansione unità rimovibili**.
5. Utilizzare l'interruttore **Scansione unità rimovibili ABILITATA** per abilitare o disabilitare il componente.
6. Nel blocco **Tipo di scansione**, selezionare **Scansione dettagliata** o **Scansione rapida**.
7. Configurare le opzioni avanzate per Scansione unità rimovibili (vedere la tabella riportata di seguito).
8. Salvare le modifiche.

Come configurare l'esecuzione di Scansione unità rimovibili nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.
2. Nell'elenco delle attività, selezionare l'attività di scansione e fare clic su .

3. Utilizzare l'interruttore **Scansione unità rimovibili** per abilitare o disabilitare le scansioni delle unità rimovibili al momento della connessione al computer.

4. Configurare le opzioni avanzate per Scansione unità rimovibili (vedere la tabella riportata di seguito).

5. Salvare le modifiche.

A questo punto, Kaspersky Endpoint Security esegue l'attività Scansione unità rimovibili per le unità rimovibili che non sono più grandi della dimensione massima specificata. Se l'attività *Scansione unità rimovibili* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

Impostazioni dell'attività Scansione unità rimovibili

Parametro	Descrizione
Tipo di scansione	**Scansione dettagliata**. Se questa opzione è selezionata, quando viene connessa un'unità rimovibile Kaspersky Endpoint Security esamina tutti i file, inclusi i file annidati in oggetti compositi, archivi, pacchetti di distribuzione e file in formato Office. Kaspersky Endpoint Security non esamina i file nei formati di posta o gli archivi protetti da password. **Scansione rapida**. Se questa opzione è selezionata, quando viene connessa un'unità rimovibile Kaspersky Endpoint Security esamina solo i file con formati specifici che presentano la maggiore vulnerabilità alle infezioni e non decomprime gli oggetti compositi.
Dimensione massima dell'unità (MB)	Se la casella di controllo è selezionata, Kaspersky Endpoint Security esegue l'azione selezionata nell'azione sulle unità rimovibili con una dimensione inferiore alla dimensione massima specificata. Se le dimensioni dell'unità rimovibile superano il valore configurato, Kaspersky Endpoint Security ignora la scansione. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esegue l'azione selezionata sulle unità rimovibili di qualsiasi dimensione.
Nascondi barra di avanzamento della scansione	Se la casella di controllo è selezionata, Kaspersky Endpoint Security visualizza l'avanzamento della scansione delle unità rimovibili in una finestra separata e nella sezione **Attività**. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esegue la scansione delle unità rimovibili in background.
Vieta agli utenti di interrompere la scansione	Se questa casella di controllo è selezionata, per l'attività di scansione delle unità rimovibili nell'interfaccia locale di Kaspersky Endpoint Security, il pulsante **Interrompi** nella sezione **Attività** e il pulsante **Interrompi** nella finestra di scansione delle unità rimovibili non sono disponibili.

Scansione in background

Scansione in background è una modalità di scansione di Kaspersky Endpoint Security che non mostra notifiche per l'utente. La scansione in background richiede meno risorse del computer rispetto ad altri tipi di scansioni (ad esempio la scansione completa). In questa modalità, Kaspersky Endpoint Security esegue la scansione degli oggetti di avvio, del settore di avvio, della memoria di sistema e della partizione di sistema.

Per ridurre l'utilizzo delle risorse del computer, è consigliabile utilizzare un'attività di scansione in background anziché un'attività di scansione completa. Questo non influenzerà il livello di sicurezza del computer. Queste attività hanno lo stesso ambito di scansione. Per ottimizzare il carico sul computer, l'applicazione non esegue contemporaneamente un'attività di scansione completa e un'attività di scansione in background. Se è già stata eseguita un'attività di scansione completa, Kaspersky Endpoint Security non avvierà un'attività di scansione in background per sette giorni dopo il completamento dell'attività di scansione completa.

Viene avviata una scansione in background nei seguenti casi:

- Dopo l'aggiornamento di un database anti-virus.
- 30 minuti dopo l'avvio di Kaspersky Endpoint Security.
- Ogni sei ore.
- Quando il computer è inattivo per cinque minuti o più (il computer è bloccato o lo screensaver è attivo).

La scansione in background quando il computer è inattivo viene interrotta quando si verifica una delle seguenti condizioni:

- Il computer è entrato in modalità attiva.

  Se la scansione in background non viene eseguita da più di dieci giorni, la scansione non viene interrotta.

- Il computer (laptop) è passato alla modalità batteria.

Durante l'esecuzione di una scansione in background, Kaspersky Endpoint Security non esamina i file con contenuti memorizzati in un archivio cloud OneDrive.

Come abilitare la scansione in background in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Attività locali** → **Scansione in background**.
4. Utilizzare la casella di controllo **Abilita scansione in background** per abilitare o disabilitare la scansione in background.
5. Salvare le modifiche.

Come abilitare la scansione in background in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Protezione minacce file**.
5. In **Scansione in background**, utilizzare l'interruttore **Scansione in background ABILITATA** per abilitare o disabilitare la scansione in background.
6. Salvare le modifiche.

Come abilitare la scansione in background nell'interfaccia dell'applicazione

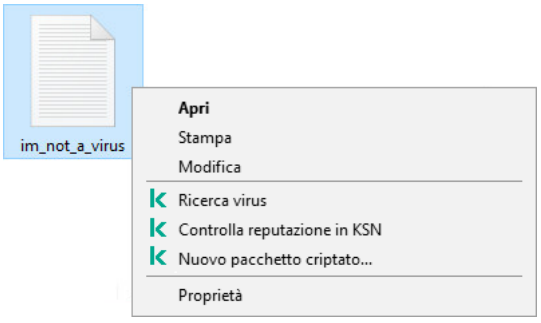
1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.
2. Nell'elenco delle attività, selezionare l'attività di scansione e fare clic su ⚙.
3. Utilizzare l'interruttore **Scansione in background** per abilitare o disabilitare le scansioni in background.
4. Salvare le modifiche.

Se *Scansione in background* non viene visualizzata, significa che l'amministratore ha vietato l'utilizzo delle attività locali nel criterio.

Scansione dal menu di scelta rapida

Kaspersky Endpoint Security consente di eseguire una scansione di file singoli per rilevare virus e altri malware dal menu di scelta rapida (vedere la figura di seguito).

Durante l'esecuzione di una scansione dal menu di scelta rapida, Kaspersky Endpoint Security non esamina i file con contenuti memorizzati in un archivio cloud OneDrive.



Scansione dal menu di scelta rapida

Come configurare Scansione dal menu di scelta rapida in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Attività locali** → **Scansione dal menu di scelta rapida**.
4. Configurare Scansione dal menu di scelta rapida (vedere la tabella riportata di seguito).
5. Salvare le modifiche.

Come configurare Scansione dal menu di scelta rapida in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Protezione minacce file**.
5. In **Scansione dal menu di scelta rapida**, configurare Scansione dal menu di scelta rapida (vedere la tabella riportata di seguito)
6. Salvare le modifiche.

Come configurare Scansione dal menu di scelta rapida nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.
2. Nell'elenco delle attività, selezionare l'attività di scansione e fare clic su ⚙.
3. Configurare Scansione dal menu di scelta rapida (vedere la tabella riportata di seguito).
4. Salvare le modifiche.

Se l'attività *Scansione dal menu di scelta rapida* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

Impostazioni dell'attività Scansione dal menu di scelta rapida

Parametro	Descrizione
Livello di sicurezza	Kaspersky Endpoint Security può utilizzare diversi gruppi di impostazioni per eseguire una scansione. I gruppi di impostazioni archiviate nell'applicazione sono denominati *livelli di protezione*: • **Alto**. Kaspersky Endpoint Security esegue la scansione di tutti i tipi di file. Durante la scansione dei file compositi, l'applicazione esegue la scansione di archivi, pacchetti di distribuzione, file dei formati Office, ma non degli archivi protetti da password. Quando è impostato questo livello di protezione, l'applicazione utilizza l'analisi euristica con il livello di dettaglio **Approfondita**. • **Consigliato**. Kaspersky Endpoint Security esegue la scansione di tutti i tipi di file. Durante la scansione dei file compositi, l'applicazione esegue la scansione di archivi, pacchetti di distribuzione, file dei formati Office, ma non degli archivi protetti da password. Quando è impostato questo livello di protezione, l'applicazione utilizza l'analisi euristica con il livello di dettaglio **Media**. • **Basso**. Kaspersky Endpoint Security esegue la scansione solo dei formati file specificati. Durante la scansione dei file compositi, l'applicazione esegue la scansione di archivi, pacchetti di distribuzione, file dei formati Office, ma non degli archivi protetti da password. Quando è impostato questo livello di protezione, l'applicazione utilizza l'analisi euristica con il livello di dettaglio **Superficiale**.
Azione se viene rilevata una minaccia	**Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato. **Disinfetta (se la disinfezione non riesce, informa)**. Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive. **Informa**. Se questa opzione è selezionata, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti all'elenco delle minacce attive in caso di rilevamento di tali file.
Tipi di file	Kaspersky Endpoint Security considera i file privi di estensione come eseguibili. I file eseguibili vengono sempre esaminati, indipendentemente dai tipi di file selezionati per la scansione. **Tutti i file**. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina tutti i file senza eccezioni (tutti i formati e le estensioni). **File esaminati per formato**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Prima di esaminare un file alla ricerca di codice dannoso, viene analizzata l'intestazione interna del file per determinarne il formato (ad esempio, .txt, .doc o .exe). La scansione cerca inoltre i file con estensioni file particolari. **File esaminati per estensione**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Il formato del file viene quindi determinato in base all'estensione. Per impostazione predefinita, Kaspersky Endpoint Security esegue la scansione dei file in base al loro formato. La scansione dei file per estensione è meno sicura perché un file dannoso può avere un'estensione che non è nell'elenco dei file potenzialmente infettabili (ad esempio, `.123`).
Esamina solo i file nuovi e modificati	Esamina solo i nuovi file e i file che sono stati modificati dopo l'ultima scansione. Questo consente di ridurre la durata di una scansione. Questa modalità si applica sia ai file semplici che compositi.
Ignora i file esaminati per più di N secondi	Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione.
Esamina gli archivi	Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio).
Esamina i pacchetti di distribuzione	Questa casella di controllo consente di abilitare o disabilitare la scansione dei pacchetti di distribuzione.

Parametro	Descrizione
Esamina i file nei formati Microsoft Office	Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE. L'applicazione analizza i file in formato Office di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Esamina i file in formato e-mail	Scansione dei file in formato e-mail e del database delle e-mail. L'applicazione esamina i file PST e OST utilizzati dai client di posta MS Outlook e Windows Mail, nonché i file EML. Kaspersky Endpoint Security non supporta la versione a 64 bit del client di posta Microsoft Outlook. Di conseguenza, Kaspersky Endpoint Security non esegue la scansione dei file Microsoft Outlook (file PST e OST) se nel computer è installata una versione a 64 bit di Microsoft Outlook, anche se la posta è inclusa nell'ambito della scansione. Se la casella di controllo è selezionata, Kaspersky Endpoint Security suddivide il file in formato e-mail nei relativi componenti (intestazione, corpo e allegati) e li analizza alla ricerca di potenziali minacce. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security analizza il file in formato e-mail come un singolo file. Quando un oggetto dannoso viene individuato nei file PST o OST, Kaspersky Endpoint Security lo rende innocuo in base all'azione selezionata (ad esempio, la disinfezione o l'eliminazione del file). Se vengono rilevati oggetti dannosi nei file di altri client e-mail, ad esempio Mozilla Thunderbird, Kaspersky Endpoint Security non disinfetta né elimina tali file per evitare l'eliminazione indesiderata dei messaggi e-mail. Kaspersky Endpoint Security aggiunge solo le informazioni sugli oggetti rilevati all'elenco delle minacce attive. È necessario eliminare le e-mail contenenti file dannosi negli allegati tramite l'interfaccia utente del client di posta. Se per qualsiasi motivo non è possibile eliminare i messaggi contenenti oggetti dannosi, è possibile gestire tali minacce nell'interfaccia utente di Kaspersky Endpoint Security aggiungendo gli oggetti rilevati all'elenco delle esclusioni dalla scansione.
Esamina gli archivi protetti da password	Se la casella di controllo è selezionata, l'applicazione esamina gli archivi protetti tramite password. Prima di eseguire la scansione dei file in un archivio, viene richiesto di immettere la password. Se la casella di controllo è deselezionata, l'applicazione ignora la scansione degli archivi protetti tramite password.
Non decomprimere i file compositi di grandi dimensioni	Se la casella di controllo è selezionata, l'applicazione non esegue la scansione dei file compositi se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, l'applicazione esamina i file compositi di qualsiasi dimensione. L'applicazione esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Machine Learning e analisi delle firme	Il metodo Machine Learning e analisi delle firme utilizza i database di Kaspersky Endpoint Security, che contengono le descrizioni delle minacce conosciute, nonché i metodi per neutralizzarle. La protezione che utilizza questo metodo fornisce il livello di sicurezza minimo accettabile. In base ai suggerimenti degli esperti Kaspersky, il metodo Machine Learning e analisi delle firme è sempre abilitato.
Analisi euristica	Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto. Durante la scansione dei file alla ricerca di codice dannoso, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.
Tecnologia iSwift	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.
Tecnologia iChecker	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

Controllo dell'integrità dell'applicazione

Kaspersky Endpoint Security verifica se i moduli dell'applicazione risultano danneggiati o modificati. Se ad esempio una libreria dell'applicazione presenta una firma digitale errata, la libreria viene considerata danneggiata. L'attività *Controllo integrità applicazione* consente di controllare i file delle applicazioni. Eseguire l'attività *Controllo integrità applicazione* se Kaspersky Endpoint Security ha rilevato un oggetto dannoso ma non lo ha neutralizzato.

È possibile creare l'attività *Controllo integrità applicazione* sia in Kaspersky Security Center Web Console che in Administration Console. Non è possibile creare un'attività in Kaspersky Security Center Cloud Console.

Possono verificarsi violazioni dell'integrità di un'applicazione nei seguenti casi:

- Un oggetto dannoso ha modificato i file di Kaspersky Endpoint Security. In tal caso, eseguire la procedura per il ripristino di Kaspersky Endpoint Security utilizzando gli strumenti del sistema operativo. Dopo il ripristino, eseguire una scansione completa del computer e ripetere il controllo integrità.
- La firma digitale è scaduta. In questo caso, aggiornare Kaspersky Endpoint Security.

Come eseguire un controllo integrità dell'applicazione tramite Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Controllo integrità applicazione**.

Passaggio 2. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 3. Configurazione di una pianificazione di avvio dell'attività

Configurare una pianificazione per l'avvio di un'attività, ad esempio manualmente o quando viene rilevata un'epidemia di virus.

Passaggio 4. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Controllo integrità dopo l'infezione del computer*.

Passaggio 5. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività. Successivamente Kaspersky Endpoint Security verificherà l'integrità dell'applicazione. È inoltre possibile configurare la pianificazione di un controllo integrità dell'applicazione nelle proprietà dell'attività (vedere la tabella riportata di seguito).

Come eseguire un controllo integrità dell'applicazione tramite Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Controllo integrità applicazione**.

   c. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Controllare l'integrità dell'applicazione dopo un'infezione del computer*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Selezione dell'account per eseguire l'attività. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.

6. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Selezionare la casella di controllo accanto all'attività.

Successivamente Kaspersky Endpoint Security verificherà l'integrità dell'applicazione. È inoltre possibile configurare la pianificazione di un controllo integrità dell'applicazione nelle proprietà dell'attività (vedere la tabella riportata di seguito).

Come eseguire un controllo di integrità nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.
2. Si apre l'elenco delle attività; selezionare l'attività *Controllo integrità applicazione* e fare clic su **Esegui**.

Successivamente Kaspersky Endpoint Security verificherà l'integrità dell'applicazione. È inoltre possibile configurare la pianificazione di un controllo integrità dell'applicazione nelle proprietà dell'attività (vedere la tabella riportata di seguito). Se l'attività *Controllo integrità applicazione* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

Impostazioni dell'attività Controllo integrità

Parametro	Descrizione
Pianificazione scansione	**Manualmente**. Modalità di esecuzione in cui è possibile avviare la scansione manualmente nel momento più opportuno. **In base alla pianificazione**. In questa modalità di esecuzione dell'attività di scansione, l'applicazione avvia l'attività di scansione in base alla pianificazione creata dall'utente. Se si seleziona questa modalità di esecuzione dell'attività di scansione, è anche possibile avviare l'attività di scansione manualmente.
Esegui attività ignorate	Se la casella di controllo è selezionata, Kaspersky Endpoint Security avvia l'attività ignorata appena possibile. L'attività può ad esempio essere ignorata se il computer è spento all'orario impostato per l'avvio dell'attività pianificata. Quando l'applicazione ha l'opportunità di eseguire le attività non effettuate, esegue le attività in modo casuale entro un determinato intervallo di tempo per distribuire il carico sul computer. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non esegue le attività ignorate. Viene invece eseguita l'attività successiva, in base alla pianificazione corrente.
Esegui solo quando il computer è inattivo	Avvio posticipato dell'attività quando le risorse del computer sono occupate. Kaspersky Endpoint Security avvia l'attività di scansione se il computer è bloccato o se lo screensaver è attivo. Se l'esecuzione dell'attività è stata interrotta, ad esempio sbloccando il computer, Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui era stata interrotta. Questa opzione di pianificazione consente di conservare le risorse del computer durante l'utilizzo del computer.

Modifica dell'ambito della scansione

L'*ambito della scansione* è un elenco di percorsi a cartelle e percorsi in cui Kaspersky Endpoint Security esegue la scansione durante l'esecuzione dell'attività. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

Per modificare l'ambito della scansione, si consiglia di utilizzare l'attività *Scansione personalizzata*. Gli esperti di Kaspersky consigliano di non modificare l'ambito della scansione delle attività *Scansione completa* e *Scansione delle aree critiche*.

Kaspersky Endpoint Security include i seguenti oggetti predefiniti come parte dell'ambito della scansione:

- **Memoria di sistema**.
- **Processi in esecuzione e oggetti di avvio**.

  Memoria occupata da processi e file eseguibili dell'applicazione eseguiti all'avvio del sistema.
- **Settori di avvio del disco**.

  Settori di avvio del disco rigido e del disco rimovibile.

- **Backup di sistema**.

  Contenuto della cartella System Volume Information.

- **Tutti i dispositivi esterni**.

- **Tutti i dischi rigidi**.

- **Tutte le unità di rete**.

> In Kaspersky Endpoint Security for Windows 12.12, l'e-mail è esclusa dall'ambito della scansione dell'applicazione. La scansione dei messaggi e-mail in entrata e in uscita viene eseguita dal componente Protezione minacce di posta. Se si utilizza una versione precedente del plug-in di gestione, l'applicazione esclude la posta elettronica dall'ambito di scansione, anche se il criterio la include.

> Si consiglia di creare un'attività di scansione separata per la scansione delle unità di rete o delle cartelle condivise. Nelle impostazioni dell'attività *Scansione malware*, specificare un utente che ha accesso in scrittura a questa unità; ciò è necessario per attenuare le minacce rilevate. Se il server in cui si trova l'unità di rete dispone dei propri strumenti di sicurezza, non eseguire l'attività di scansione per tale unità. In questo modo, è possibile evitare di controllare due volte l'oggetto e migliorare le prestazioni del server.

Per escludere cartelle o file dall'ambito della scansione, aggiungere la cartella o il file all'area attendibile.

Come modificare un'ambito della scansione in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Attività**.
3. Selezionare l'attività di scansione e fare doppio clic per aprire le proprietà dell'attività.

   Se necessario, creare l'attività *Scansione malware*.
4. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.
5. Nella sezione **Ambito della scansione**, fare clic su **Impostazioni**.
6. Nella finestra visualizzata, selezionare gli oggetti che si desidera aggiungere o escludere dall'ambito della scansione.
7. Per aggiungere un nuovo oggetto all'ambito della scansione:

   a. Fare clic su **Aggiungi**.

   b. Nel campo **Oggetto**, immettere il percorso del file o della cartella.

Utilizzare le maschere:

- Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

- Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

- Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

È possibile usare le maschere ovunque in un percorso di file o cartella. Ad esempio, se si desidera che l'ambito della scansione includa la cartella Downloads per tutti gli account utente sul computer, immettere la maschera `C:\Users\*\Downloads\`.

L'oggetto **Questo PC** nell'elenco delle risorse file del computer include i seguenti oggetti: **Tutti i dischi rigidi**, **Tutte le unità di rete** e **Tutte le unità rimovibili**.

È possibile escludere un oggetto dalle scansioni senza eliminarlo dall'elenco degli oggetti nell'ambito della scansione. A tale scopo, deselezionare la casella di controllo accanto all'oggetto.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come modificare un'ambito della scansione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività di scansione.

   Verrà visualizzata la finestra delle proprietà dell'attività. Se necessario, creare l'attività *Scansione malware*.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Nella sezione **Ambito della scansione**, selezionare gli oggetti che si desidera aggiungere o escludere dall'ambito della scansione.

5. Per aggiungere un nuovo oggetto all'ambito della scansione:

   a. Fare clic su **Aggiungi**.

   b. Immettere il percorso della cartella o del file.

Utilizzare le maschere:

- Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

- Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

- Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

È possibile usare le maschere ovunque in un percorso di file o cartella. Ad esempio, se si desidera che l'ambito della scansione includa la cartella Downloads per tutti gli account utente sul computer, immettere la maschera `C:\Users\*\Downloads\`.

È possibile escludere un oggetto dalle scansioni senza eliminarlo dall'elenco degli oggetti nell'ambito della scansione. A tale scopo, impostare l'interruttore accanto ad esso in posizione disattivato.

6. Salvare le modifiche.

Come modificare un ambito della scansione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.

2. Si apre l'elenco delle attività; selezionare l'attività *Scansione personalizzata* e fare clic su **Seleziona**.

   È inoltre possibile modificare l'ambito di scansione per altre attività. Gli esperti di Kaspersky consigliano di non modificare l'ambito della scansione delle attività *Scansione completa* e *Scansione delle aree critiche*.

3. Nella finestra visualizzata, selezionare gli oggetti che si desidera aggiungere all'ambito della scansione.

4. Salvare le modifiche.

Se l'attività di scansione non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

Esecuzione di una scansione pianificata

La scansione del malware tramite l'attività *Scansione malware* può richiedere molto tempo e aumentare l'utilizzo delle risorse del computer da parte di Kaspersky Endpoint Security. È pertanto consigliabile selezionare un momento ottimale per l'esecuzione dell'attività in modo da ridurre al minimo l'impatto sulle prestazioni delle altre applicazioni.

Ad esempio, se i dipendenti dell'organizzazione lavorano con una pianificazione fissa, è possibile configurare una scansione del computer da eseguire di notte o nei fine settimana. Se per qualsiasi motivo non è possibile eseguire l'attività, ad esempio perché all'ora prevista il computer è spento, è possibile configurare l'attività non eseguita in modo che venga avviata automaticamente appena possibile. Questa funzione deve essere utilizzata con cautela, poiché potrebbe rallentare le applicazioni nel computer dell'utente quando il computer viene acceso al mattino.

Se non è possibile determinare la pianificazione della scansione ottimale adatta alle proprie esigenze, è possibile configurare la scansione da eseguire quando viene soddisfatta una delle seguenti condizioni speciali:

- Dopo l'aggiornamento di un database.

  Kaspersky Endpoint Security esegue la scansione del computer con il database di firme aggiornato.

- Dopo l'avvio dell'applicazione.

  Kaspersky Endpoint Security esegue una scansione del computer quando trascorre un periodo di tempo specificato in seguito all'avvio dell'applicazione. All'avvio del sistema operativo, molti processi sono in esecuzione, pertanto è preferibile rimandare l'attività di scansione anziché eseguirla immediatamente dopo l'avvio di Kaspersky Endpoint Security.

- Funzionalità Wake-on-LAN.

  Kaspersky Endpoint Security esegue una scansione del computer pianificata anche se il computer è spento. A tale scopo, l'applicazione utilizza la funzionalità Wake-on-LAN del sistema operativo. La funzionalità Wake-on-LAN consente di accendere il computer da remoto inviando un segnale speciale sulla rete locale. Per utilizzare questa funzionalità, è necessario abilitare Wake-on-LAN nelle impostazioni BIOS.

  È possibile configurare l'esecuzione della scansione con Wake-on-LAN solo per l'attività *Scansione malware* in Kaspersky Security Center. Non è possibile abilitare Wake-on-LAN per la scansione del computer nell'interfaccia dell'applicazione.

- Quando il computer è inattivo.

  Kaspersky Endpoint Security esegue una scansione del computer pianificata quando lo screensaver è attivo o lo schermo è bloccato. Se l'utente sblocca il computer, Kaspersky Endpoint Security sospende la scansione. In questo caso, il completamento della Scansione completa potrebbe richiedere diversi giorni.

- Quando l'attività è stata ignorata.

  Kaspersky Endpoint Security esegue l'attività ignorata non appena possibile. L'attività può ad esempio essere ignorata se il computer è spento all'orario impostato per l'avvio dell'attività pianificata. Quando l'applicazione ha l'opportunità di eseguire le attività non effettuate, esegue le attività in modo casuale entro un determinato intervallo di tempo per distribuire il carico sul computer.

Come configurare la pianificazione della scansione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività di scansione.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

4. Configurare la pianificazione dell'attività di scansione.

5. A seconda della frequenza selezionata, configurare le impostazioni avanzate che specificano la pianificazione di esecuzione dell'attività (vedere la tabella riportata di seguito).

6. Salvare le modifiche.

Come configurare la pianificazione della scansione nell'interfaccia dell'applicazione

È possibile configurare la pianificazione della scansione solo se al computer non è applicato un criterio. Per i computer a cui è applicato un criterio, è possibile configurare l'attività *Scansione malware* in Kaspersky Security Center.

1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.
2. Nell'elenco delle attività, selezionare l'attività di scansione e fare clic su ⚙.

   È possibile configurare una pianificazione per l'esecuzione di una Scansione completa, una Scansione delle aree critiche o un Controllo integrità. Una Scansione personalizzata può essere eseguita solo manualmente.
3. Fare clic su **Pianificazione scansione**.
4. Nella finestra visualizzata, configurare la pianificazione dell'esecuzione dell'attività di scansione.
5. A seconda della frequenza selezionata, configurare le impostazioni avanzate che specificano la pianificazione di esecuzione dell'attività (vedere la tabella riportata di seguito).
6. Salvare le modifiche.

Impostazioni di pianificazione della scansione

Parametro	Descrizione
Pianificazione scansione	**Manualmente**. Modalità di esecuzione in cui è possibile avviare la scansione manualmente nel momento più opportuno. **In base alla pianificazione**. In questa modalità di esecuzione dell'attività di scansione, l'applicazione avvia l'attività di scansione in base alla pianificazione creata dall'utente. Se si seleziona questa modalità di esecuzione dell'attività di scansione, è anche possibile avviare l'attività di scansione manualmente.
Rimanda l'esecuzione dopo l'avvio dell'applicazione di N minuti	Avvio rimandato dell'attività di scansione dopo l'avvio dell'applicazione. All'avvio del sistema operativo, molti processi sono in esecuzione, pertanto è preferibile rimandare l'attività di scansione anziché eseguirla immediatamente dopo l'avvio di Kaspersky Endpoint Security.
Esegui attività ignorate	Se la casella di controllo è selezionata, Kaspersky Endpoint Security avvia l'attività ignorata appena possibile. L'attività può ad esempio essere ignorata se il computer è spento all'orario impostato per l'avvio dell'attività pianificata. Quando l'applicazione ha l'opportunità di eseguire le attività non effettuate, esegue le attività in modo casuale entro un determinato intervallo di tempo per distribuire il carico sul computer. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non esegue le attività ignorate. Viene invece eseguita l'attività successiva, in base alla pianificazione corrente.
Esegui solo quando il computer è inattivo	Avvio posticipato dell'attività quando le risorse del computer sono occupate. Kaspersky Endpoint Security avvia l'attività di scansione se il computer è bloccato o se lo screensaver è attivo. Se l'esecuzione dell'attività è stata interrotta, ad esempio sbloccando il computer, Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui era stata interrotta. Questa opzione di pianificazione consente di conservare le risorse del computer durante l'utilizzo del computer.
Usa &automaticamente il ritardo casuale per l'avvio delle attività *(disponibile solo in Kaspersky Security Center Console)*	Se questa casella di controllo è selezionata, l'attività non viene eseguita tassativamente quando pianificata, ma casualmente in un certo intervallo, ovvero gli orari di inizio dell'attività vengono estesi. Gli orari di inizio casuali consentono di evitare che un gran numero di computer accedano contemporaneamente ad Administration Server quando l'attività viene eseguita in base alle tempistiche pianificate. L'intervallo di ora di inizio casuali viene calcolato automaticamente al momento della creazione dell'attività, in base al numero di computer a cui è stata assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, se le impostazioni dell'attività vengono modificate oppure l'attività viene eseguita manualmente, l'ora di inizio calcolata cambia. Se la casella di controllo è deselezionata, l'attività viene eseguita esattamente all'ora pianificata.
Usa ritar&do casuale per l'avvio delle attività con un intervallo di (min.)	Se questa casella di controllo è selezionata, l'attività viene eseguita nei computer a un'ora casuale entro un determinato intervallo di tempo. Gli orari di inizio casuali consentono di evitare che un gran numero di computer accedano contemporaneamente ad Administration Server quando l'attività viene eseguita in base alle tempistiche pianificate. Se la casella di controllo è deselezionata, l'attività viene eseguita esattamente all'ora pianificata.

Parametro	Descrizione
&Arresta se l'attività viene eseguita per più di (min) *(disponibile solo in Kaspersky Security Center Console)*	Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione. Per ridurre il tempo di esecuzione dell'attività, è possibile, ad esempio, configurare l'ambito della scansione oppure ottimizzare la scansione.
Accendi i dispositivi utilizzando la funzione &Wake-on-LAN prima di avviare l'attività (min) *(disponibile solo in Kaspersky Security Center Console)*	Se la casella di controllo è selezionata, al sistema operativo del computer viene assegnato un tempo di esecuzione specificato per completare l'avvio prima che l'attività venga eseguita. Il tempo di esecuzione predefinito è 5 minuti. Selezionare la casella di controllo se si desidera eseguire l'attività su tutti i computer, inclusi quelli spenti.
&Spegni i dispositivi dopo il completamento dell'attività *(disponibile solo in Kaspersky Security Center Console)*	Se questa casella di controllo è selezionata, il computer verrà arrestato al termine dell'attività. È ad esempio possibile abilitare questa funzionalità per eseguire la scansione del computer il venerdì dopo l'orario di lavoro. Al termine dell'attività, l'applicazione spegne il computer per il fine settimana.
Sospendi l'attività	È possibile specificare un intervallo di tempo durante il quale verrà sospesa l'esecuzione di un'attività pianificata in precedenza. Al termine del periodo di tempo specificato, l'attività riprenderà. Ciò potrebbe essere necessario, ad esempio, per ridurre al minimo l'impatto di Kaspersky Endpoint Security sulle prestazioni del computer durante i periodi di picco di utilizzo.
Disabilita pianificazione da	Se la casella di controllo è selezionata, Kaspersky Endpoint Security interromperà l'esecuzione dell'attività pianificata a partire dalla data specificata. L'attività verrà impostata sulla modalità **Manualmente**.

Esecuzione di una scansione come utente diverso

Per impostazione predefinita, l'attività di scansione viene eseguita per conto dell'utente i cui diritti sono registrati nel sistema operativo. L'ambito della protezione può includere unità di rete o altri oggetti che richiedono diritti di accesso speciali. È possibile specificare un utente che dispone dei diritti appropriati nelle impostazioni dell'applicazione ed eseguire l'attività di scansione tramite l'account di questo utente.

È possibile eseguire le seguenti scansioni come utente diverso:

- Scansione delle aree critiche.
- Scansione completa.
- Scansione personalizzata.
- Scansione dal menu di scelta rapida.

Non è possibile configurare i diritti utente per l'esecuzione di una Scansione unità rimovibili, una Scansione in background o un Controllo integrità.

Come eseguire una scansione come utente diverso in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, aprire la cartella con il nome del gruppo di amministrazione a cui appartengono i computer client desiderati.
3. Nell'area di lavoro, selezionare la scheda **Attività**.
4. Selezionare l'attività di scansione e fare doppio clic per aprire le proprietà dell'attività.
5. Nella finestra delle proprietà dell'attività, selezionare la sezione **Account**.

6. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire un'attività di scansione.

7. Salvare le modifiche.

Come eseguire una scansione come utente diverso in Web Console o Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività di scansione.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Selezionare la scheda **Impostazioni**.

4. Nel blocco **Account**, fare clic sul pulsante **Impostazioni**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire un'attività di scansione.

6. Salvare le modifiche.

Come eseguire una scansione come utente diverso nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.

2. Nell'elenco delle attività, selezionare l'attività di scansione e fare clic su ⚙.

3. Nelle proprietà dell'attività, selezionare **Impostazioni avanzate** → **Esegui scansione come**.

4. Nella finestra visualizzata, immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire un'attività di scansione.

5. Salvare le modifiche.

Se l'attività di scansione non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

Ottimizzazione della scansione

Limitazione dell'utilizzo della CPU durante la scansione del computer

È possibile limitare l'utilizzo della CPU durante l'esecuzione dell'attività *Scansione malware*. Questo potrebbe aumentare il tempo necessario per eseguire la scansione del computer.

Come limitare l'utilizzo della CPU durante la scansione del computer in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni applicazione**.

4. In **Prestazioni**, selezionare la casella di controllo **Limita l'utilizzo della CPU per le attività di scansione** e immettere il valore medio del consumo di risorse CPU in percentuale.

5. Salvare le modifiche.

Come limitare l'utilizzo della CPU durante la scansione del computer in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Prestazioni**.

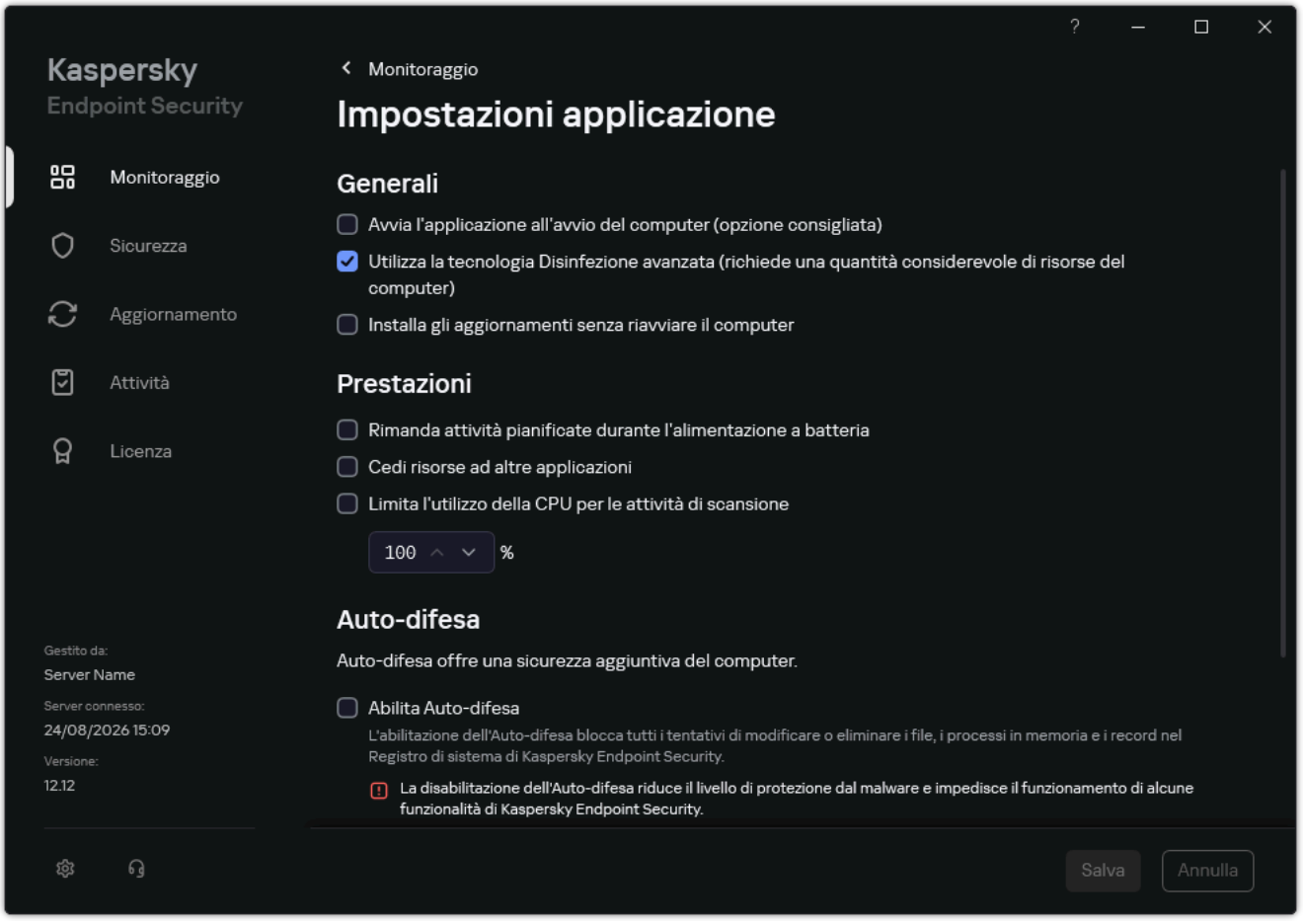
5. In **Limita l'utilizzo della CPU per le attività di scansione**, impostare l'interruttore su **Limita l'utilizzo della CPU per le attività di scansione e immettere il valore medio del** consumo di risorse CPU in percentuale.

6. Salvare le modifiche.

Come limitare l'utilizzo della CPU durante la scansione del computer nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.



3. In **Prestazioni**, selezionare la casella di controllo **Limita l'utilizzo della CPU per le attività di scansione** e immettere il valore medio del consumo di risorse CPU in percentuale.

4. Salvare le modifiche.

Configurazione delle impostazioni avanzate delle attività per Scansione malware.

È possibile ottimizzare la scansione dei file riducendo il tempo di scansione e aumentando la velocità di esecuzione di Kaspersky Endpoint Security. Per ottenere questo risultato, è possibile eseguire la scansione solo dei file nuovi e modificati dopo l'ultima scansione. Questa modalità si applica sia ai file semplici che compositi. È anche possibile impostare un limite per la scansione di un singolo file. Al termine dell'intervallo di tempo specificato, il file viene escluso dalla scansione corrente (ad eccezione degli archivi e degli oggetti che contengono più file).

Una tecnica comune per nascondere virus e altro malware è inserirli in file compositi, come ad esempio archivi o database. Per rilevare i virus e il malware nascosti in questo modo, è necessario decomprimere il file composito, cosa che può rallentare la scansione. È possibile limitare i tipi di file compositi da esaminare, velocizzando la scansione.

È inoltre possibile abilitare le tecnologie iChecker e iSwift. Le tecnologie iChecker e iSwift ottimizzano la velocità di scansione dei file escludendo i file che non sono stati modificati dall'ultima scansione.

Come ottimizzare la scansione in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella struttura della console, selezionare **Attività**.

3. Selezionare l'attività di scansione e fare doppio clic per aprire le proprietà dell'attività.

   Se necessario, creare l'attività *Scansione malware*.

4. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.

5. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.

   Si apre la finestra delle impostazioni dell'attività di scansione.

6. Nel blocco **Ottimizzazione**, configurare le impostazioni di scansione:

   - **Esamina solo i file nuovi e modificati**. Esamina solo i nuovi file e i file che sono stati modificati dopo l'ultima scansione. Questo consente di ridurre la durata di una scansione. Questa modalità si applica sia ai file semplici che compositi.

     È inoltre possibile configurare la scansione di nuovi file in base al tipo. Ad esempio, è possibile eseguire la scansione di tutti i pacchetti di distribuzione ed eseguire la scansione solo dei nuovi archivi e dei file in formato Office.

- **Ignora i file esaminati per più di N sec**. Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione.

- **Non eseguire più attività di scansione contemporaneamente**. Ritardare le attività di scansione pianificata se una scansione pianificata avviata in precedenza è ancora in esecuzione. Kaspersky Endpoint Security metterà in coda le attività di scansione pianificata se la scansione corrente è ancora in esecuzione. In questo modo, è possibile ottimizzare il carico sul computer. Ad esempio, sono state pianificate attività di scansione da eseguire alle 18:00 e alle 20:00. Kaspersky Endpoint Security rinvierà l'attività di scansione delle 20:00 se l'attività di scansione pianificata per le 18:00 è ancora in esecuzione. L'applicazione eseguirà una scansione al termine dell'attività avviata alle 18:00.

7. Fare clic su **Avanzate**.

   Si apre la finestra delle impostazioni di scansione dei file compositi.

8. Nella sezione **Dimensione massima** selezionare la casella di controllo **Non decomprimere i file compositi di grandi dimensioni**. Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione.

   Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi, indipendentemente dal fatto che la casella di controllo **Non decomprimere i file compositi di grandi dimensioni** sia selezionata o meno.

9. Fare clic su **OK**.

10. Passare alla scheda **Avanzate**.

11. Nella sezione **Tecnologie di scansione** selezionare le caselle di controllo accanto ai nomi delle tecnologie da utilizzare durante una scansione:

    - **Tecnologia iSwift**. Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.

    - **Tecnologia iChecker**. Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

12. Salvare le modifiche.

Come ottimizzare la scansione in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività di scansione.

   Verrà visualizzata la finestra delle proprietà dell'attività. Se necessario, creare l'attività *Scansione malware*.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Nella sezione **Azione se viene rilevata una minaccia** selezionare la casella di controllo **Esamina solo i file nuovi e modificati**. Esamina solo i nuovi file e i file che sono stati modificati dopo l'ultima scansione. Questo consente di ridurre la durata di una scansione. Questa modalità si applica sia ai file semplici che compositi.

   È inoltre possibile configurare la scansione di nuovi file in base al tipo. Ad esempio, è possibile eseguire la scansione di tutti i pacchetti di distribuzione ed eseguire la scansione solo dei nuovi archivi e dei file in formato Office.

5. Nella sezione **Ottimizzazione della scansione** selezionare la casella di controllo **Non decomprimere i file compositi di grandi dimensioni**. Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione.

   > Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi, indipendentemente dal fatto che la casella di controllo **Non decomprimere i file compositi di grandi dimensioni** sia selezionata o meno.

6. Selezionare la casella di controllo **Non eseguire più attività di scansione contemporaneamente**. Ritardare le attività di scansione pianificata se una scansione pianificata avviata in precedenza è ancora in esecuzione. Kaspersky Endpoint Security metterà in coda le attività di scansione pianificata se la scansione corrente è ancora in esecuzione. In questo modo, è possibile ottimizzare il carico sul computer. Ad esempio, sono state pianificate attività di scansione da eseguire alle 18:00 e alle 20:00. Kaspersky Endpoint Security rinvierà l'attività di scansione delle 20:00 se l'attività di scansione pianificata per le 18:00 è ancora in esecuzione. L'applicazione eseguirà una scansione al termine dell'attività avviata alle 18:00.

7. Nella sezione **Impostazioni avanzate** selezionare la casella di controllo **Ignora file scansionato per più di (sec)**. Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione.

8. Salvare le modifiche.

Come ottimizzare la scansione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.

2. Nell'elenco delle attività, selezionare l'attività di scansione e fare clic su ⚙.

3. Fare clic su **Impostazioni avanzate**.

4. Nel blocco **Ottimizzazione**, configurare le impostazioni di scansione:

   - **Esamina solo i file nuovi e modificati**. Esamina solo i nuovi file e i file che sono stati modificati dopo l'ultima scansione. Questo consente di ridurre la durata di una scansione. Questa modalità si applica sia ai file semplici che compositi.

     È inoltre possibile configurare la scansione di nuovi file in base al tipo. Ad esempio, è possibile eseguire la scansione di tutti i pacchetti di distribuzione ed eseguire la scansione solo dei nuovi archivi e dei file in formato Office.

- **Ignora i file esaminati per più di N secondi**. Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione.

- **Non eseguire più attività di scansione contemporaneamente**. Ritardare le attività di scansione pianificata se una scansione pianificata avviata in precedenza è ancora in esecuzione. Kaspersky Endpoint Security metterà in coda le attività di scansione pianificata se la scansione corrente è ancora in esecuzione. In questo modo, è possibile ottimizzare il carico sul computer. Ad esempio, sono state pianificate attività di scansione da eseguire alle 18:00 e alle 20:00. Kaspersky Endpoint Security rinvierà l'attività di scansione delle 20:00 se l'attività di scansione pianificata per le 18:00 è ancora in esecuzione. L'applicazione eseguirà una scansione al termine dell'attività avviata alle 18:00.

5. Nella sezione **Dimensione massima** selezionare la casella di controllo **Non decomprimere i file compositi di grandi dimensioni**. Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione.

   Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi, indipendentemente dal fatto che la casella di controllo **Non decomprimere i file compositi di grandi dimensioni** sia selezionata o meno.

6. Nella sezione **Tecnologie di scansione** selezionare le caselle di controllo accanto ai nomi delle tecnologie da utilizzare durante una scansione:

   - **Tecnologia iSwift**. Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.

   - **Tecnologia iChecker**. Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).

7. Salvare le modifiche.

Se l'attività di scansione non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

Aggiornamento di database e moduli software dell'applicazione

L'aggiornamento dei database e dei moduli dell'applicazione di Kaspersky Endpoint Security assicura il massimo livello di protezione del computer. In tutto il mondo appaiono quotidianamente nuovi virus e altri tipi di malware. I database di Kaspersky Endpoint Security contengono informazioni sulle minacce e sui metodi per eliminarle. Per rilevare rapidamente le minacce, è importante eseguire periodicamente l'aggiornamento dei database e dei moduli dell'applicazione.

La funzionalità Aggiornamenti (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) potrebbe non essere disponibile nell'applicazione negli Stati Uniti.

Gli aggiornamenti periodici richiedono una licenza valida. Se non è disponibile alcuna licenza, è possibile eseguire un aggiornamento una sola volta.

Il computer deve essere connesso a Internet per consentire il download del pacchetto di aggiornamento dai server degli aggiornamenti Kaspersky. Per impostazione predefinita, le impostazioni di connessione a Internet vengono determinate automaticamente. Se si utilizza un server proxy, è necessario configurare le impostazioni del server proxy.

Gli aggiornamenti vengono scaricati tramite il protocollo HTTPS. Possono inoltre essere scaricati tramite il protocollo HTTP quando non è possibile scaricare gli aggiornamenti tramite il protocollo HTTPS.

Durante l'esecuzione di un aggiornamento, vengono scaricati e installati nel computer i seguenti oggetti:

- Database di Kaspersky Endpoint Security. La protezione del computer viene garantita dai database che contengono le firme di virus e altre minacce e informazioni sulle modalità per neutralizzarli. I componenti della protezione utilizzano queste informazioni per cercare e neutralizzare i file infetti nel computer. I database vengono costantemente aggiornati con i record relativi alle nuove minacce e i metodi per contrastarle. È pertanto consigliabile aggiornare periodicamente i database.

  Oltre ai database di Kaspersky Endpoint Security, vengono aggiornati i driver di rete che consentono ai componenti dell'applicazione di intercettare il traffico di rete.

- Moduli dell'applicazione. Oltre ai database di Kaspersky Endpoint Security, è possibile aggiornare i moduli dell'applicazione. L'aggiornamento dei moduli dell'applicazione consente di correggere le vulnerabilità di Kaspersky Endpoint Security, aggiungere nuove funzioni o migliorare quelle esistenti.

Durante un aggiornamento, i moduli dell'applicazione e i database nel computer vengono confrontati con la versione aggiornata disponibile nella sorgente degli aggiornamenti. Se i database e i moduli dell'applicazione correnti sono differenti dalle rispettive versioni più recenti, la parte mancante di aggiornamenti viene installata nel computer.

Se i database sono obsoleti, il pacchetto di aggiornamento può essere di grandi dimensioni, causando traffico internet aggiuntivo (fino a decine di MB).

Le informazioni sullo stato corrente dei database di Kaspersky Endpoint Security vengono visualizzate nella finestra principale dell'applicazione o nella descrizione comandi visualizzata quando si passa il cursore sull'icona dell'applicazione nell'area di notifica.

Le informazioni sui risultati dell'aggiornamento e su tutti gli eventi che si verificano durante l'esecuzione dell'attività vengono registrate in un rapporto di Kaspersky Endpoint Security.

Se l'applicazione funziona in modalità Light Agent, considerazioni speciali sono coinvolte nell'aggiornamento dei database e dei moduli dell'applicazione.

Scenari di aggiornamento dei database e dei moduli dell'applicazione

L'aggiornamento dei database e dei moduli dell'applicazione di Kaspersky Endpoint Security assicura il massimo livello di protezione del computer. In tutto il mondo appaiono quotidianamente nuovi virus e altri tipi di malware. I database di Kaspersky Endpoint Security contengono informazioni sulle minacce e sui metodi per eliminarle. Per rilevare rapidamente le minacce, è importante eseguire periodicamente l'aggiornamento dei database e dei moduli dell'applicazione.

I seguenti oggetti vengono aggiornati nei computer degli utenti:

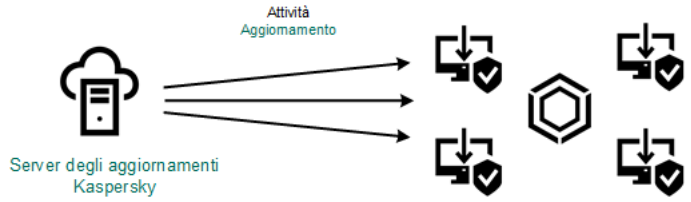
- Database anti-virus. I database anti-virus includono i database delle firme malware, una descrizione degli attacchi di rete, i database degli indirizzi Web di phishing e dannosi, i database dei banner, i database spam e altri dati.

- Moduli dell'applicazione. Gli aggiornamenti dei moduli sono destinati all'eliminazione delle vulnerabilità nell'applicazione e all'ottimizzazione dei metodi di protezione del computer. Gli aggiornamenti dei moduli possono modificare il comportamento dei componenti dell'applicazione e aggiungere nuove funzionalità.

Kaspersky Endpoint Security supporta i seguenti scenari per l'aggiornamento dei database e dei moduli dell'applicazione:

- Eseguire l'aggiornamento dai server Kaspersky.

  I server degli aggiornamenti Kaspersky si trovano in diversi paesi del mondo. In questo modo viene garantita l'elevata affidabilità degli aggiornamenti. Se un aggiornamento non può essere eseguito da un determinato server, Kaspersky Endpoint Security passa al server successivo.



Aggiornamento dai server Kaspersky

- Aggiornamento centralizzato.

  L'aggiornamento centralizzato riduce il traffico Internet esterno e consente un pratico monitoraggio dell'aggiornamento.

L'aggiornamento centralizzato comprende i seguenti passaggi:

1. Scaricare il pacchetto di aggiornamenti in un archivio all'interno della rete dell'organizzazione.

   Il pacchetto di aggiornamenti viene scaricato nell'archivio dall'attività di Administration Server denominata *Scarica aggiornamenti nell'archivio dell'Administration Server*.

2. Scaricare il pacchetto di aggiornamenti in una cartella condivisa (opzione facoltativa).

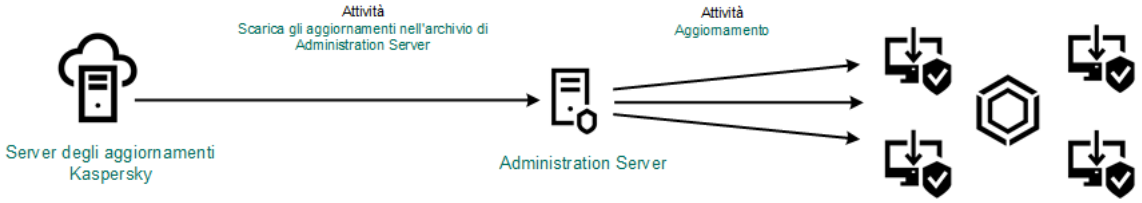
   È possibile scaricare il pacchetto di aggiornamenti in una cartella condivisa utilizzando i seguenti metodi:

   - Utilizzando l'attività *Aggiornamento di database e moduli dell'applicazione* di Kaspersky Endpoint Security. L'attività è destinata a uno dei computer della rete locale dell'azienda.

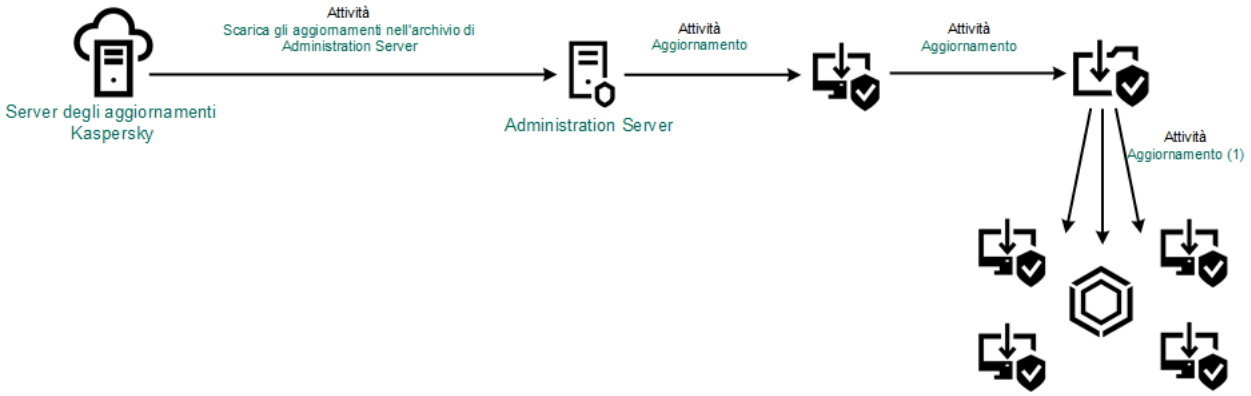
   - Tramite Kaspersky Update Utility. Per informazioni dettagliate sull'utilizzo di Kaspersky Update Utility, consultare la Knowledge Base di Kaspersky.

3. Distribuire il pacchetto di aggiornamenti ai computer client.

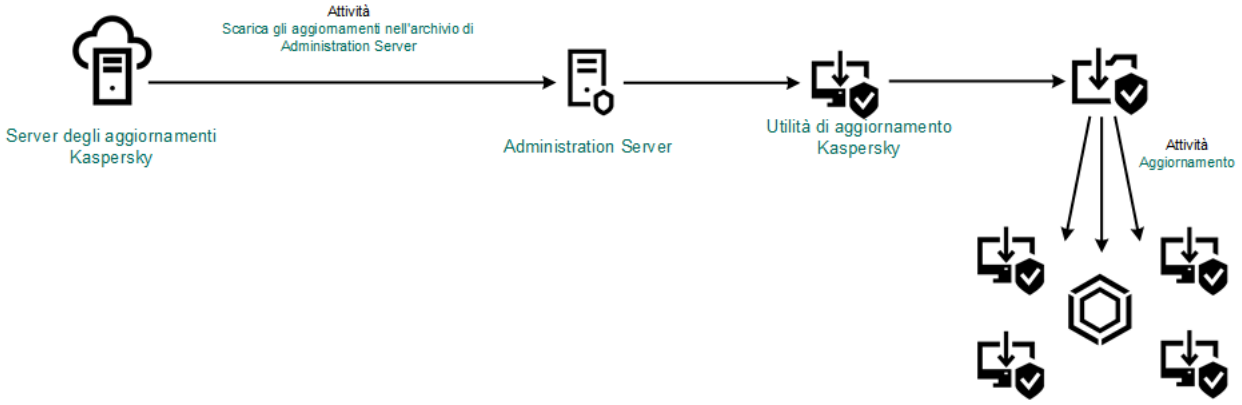
   Il pacchetto di aggiornamenti viene distribuito ai computer client da parte dell'attività *Aggiornamento di database e moduli dell'applicazione* di Kaspersky Endpoint Security. È possibile creare un numero illimitato di attività di aggiornamento per ogni gruppo di amministrazione.



Aggiornamento da un archivio server



Aggiornamento da una cartella condivisa



Aggiornamento tramite Kaspersky Update Utility

Per Kaspersky Security Center l'elenco predefinito di sorgenti degli aggiornamenti contiene Kaspersky Security Center Administration Server e i server degli aggiornamenti Kaspersky. Per Kaspersky Security Center Cloud Console, l'elenco predefinito di sorgenti degli aggiornamenti contiene punti di distribuzione e server degli aggiornamenti Kaspersky. Per informazioni dettagliate sui punti di distribuzione, consultare la Guida di Kaspersky Security Center Cloud Console. È possibile aggiungere all'elenco altre sorgenti degli aggiornamenti. È possibile specificare server HTTP/FTP e cartelle condivise come sorgenti degli aggiornamenti. Se un aggiornamento non può essere eseguito da una determinata sorgente degli aggiornamenti, Kaspersky Endpoint Security passa a quella successiva.

Gli aggiornamenti vengono scaricati dai server degli aggiornamenti Kaspersky o da altri server FTP o HTTP tramite i protocolli di rete standard. Se la connessione a un server proxy è necessaria per l'accesso alla sorgente degli aggiornamenti, specificare le impostazioni del server proxy nel criterio di Kaspersky Endpoint Security.

Aggiornamento da un archivio server

Per ridurre il traffico Internet, è possibile configurare gli aggiornamenti dei database e dei moduli dell'applicazione nei computer della LAN aziendale da un archivio server. A tale scopo, Kaspersky Security Center deve scaricare un pacchetto di aggiornamenti nell'archivio (server FTP o HTTP, rete o cartella locale) dai server degli aggiornamenti Kaspersky. Gli altri computer della LAN aziendale saranno in grado di ricevere il pacchetto di aggiornamenti dall'archivio server.

La configurazione degli aggiornamenti dei database e dei moduli dell'applicazione da un archivio server comprende i seguenti passaggi:

1. Configurare il download di un pacchetto di aggiornamenti nell'archivio di Administration Server (attività *Scarica aggiornamenti nell'archivio dell'Administration Server*).

   L'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* viene creata automaticamente dall'Avvio rapido guidato di Administration Server e può avere solo un'istanza. Per impostazione predefinita, Kaspersky Security Center copia il pacchetto di aggiornamento nella cartella `\\<server name>\KLSHARE\Updates`. Per ulteriori informazioni sul download degli aggiornamenti dell'archivio dell'Administration Server, consultare la Guida di Kaspersky Security Center.

2. Configurare gli aggiornamenti dei database e dei moduli dell'applicazione dall'archivio server specificato negli altri computer della LAN aziendale (attività *Aggiornamento di database e moduli dell'applicazione*).

   Come configurare l'aggiornamento di Kaspersky Endpoint Security dall'archivio server specificato in Administration Console (MMC)

   1. Aprire Kaspersky Security Center Administration Console.

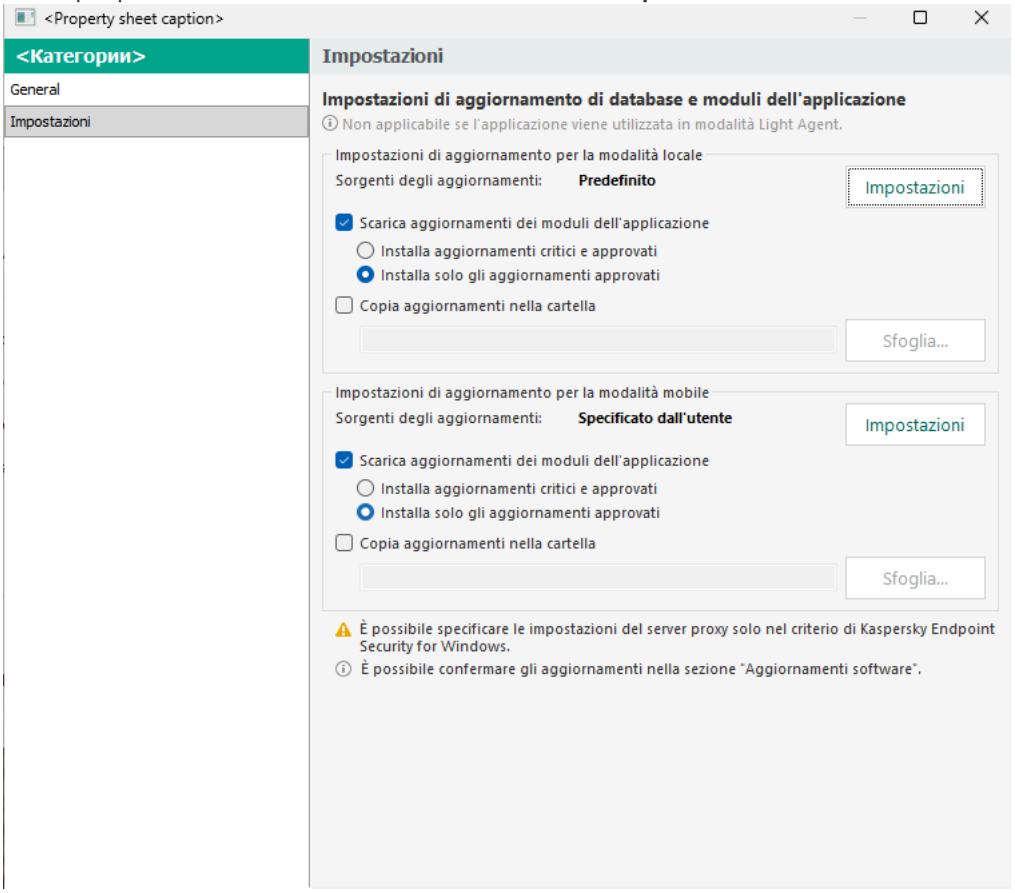
      Nella struttura della console, selezionare **Attività**.

   2. Fare clic sull'attività **Aggiornamento di database e moduli dell'applicazione** di Kaspersky Endpoint Security.

      Verrà visualizzata la finestra delle proprietà dell'attività.

      L'attività *Aggiornamento di database e moduli dell'applicazione* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento di database e moduli dell'applicazione*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

3. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.



Impostazioni attività di Aggiornamento di database e moduli dell'applicazione

4. Nel blocco **Impostazioni di aggiornamento per la modalità locale**, fare clic sul pulsante **Impostazioni**.

5. Nell'elenco delle sorgenti degli aggiornamenti, assicurarsi che l'aggiornamento dalla sorgente **Kaspersky Security Center** sia abilitato. Inoltre, la sorgente **Kaspersky Security Center** deve avere la massima priorità.

6. Se necessario, aggiungere le sorgenti degli aggiornamenti:

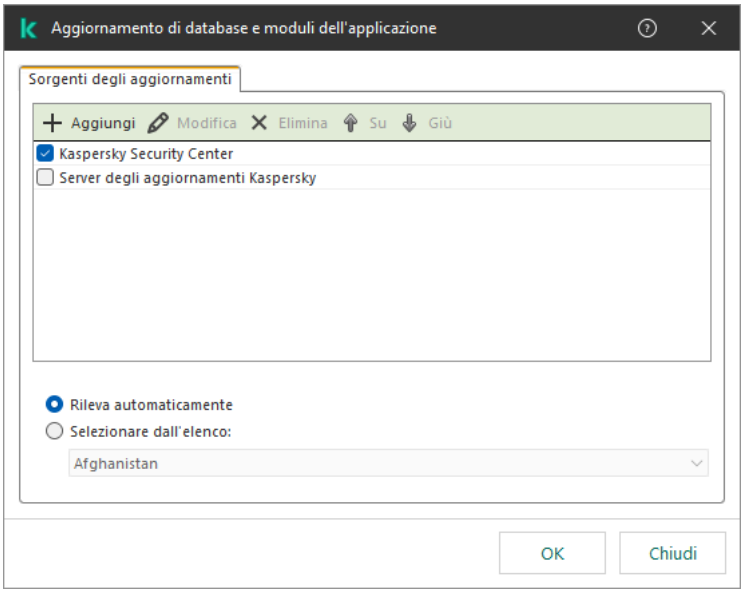
   a. Nell'elenco delle sorgenti degli aggiornamenti fare clic sul pulsante **Aggiungi**.

   b. Nel campo **Sorgenti degli aggiornamenti** specificare l'indirizzo del server FTP o HTTP, la cartella di rete o la cartella locale in cui Kaspersky Security Center copierà il pacchetto degli aggiornamenti ricevuto dai server Kaspersky.

   > L'indirizzo della sorgente degli aggiornamenti deve corrispondere all'indirizzo specificato nel campo **Cartella per l'archiviazione degli aggiornamenti** in cui è stato configurato il download degli aggiornamenti nell'archivio server (attività *Scarica aggiornamenti nell'archivio dell'Administration Server*).

   c. Fare clic su **OK**.

È possibile escludere la sorgente degli aggiornamenti senza rimuoverla nell'elenco delle sorgenti degli aggiornamenti. A tale scopo, deselezionare la casella di controllo accanto all'oggetto.



Sorgenti dell'aggiornamento

7. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

   Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.

8. Nella finestra delle proprietà dell'attività, selezionare la sezione **Pianificazione** e configurare la modalità di esecuzione dell'attività.

9. Per impostazione predefinita, Kaspersky Endpoint Security esegue l'attività in modalità manuale.

10. Salvare le modifiche.

Come configurare l'aggiornamento di Kaspersky Endpoint Security dall'archivio server specificato in Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Aggiornamento** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   L'attività *Aggiornamento* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

3. Selezionare la scheda **Impostazioni applicazione → Modalità locale**.

4. Nell'elenco delle sorgenti degli aggiornamenti, assicurarsi che l'aggiornamento dalla sorgente **Kaspersky Security Center** sia abilitato. Inoltre, la sorgente **Kaspersky Security Center** deve avere la massima priorità.

5. Se necessario, aggiungere le sorgenti degli aggiornamenti:

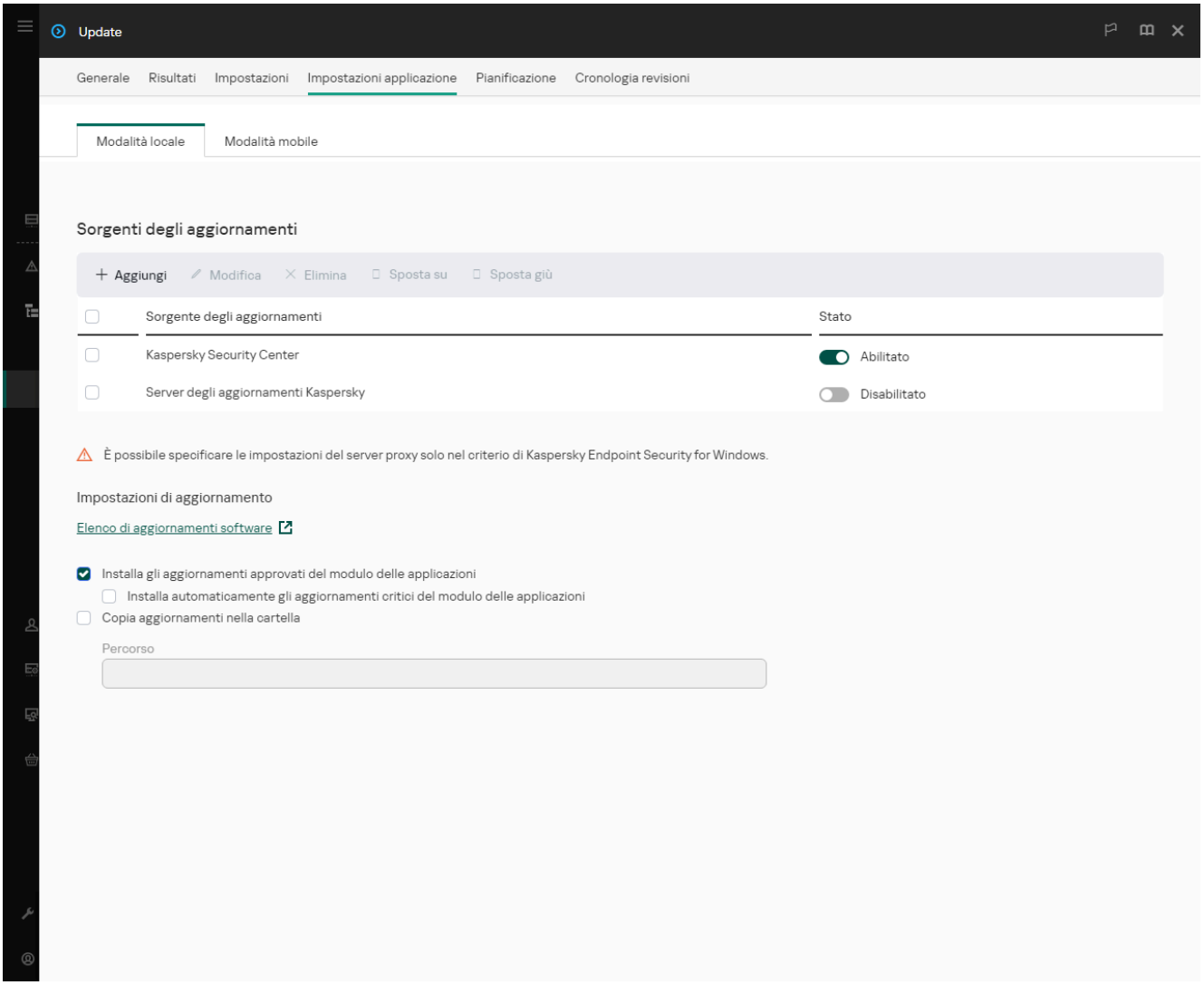
   a. Nell'elenco delle sorgenti degli aggiornamenti fare clic sul pulsante **Aggiungi**.

   b. Nel campo **Aggiorna origini** specificare l'indirizzo del server FTP o HTTP, la cartella di rete o la cartella locale in cui Kaspersky Security Center copierà il pacchetto degli aggiornamenti ricevuto dai server Kaspersky.

      L'indirizzo della sorgente degli aggiornamenti deve corrispondere all'indirizzo specificato nel campo **Cartella per l'archiviazione degli aggiornamenti** in cui è stato configurato il download degli aggiornamenti nell'archivio server (attività *Scarica aggiornamenti nell'archivio dell'Administration Server*).

   c. Fare clic su **Salva**.

È possibile escludere la sorgente degli aggiornamenti senza rimuoverla nell'elenco delle sorgenti degli aggiornamenti. A tale scopo, impostare l'interruttore accanto ad esso in posizione disattivato.



Sorgenti dell'aggiornamento

6. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Sposta su** e **Sposta giù**.

   Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.

7. Nella finestra delle proprietà dell'attività, selezionare la sezione **Pianificazione** e configurare la modalità di esecuzione dell'attività.

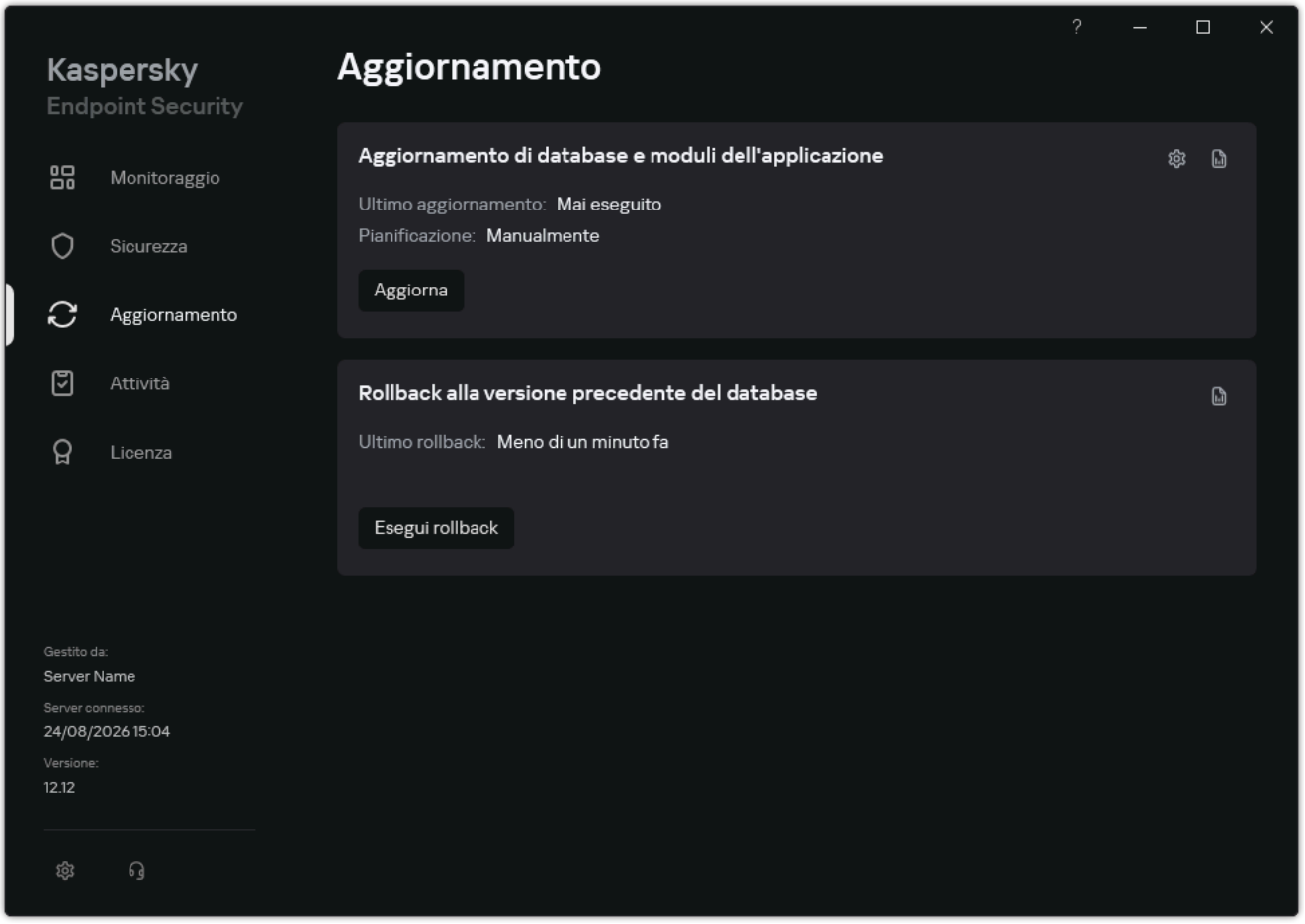
8. Per impostazione predefinita, Kaspersky Endpoint Security esegue l'attività in modalità manuale.

9. Salvare le modifiche.

Come configurare l'aggiornamento di Kaspersky Endpoint Security dall'archivio server specificato nell'interfaccia dell'applicazione

Non è possibile configurare l'attività di gruppo *Aggiornamento di database e moduli dell'applicazione* nell'interfaccia dell'applicazione. Solo un'attività di aggiornamento locale, *Aggiornamento di database e moduli dell'applicazione*, è disponibile per l'utente. Se l'attività *Aggiornamento di database e moduli dell'applicazione* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.



Attività di aggiornamento locali

2. Si apre l'elenco delle attività; selezionare l'attività *Aggiornamento di database e moduli dell'applicazione* e fare clic su ⚙.

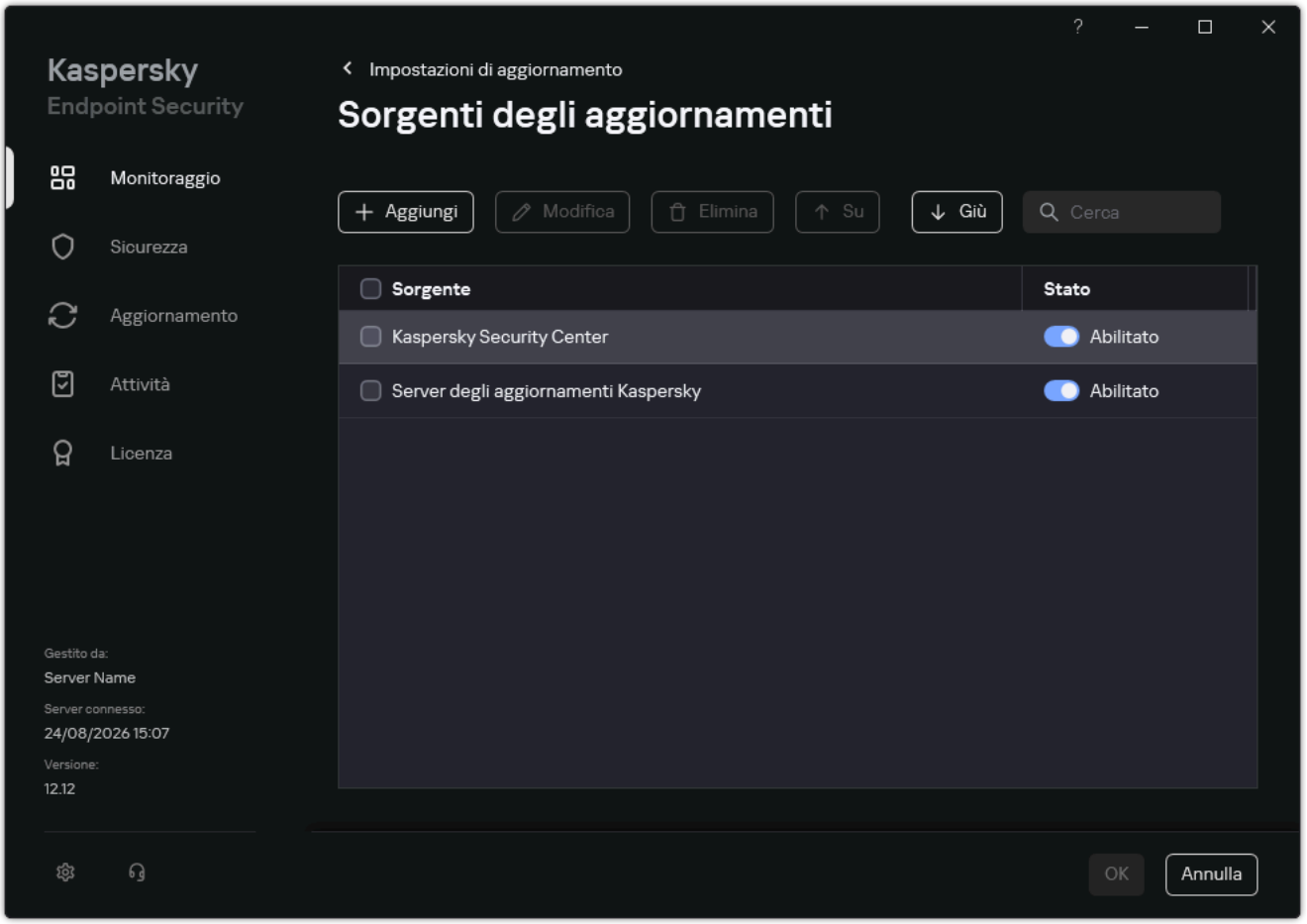
   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Nella finestra delle proprietà dell'attività, fare clic su **Seleziona sorgenti degli aggiornamenti**.

4. Nell'elenco delle sorgenti degli aggiornamenti, assicurarsi che l'aggiornamento dalla sorgente **Kaspersky Security Center** sia abilitato. Inoltre, la sorgente **Kaspersky Security Center** deve avere la massima priorità.

5. Se necessario, aggiungere le sorgenti degli aggiornamenti:

   a. Nell'elenco delle sorgenti degli aggiornamenti fare clic sul pulsante **Aggiungi**.



Sorgenti dell'aggiornamento

   a. Specificare l'indirizzo del server FTP o HTTP, la cartella di rete o la cartella locale in cui Kaspersky Security Center copierà il pacchetto degli aggiornamenti ricevuto dai server Kaspersky.

      L'indirizzo della sorgente degli aggiornamenti deve corrispondere all'indirizzo specificato nel campo **Cartella per l'archiviazione degli aggiornamenti** in cui è stato configurato il download degli aggiornamenti nell'archivio server (attività *Scarica aggiornamenti nell'archivio dell'Administration Server*).

   b. Fare clic su **Seleziona**.

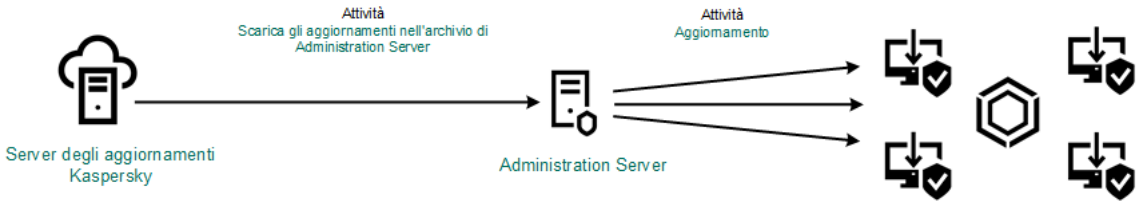
   È possibile escludere la sorgente degli aggiornamenti senza rimuoverla nell'elenco delle sorgenti degli aggiornamenti. A tale scopo, impostare l'interruttore accanto ad esso in posizione disattivato.

6. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

   Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.

Se un computer è gestito da Kaspersky Security Center, non è possibile configurare la modalità di esecuzione per l'attività *Aggiornamento di database e moduli dell'applicazione*. L'attività può essere eseguita solo manualmente.

7. Salvare le modifiche.



Aggiornamento da un archivio server

Aggiornamento da una cartella condivisa

Per ridurre il traffico Internet, è possibile configurare gli aggiornamenti dei database e dei moduli dell'applicazione nei computer della LAN aziendale da una cartella condivisa. A tale scopo, uno dei computer della LAN aziendale deve ricevere i pacchetti degli aggiornamenti da Kaspersky Security Center Administration Server o dai server degli aggiornamenti Kaspersky, quindi copia il pacchetto degli aggiornamenti ricevuto nella cartella condivisa. Gli altri computer della LAN aziendale saranno in grado di ricevere il pacchetto di aggiornamenti da questa cartella condivisa.

La versione e la localizzazione dell'applicazione Kaspersky Endpoint Security che copia il pacchetto di aggiornamento in una cartella condivisa devono corrispondere alla versione e alla localizzazione dell'applicazione che aggiorna i database dalla cartella condivisa. Se le versioni o le localizzazioni delle applicazioni non corrispondono, l'aggiornamento del database potrebbe terminare con un errore.

La configurazione degli aggiornamenti dei database e dei moduli dell'applicazione da una cartella condivisa comprende i seguenti passaggi:

1. Configurazione degli aggiornamenti del database e del modulo dell'applicazione da un archivio server.

2. L'abilitazione della copia di un pacchetto di aggiornamento in una cartella condivisa in uno dei computer nella rete locale.

   Come abilitare la copia del pacchetto di aggiornamento nella cartella condivisa in Administration Console (MMC)

   1. Aprire Kaspersky Security Center Administration Console.

   2. Nella struttura della console, selezionare **Attività**.

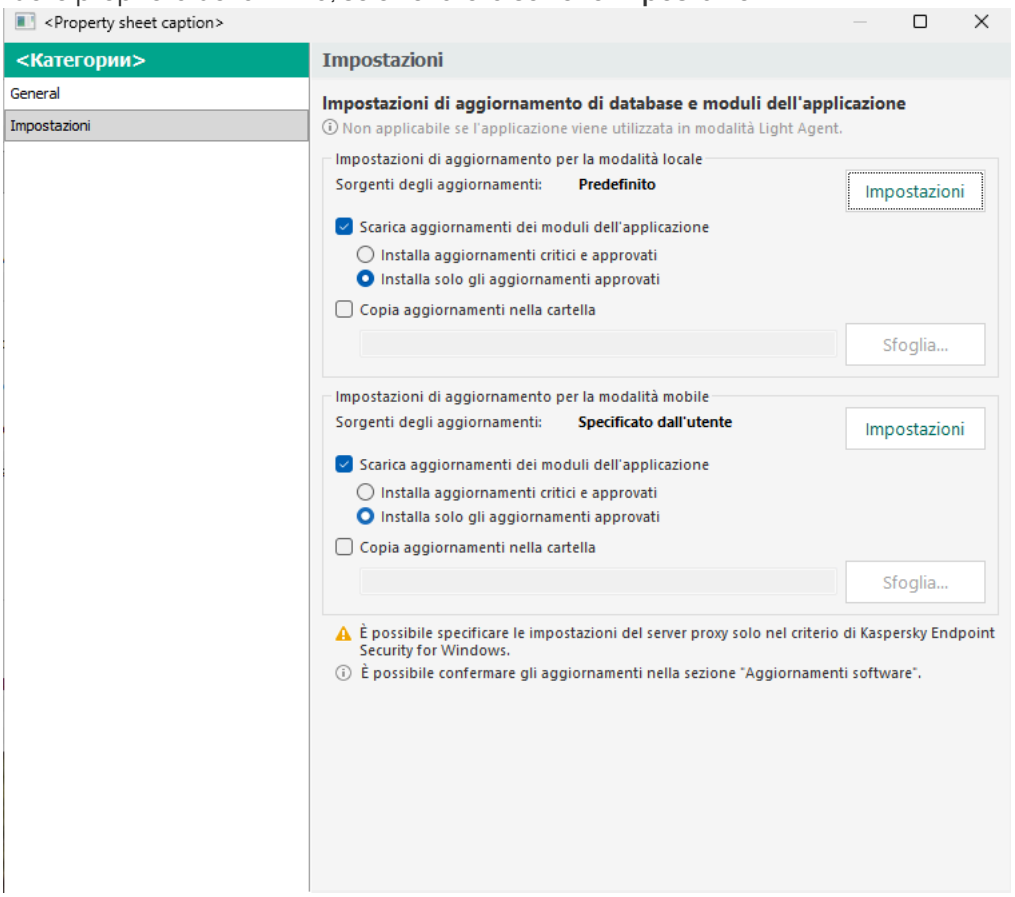
      L'attività *Aggiornamento di database e moduli dell'applicazione* deve essere assegnata per un computer che avrà il ruolo di sorgente degli aggiornamenti.

   3. Fare clic sull'attività **Aggiornamento di database e moduli dell'applicazione** di Kaspersky Endpoint Security.

      Verrà visualizzata la finestra delle proprietà dell'attività.

L'attività *Aggiornamento di database e moduli dell'applicazione* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento di database e moduli dell'applicazione*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

4. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.



Impostazioni attività di Aggiornamento di database e moduli dell'applicazione

5. Nel blocco **Impostazioni di aggiornamento per la modalità locale**, fare clic sul pulsante **Impostazioni**.

6. Configurare le sorgenti degli aggiornamenti.

   Le sorgenti degli aggiornamenti possono essere i server degli aggiornamenti Kaspersky, Kaspersky Security Center Administration Server, altri server FTP o HTTP, cartelle locali o cartelle di rete.

7. Selezionare la casella di controllo **Copia aggiornamenti nella cartella**.

8. Nel campo **Percorso cartella** immettere il percorso UNC della cartella condivisa (ad esempio, `\\<server name>\KLSHARE\Updates`).

   Se il campo rimane vuoto, Kaspersky Endpoint Security copierà il pacchetto degli aggiornamenti nella cartella `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. Salvare le modifiche.

Come abilitare la copia del pacchetto di aggiornamento nella cartella condivisa in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

L'attività *Aggiornamento* deve essere assegnata per un computer che avrà il ruolo di sorgente degli aggiornamenti.

2. Fare clic sull'attività **Aggiornamento** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   L'attività *Aggiornamento* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

3. Selezionare la scheda **Impostazioni applicazione** → **Modalità locale**.

4. Configurare le sorgenti degli aggiornamenti.

   Le sorgenti degli aggiornamenti possono essere i server degli aggiornamenti Kaspersky, Kaspersky Security Center Administration Server, altri server FTP o HTTP, cartelle locali o cartelle di rete.

5. Selezionare la casella di controllo **Copia aggiornamenti nella cartella**.

6. Nel campo **Percorso** immettere il percorso UNC della cartella condivisa (ad esempio, `\\<server name>\KLSHARE\Updates`).

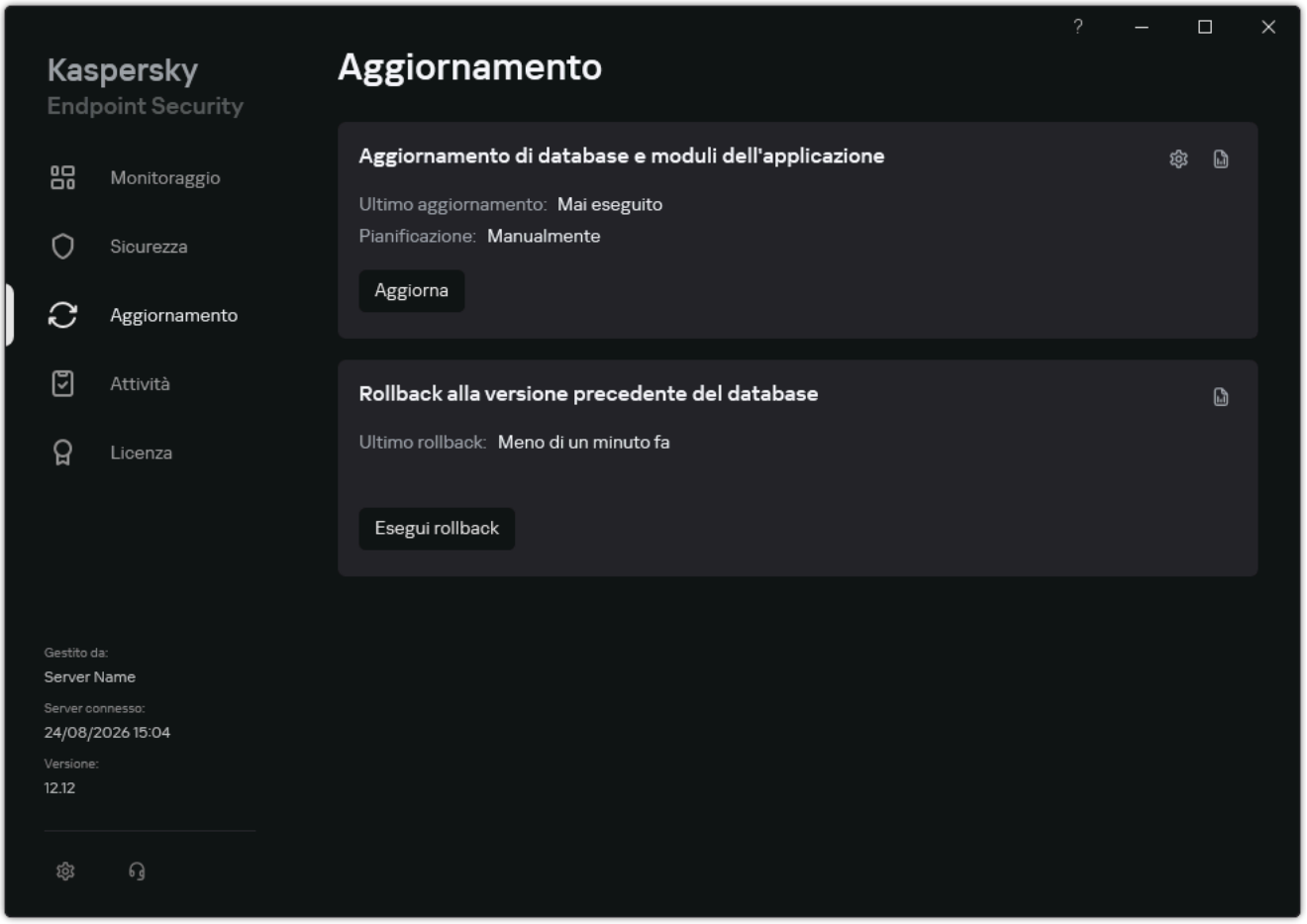
   Se il campo rimane vuoto, Kaspersky Endpoint Security copierà il pacchetto degli aggiornamenti nella cartella `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Salvare le modifiche.

Come abilitare la copia del pacchetto di aggiornamento nella cartella condivisa nell'interfaccia dell'applicazione

Non è possibile configurare l'attività di gruppo *Aggiornamento di database e moduli dell'applicazione* nell'interfaccia dell'applicazione. Solo un'attività di aggiornamento locale, *Aggiornamento di database e moduli dell'applicazione*, è disponibile per l'utente. Se l'attività *Aggiornamento di database e moduli dell'applicazione* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.



Attività di aggiornamento locali

2. Si apre l'elenco delle attività; selezionare l'attività *Aggiornamento di database e moduli dell'applicazione* e fare clic su ⚙.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Nella sezione **Distribuzione degli aggiornamenti** selezionare la casella di controllo **Copia aggiornamenti nella cartella**.

4. Immettere il percorso UNC nella cartella condivisa (ad esempio, `\\<server name>\KLSHARE\Updates`).

5. Salvare le modifiche.

3. Configurare gli aggiornamenti dei database e dei moduli dell'applicazione dalla cartella condivisa specificata negli altri computer della LAN aziendale.

Come configurare gli aggiornamenti da una cartella condivisa in Administration Console (MMC)

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Aggiornamento di database e moduli dell'applicazione**.

4. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

5. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2) → Aggiornamento di database e moduli dell'applicazione**.

Passaggio 2. Selezione delle sorgenti degli aggiornamenti

Aggiungere una nuova sorgente degli aggiornamenti: una cartella condivisa. L'indirizzo sorgente deve corrispondere all'indirizzo specificato precedentemente nel campo **Percorso cartella** quando è stata configurata la copia del pacchetto di aggiornamenti nella cartella condivisa. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

Passaggio 3. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

L'attività *Aggiornamento di database e moduli dell'applicazione* deve essere assegnata ai computer della LAN aziendale, ad eccezione del computer con il ruolo di sorgente degli aggiornamenti.

Passaggio 4. Selezione dell'account per eseguire l'attività

Selezione dell'account per eseguire l'attività *Aggiornamento di database e moduli dell'applicazione*. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.

Passaggio 5. Configurazione di una pianificazione di avvio dell'attività

Configurare una pianificazione per l'avvio di un'attività, ad esempio manualmente o dopo il download dei database anti-virus nell'archivio.

Passaggio 6. Definizione del nome dell'attività

Immettere il nome dell'attività, ad esempio *Aggiornamento da una cartella condivisa*.

Passaggio 7. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività. In seguito a questa operazione, verrà eseguita l'attività di aggiornamento nei computer degli utenti in base alla pianificazione specificata.

Come configurare gli aggiornamenti dalla cartella condivisa in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Aggiornamento**.

   c. Nel campo **Nome attività**, immettere una breve descrizione, ad esempio *Aggiornamento da una cartella condivisa*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

   > L'attività *Aggiornamento* deve essere assegnata ai computer della LAN aziendale, ad eccezione del computer con il ruolo di sorgente degli aggiornamenti.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata, quindi procedere con il passaggio successivo.

5. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nella tabella delle attività.

6. Fare clic sulla nuova attività *Aggiornamento* creata.

   Verrà visualizzata la finestra delle proprietà dell'attività.

7. Selezionare la scheda **Impostazioni applicazione** → **Modalità locale**.

8. Nel blocco **Aggiorna origini**, fare clic sul pulsante **Aggiungi**.

9. Nella finestra visualizzata, immettere il percorso della cartella condivisa.

   > L'indirizzo sorgente deve corrispondere all'indirizzo specificato precedentemente nel campo **Percorso** quando è stata configurata la copia del pacchetto di aggiornamenti nella cartella condivisa (vedere le istruzioni riportate sopra).

10. Fare clic su **OK**.

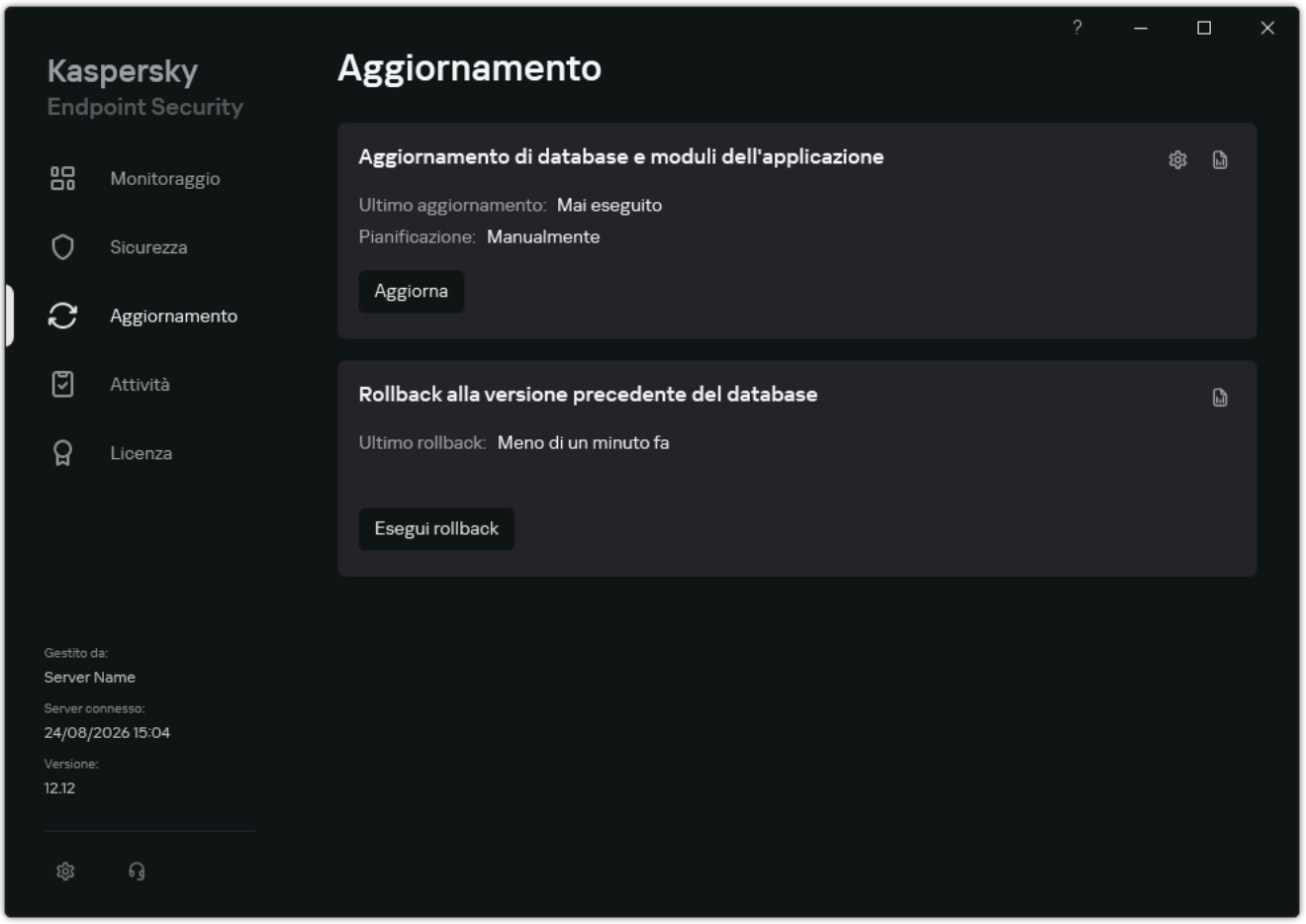
11. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Sposta su** e **Sposta giù**.

12. Salvare le modifiche.

Come configurare gli aggiornamenti dalla cartella condivisa nell'interfaccia dell'applicazione

Non è possibile configurare l'attività di gruppo *Aggiornamento di database e moduli dell'applicazione* nell'interfaccia dell'applicazione. Solo un'attività di aggiornamento locale, *Aggiornamento di database e moduli dell'applicazione*, è disponibile per l'utente. Se l'attività *Aggiornamento di database e moduli dell'applicazione* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.



Attività di aggiornamento locali

2. Si apre l'elenco delle attività; selezionare l'attività *Aggiornamento di database e moduli dell'applicazione* e fare clic su ⚙.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Fare clic su **Seleziona sorgenti degli aggiornamenti**.

4. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.

5. Nella finestra visualizzata, immettere il percorso della cartella condivisa.

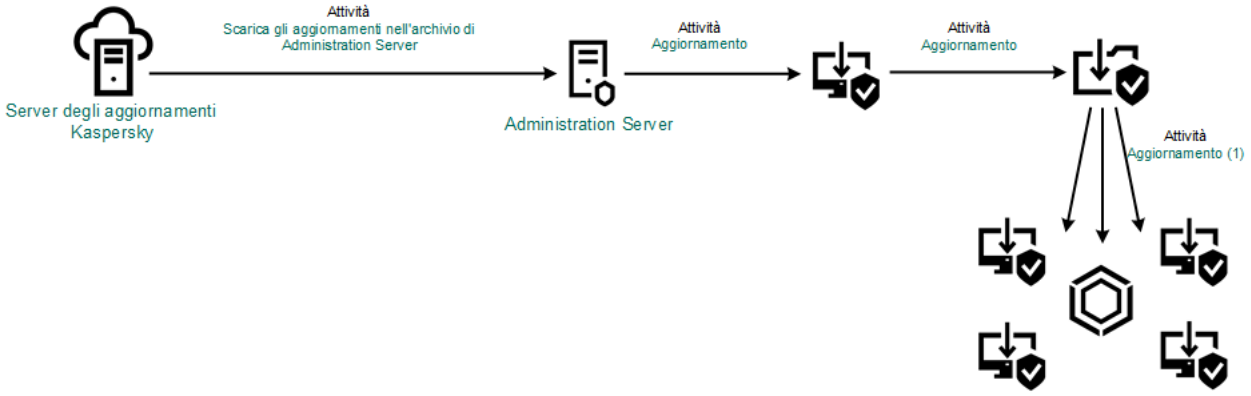
   L'indirizzo sorgente deve corrispondere all'indirizzo specificato precedentemente quando è stata configurata la copia del pacchetto di aggiornamenti nella cartella condivisa (vedere le istruzioni riportate sopra).

6. Fare clic su **Seleziona**.

7. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

   Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.

8. Salvare le modifiche.



Aggiornamento da una cartella condivisa

Aggiornamento tramite Kaspersky Update Utility

Per ridurre il traffico Internet, è possibile configurare gli aggiornamenti dei database e dei moduli dell'applicazione nei computer della LAN aziendale da una cartella condivisa utilizzando Kaspersky Update Utility. A tale scopo, uno dei computer della LAN aziendale deve ricevere i pacchetti degli aggiornamenti da Kaspersky Security Center Administration Server o dai server degli aggiornamenti Kaspersky, quindi copiare i pacchetti degli aggiornamenti ricevuti nella cartella condivisa utilizzando l'utilità. Gli altri computer della LAN aziendale saranno in grado di ricevere il pacchetto di aggiornamenti da questa cartella condivisa.

La versione e la localizzazione dell'applicazione Kaspersky Endpoint Security che copia il pacchetto di aggiornamento in una cartella condivisa devono corrispondere alla versione e alla localizzazione dell'applicazione che aggiorna i database dalla cartella condivisa. Se le versioni o le localizzazioni delle applicazioni non corrispondono, l'aggiornamento del database potrebbe terminare con un errore.

La configurazione degli aggiornamenti dei database e dei moduli dell'applicazione da una cartella condivisa comprende i seguenti passaggi:

1. Configurazione degli aggiornamenti del database e del modulo dell'applicazione da un archivio server.

2. Installare Kaspersky Update Utility in uno dei computer della LAN dell'organizzazione.

3. Configurare la copia del pacchetto di aggiornamenti nella cartella condivisa nelle impostazioni di Kaspersky Update Utility.

   È possibile scaricare il pacchetto di distribuzione di Kaspersky Update Utility dal sito Web dell'Assistenza tecnica di Kaspersky. Dopo l'installazione dell'utilità, selezionare la sorgente dell'aggiornamento (ad esempio l'archivio di Administration Server) e la cartella condivisa nella quale Kaspersky Update Utility copierà i pacchetti di aggiornamenti. Per informazioni dettagliate sull'utilizzo di Kaspersky Update Utility, consultare la Knowledge Base di Kaspersky.

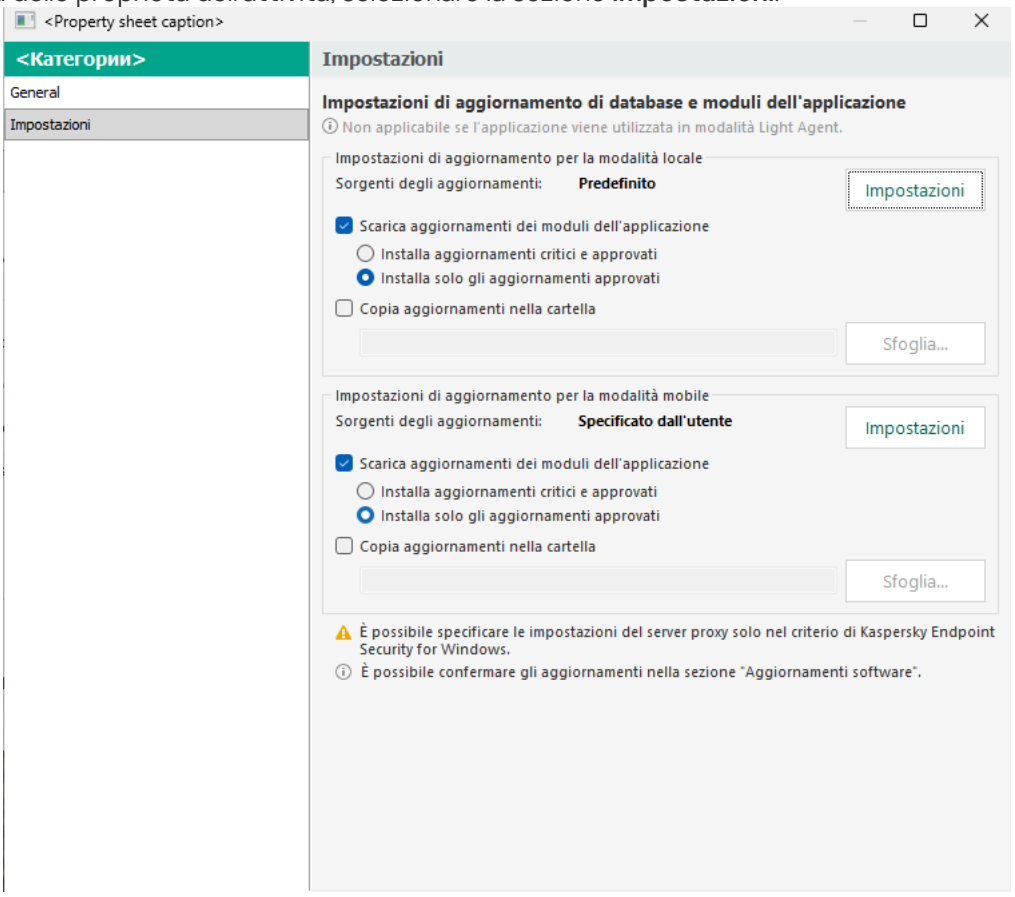
4. Configurare gli aggiornamenti dei database e dei moduli dell'applicazione dalla cartella condivisa specificata negli altri computer della LAN aziendale.

Come configurare gli aggiornamenti da una cartella condivisa in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Attività**.
3. Fare clic sull'attività **Aggiornamento di database e moduli dell'applicazione** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   L'attività *Aggiornamento di database e moduli dell'applicazione* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento di database e moduli dell'applicazione*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.
4. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.



Impostazioni attività di Aggiornamento di database e moduli dell'applicazione

5. Nel blocco **Impostazioni di aggiornamento per la modalità locale**, fare clic sul pulsante **Impostazioni**.
6. Nell'elenco delle sorgenti degli aggiornamenti fare clic sul pulsante **Aggiungi**.
7. Nella finestra visualizzata, immettere il percorso UNC della cartella condivisa (ad esempio, `\\<server name>\KLSHARE\Updates`).

   L'indirizzo sorgente deve corrispondere all'indirizzo indicato nelle impostazioni di Kaspersky Update Utility.
8. Fare clic su **OK**.

9. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

   Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.

10. Salvare le modifiche.

Come configurare gli aggiornamenti dalla cartella condivisa in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Aggiornamento** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   L'attività *Aggiornamento* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

3. Selezionare la scheda **Impostazioni applicazione** → **Modalità locale**.

4. Nell'elenco delle sorgenti degli aggiornamenti fare clic sul pulsante **Aggiungi**.

5. Nella finestra visualizzata, immettere il percorso UNC della cartella condivisa (ad esempio, `\\<server name>\KLSHARE\Updates`).

   L'indirizzo sorgente deve corrispondere all'indirizzo indicato nelle impostazioni di Kaspersky Update Utility.

6. Fare clic su **OK**.

7. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

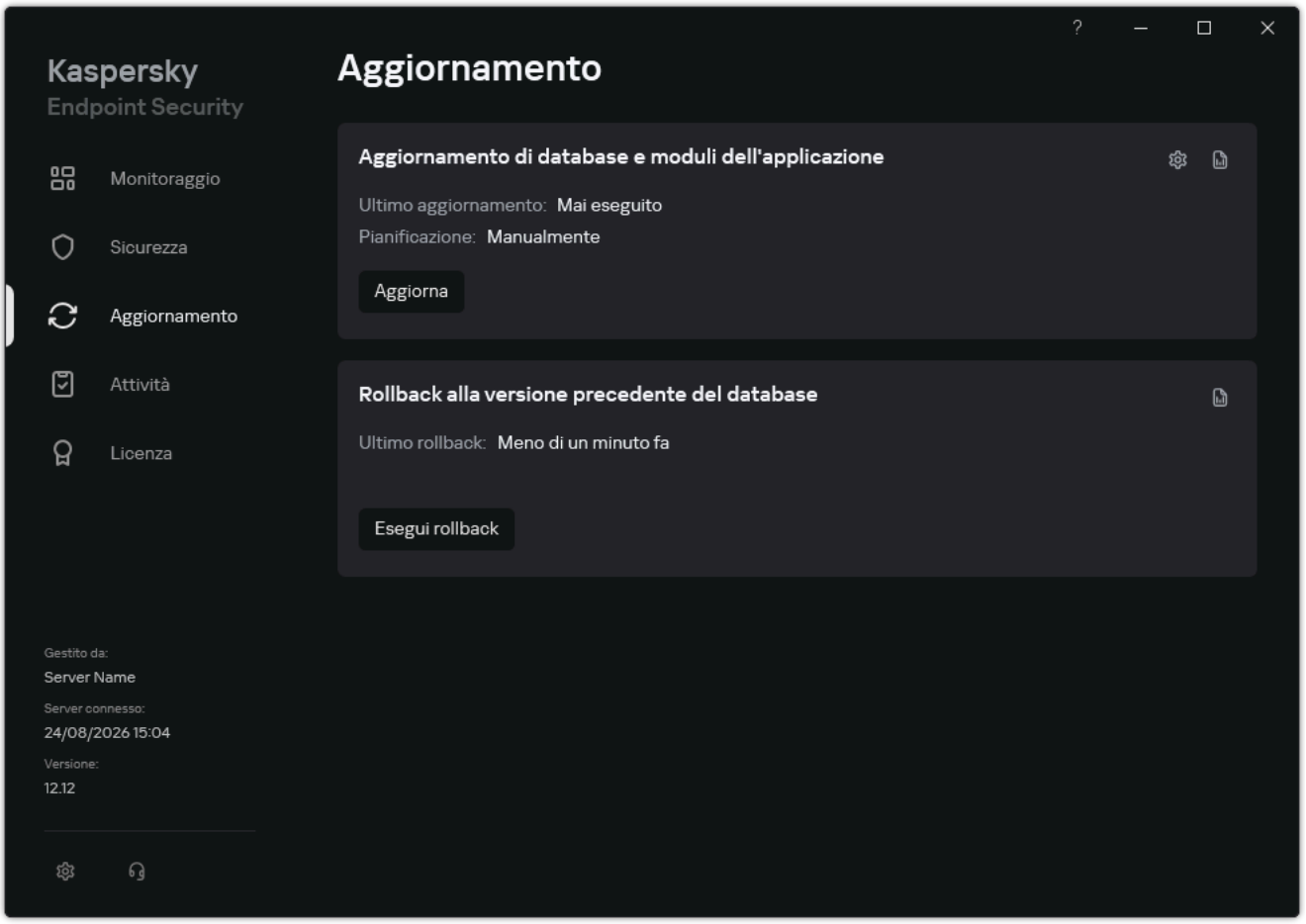
   Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.

8. Salvare le modifiche.

Come configurare gli aggiornamenti dalla cartella condivisa nell'interfaccia dell'applicazione

Non è possibile configurare l'attività di gruppo *Aggiornamento di database e moduli dell'applicazione* nell'interfaccia dell'applicazione. Solo un'attività di aggiornamento locale, *Aggiornamento di database e moduli dell'applicazione*, è disponibile per l'utente. Se l'attività *Aggiornamento di database e moduli dell'applicazione* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.



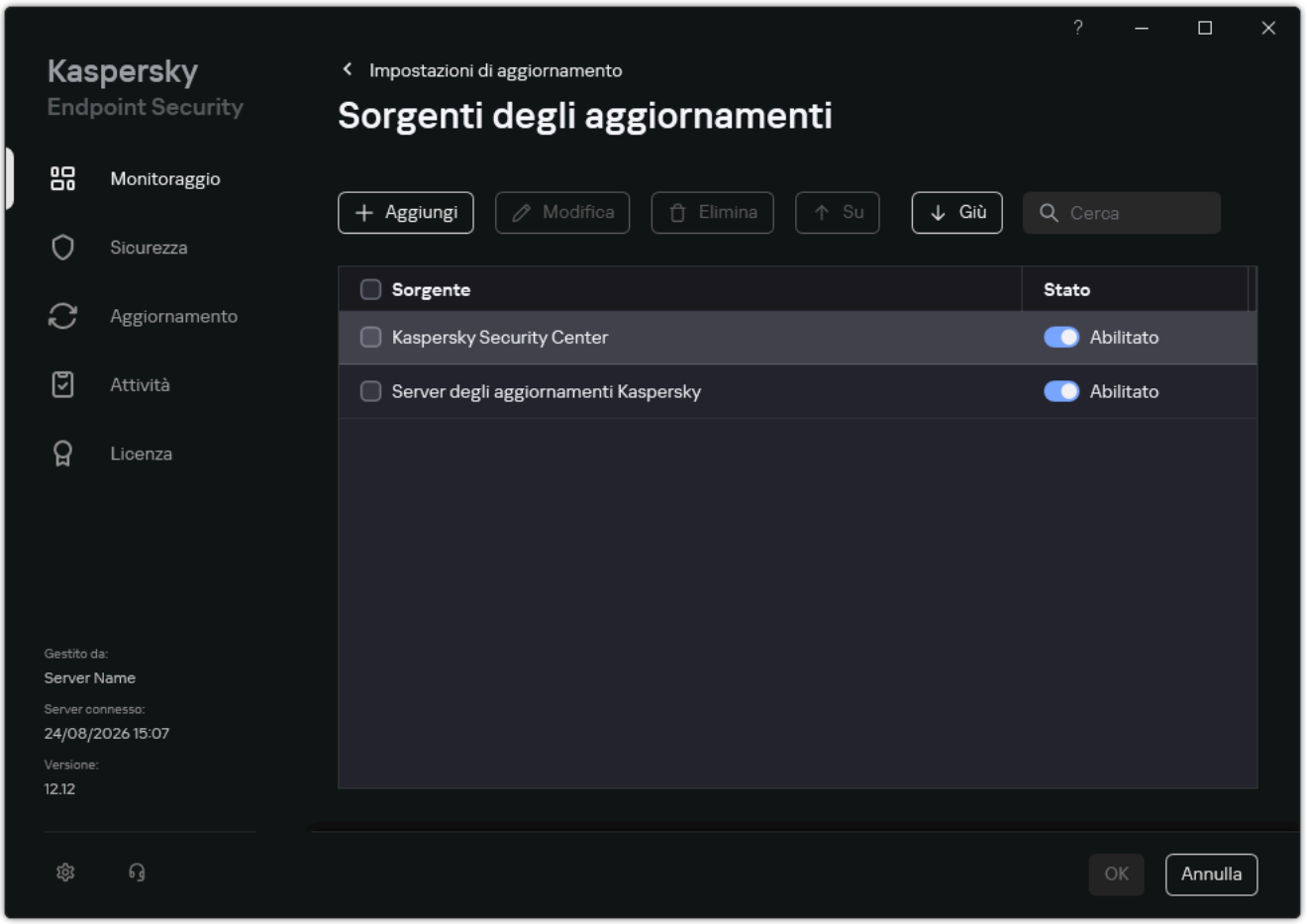
Attività di aggiornamento locali

2. Si apre l'elenco delle attività; selezionare l'attività *Aggiornamento di database e moduli dell'applicazione* e fare clic su ⚙.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Nella finestra delle proprietà dell'attività, fare clic su **Seleziona sorgenti degli aggiornamenti**.

4. Nell'elenco delle sorgenti degli aggiornamenti fare clic sul pulsante **Aggiungi**.



Sorgenti dell'aggiornamento

5. Immettere il percorso UNC nella cartella condivisa (ad esempio, `\\<server name>\KLSHARE\Updates`).

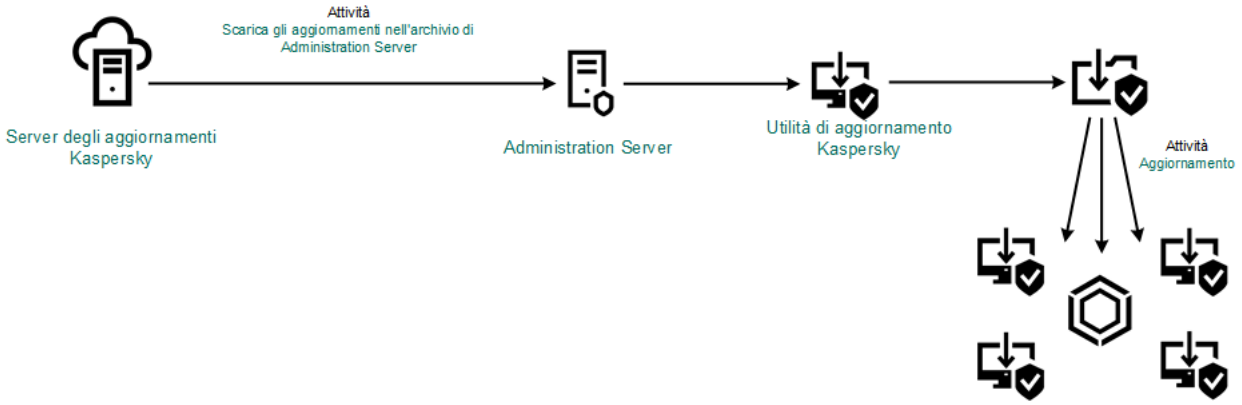
L'indirizzo sorgente deve corrispondere all'indirizzo indicato nelle impostazioni di Kaspersky Update Utility.

6. Fare clic su **Seleziona**.

7. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

   Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.

8. Salvare le modifiche.



Aggiornamento tramite Kaspersky Update Utility

Aggiornamento in modalità mobile

La *modalità mobile* è la modalità di esecuzione di Kaspersky Endpoint Security quando un computer esce dal perimetro di rete dell'organizzazione (*computer offline*). Per informazioni dettagliate sull'utilizzo dei computer offline e sugli utenti fuori sede, consultare la Guida di Kaspersky Security Center.

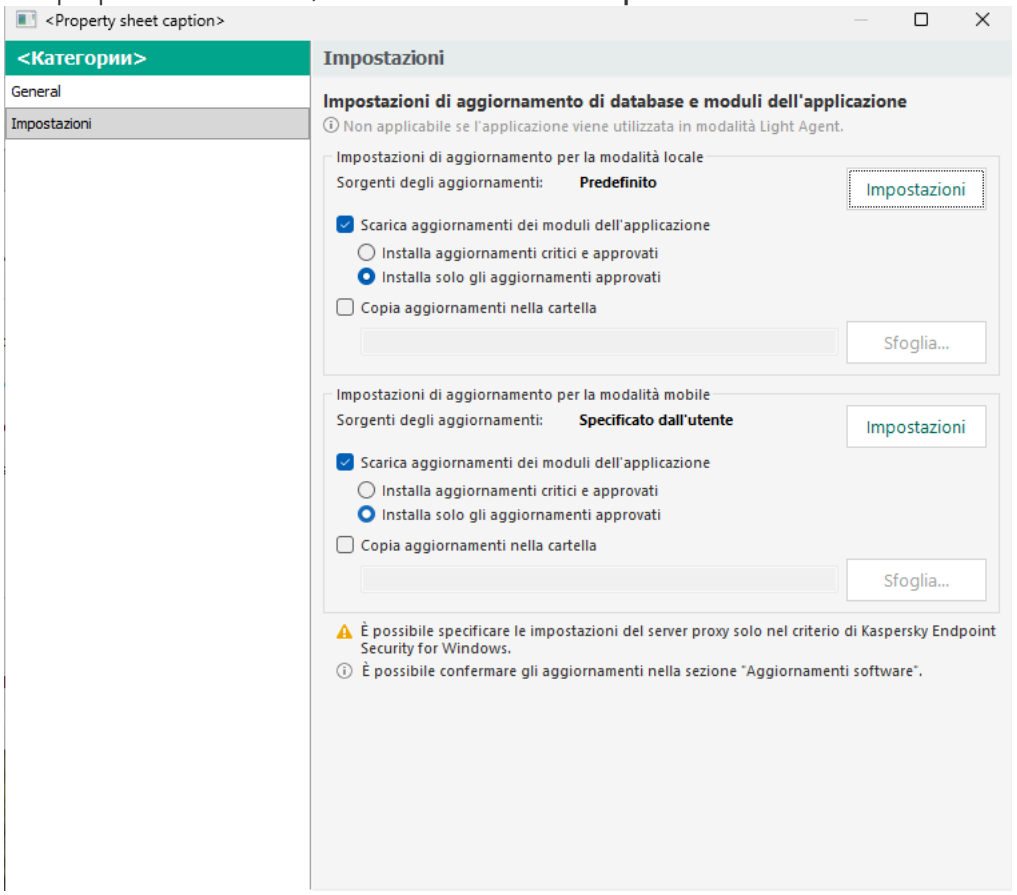
Un computer offline all'esterno della rete dell'organizzazione non può connettersi ad Administration Server per aggiornare i database e i moduli dell'applicazione. Per impostazione predefinita, solo i server degli aggiornamenti Kaspersky vengono utilizzati come sorgente degli aggiornamenti per l'aggiornamento dei database e dei moduli dell'applicazione in modalità mobile. L'utilizzo di un server proxy per la connessione a Internet è determinato da un apposito criterio fuori sede. Il criterio fuori sede deve essere creato separatamente. Quando Kaspersky Endpoint Security passa alla modalità mobile, l'attività di aggiornamento viene avviata ogni due ore.

Come configurare le impostazioni di aggiornamento per la modalità mobile in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Attività**.
3. Fare clic sull'attività **Aggiornamento di database e moduli dell'applicazione** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   L'attività *Aggiornamento di database e moduli dell'applicazione* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento di database e moduli dell'applicazione*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.
4. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.



Impostazioni attività di Aggiornamento di database e moduli dell'applicazione

5. Nel blocco **Impostazioni di aggiornamento per la modalità mobile**, fare clic sul pulsante **Impostazioni**.

6. Configurare le sorgenti degli aggiornamenti. Le sorgenti degli aggiornamenti possono essere i server degli aggiornamenti Kaspersky, altri server FTP e HTTP, cartelle locali o cartelle di rete.

7. Salvare le modifiche.

Come configurare le impostazioni di aggiornamento per la modalità mobile in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Aggiornamento** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   L'attività *Aggiornamento* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

3. Selezionare la scheda **Impostazioni applicazione** → **Modalità mobile**.

4. Configurare le sorgenti degli aggiornamenti. Le sorgenti degli aggiornamenti possono essere i server degli aggiornamenti Kaspersky, altri server FTP e HTTP, cartelle locali o cartelle di rete.

5. Salvare le modifiche.

In seguito a questa operazione, i database e i moduli dell'applicazione verranno aggiornati nei computer degli utenti quando si passa alla modalità mobile.

Avvio e arresto di un'attività di aggiornamento

Indipendentemente dalla modalità di esecuzione selezionata per l'attività di aggiornamento, è possibile avviare o arrestare un'attività di aggiornamento di Kaspersky Endpoint Security in qualsiasi momento.

Per avviare o arrestare un'attività di aggiornamento:

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.

2. Nel riquadro **Aggiornamento di database e moduli dell'applicazione**, fare clic sul pulsante **Aggiornamento** se si desidera avviare l'attività di aggiornamento.

   Kaspersky Endpoint Security inizierà ad aggiornare i moduli e i database dell'applicazione. L'applicazione visualizzerà lo stato di avanzamento dell'attività, la dimensione dei file scaricati e la sorgente degli aggiornamenti. È possibile interrompere l'attività in qualsiasi momento facendo clic sul pulsante **Interrompi aggiornamento**.

Per avviare o arrestare l'attività di aggiornamento quando viene visualizzata l'interfaccia dell'applicazione semplificata:

1. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni.

2. Nell'elenco a discesa **Attività** del menu di scelta rapida eseguire una delle seguenti operazioni:

   - selezionare un'attività di aggiornamento non in esecuzione per avviarla
   - selezionare un'attività di aggiornamento in esecuzione per interromperla
   - selezionare un'attività di aggiornamento sospesa per riprenderla o riavviarla

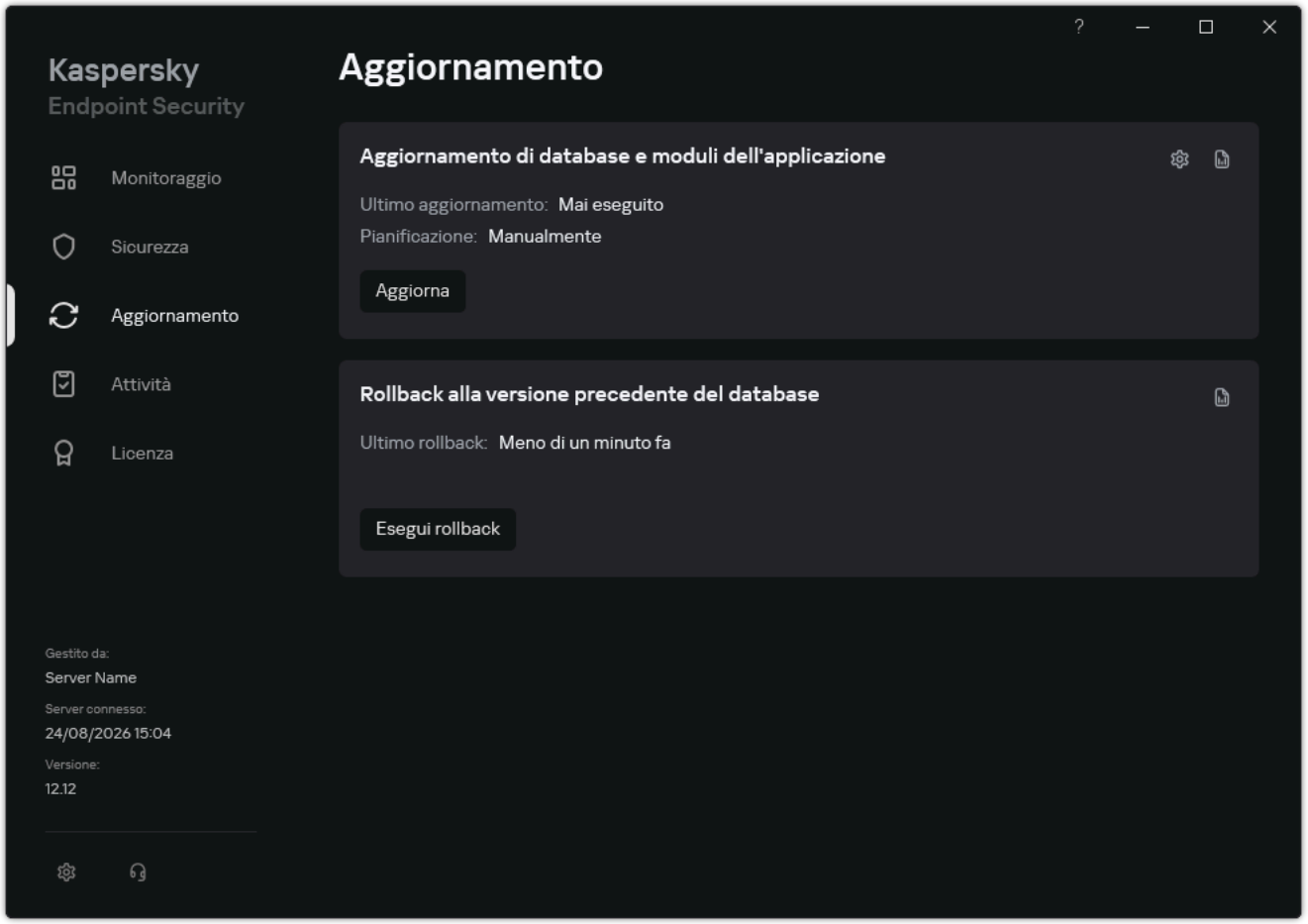
Avvio di un'attività di aggiornamento tramite i diritti di un account utente differente

Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività di aggiornamento tramite l'account utente con cui è stato eseguito l'accesso al sistema operativo. Tuttavia, Kaspersky Endpoint Security potrebbe essere aggiornato da una sorgente degli aggiornamenti a cui l'utente non può accedere perché non dispone dei diritti richiesti (ad esempio da una cartella condivisa che contiene un pacchetto di aggiornamento) oppure da una sorgente degli aggiornamenti per cui l'autenticazione sul server proxy non è configurata. Nelle impostazioni dell'applicazione, è possibile specificare un utente che dispone di tali diritti e avviare l'attività di aggiornamento di Kaspersky Endpoint Security utilizzando tale account utente.

Per avviare un'attività di aggiornamento utilizzando un altro account utente:

Non è possibile configurare l'attività di gruppo *Aggiornamento di database e moduli dell'applicazione* nell'interfaccia dell'applicazione. Solo un'attività di aggiornamento locale, *Aggiornamento di database e moduli dell'applicazione*, è disponibile per l'utente. Se l'attività *Aggiornamento di database e moduli dell'applicazione* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.



Attività di aggiornamento locali

2. Si apre l'elenco delle attività; selezionare l'attività *Aggiornamento di database e moduli dell'applicazione* e fare clic su ⚙.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Fare clic su **Esegui aggiornamenti dei database con i diritti utente**.

4. Nella finestra visualizzata, selezionare **Altro utente**.

5. Immettere le credenziali dell'account di un utente con le autorizzazioni necessarie per accedere alla sorgente degli aggiornamenti.

6. Salvare le modifiche.

Selezione della modalità di esecuzione dell'attività di aggiornamento

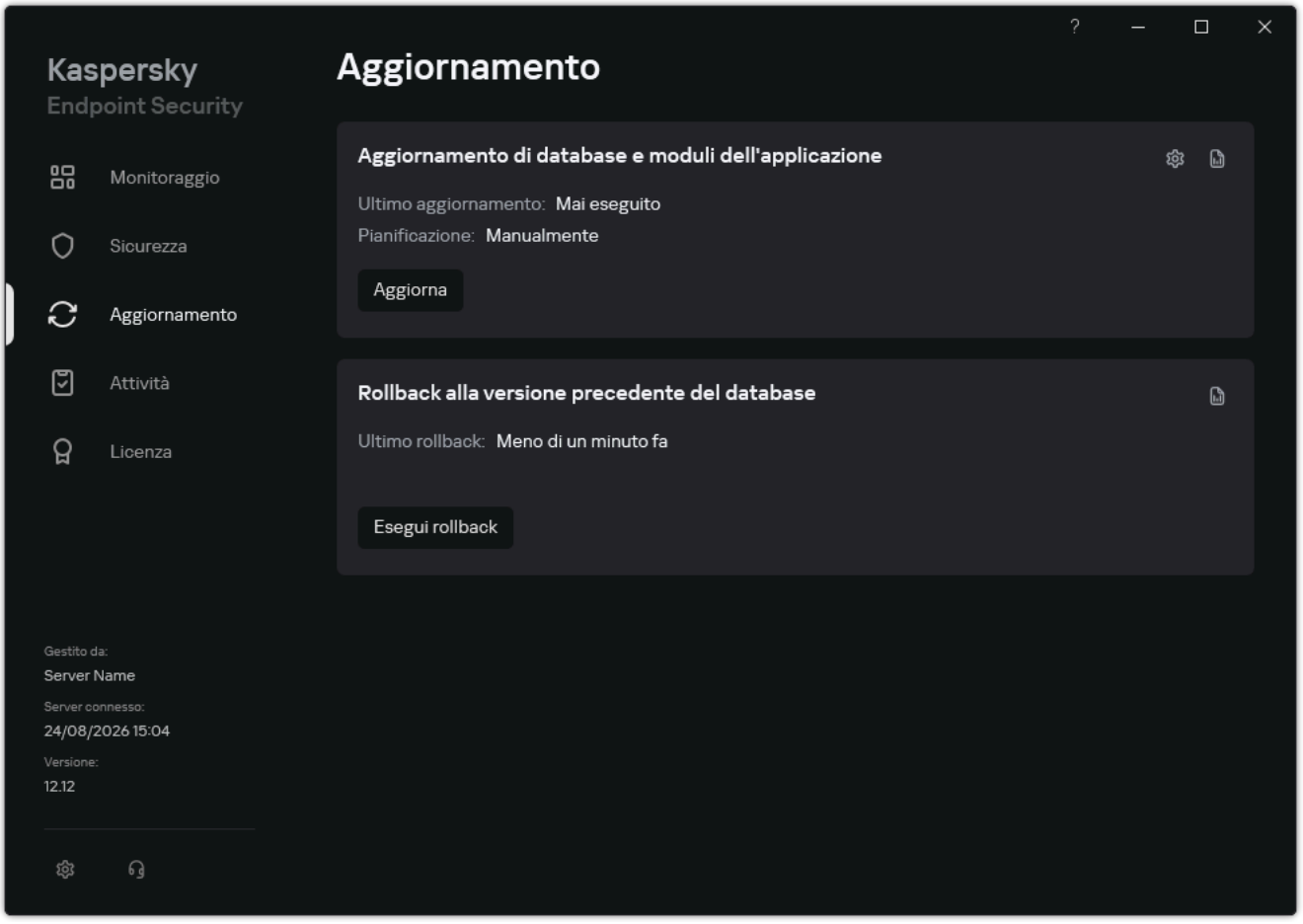
Se per qualsiasi motivo non è possibile eseguire l'attività di aggiornamento, ad esempio perché all'ora prevista il computer è spento, è possibile configurare l'attività non eseguita in modo che venga avviata automaticamente appena possibile.

È possibile rimandare l'esecuzione delle attività di aggiornamento dopo l'avvio dell'applicazione, se è stata selezionata la modalità di esecuzione **In base alla pianificazione** e se l'orario di avvio di Kaspersky Endpoint Security corrisponde alla pianificazione di avvio dell'attività di aggiornamento. L'attività di aggiornamento potrà essere eseguita solo dopo il periodo di tempo specificato dall'avvio di Kaspersky Endpoint Security.

Per selezionare la modalità di esecuzione dell'attività di aggiornamento:

Non è possibile configurare l'attività di gruppo *Aggiornamento di database e moduli dell'applicazione* nell'interfaccia dell'applicazione. Solo un'attività di aggiornamento locale, *Aggiornamento di database e moduli dell'applicazione*, è disponibile per l'utente. Se l'attività *Aggiornamento di database e moduli dell'applicazione* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.



Attività di aggiornamento locali

2. Si apre l'elenco delle attività; selezionare l'attività *Aggiornamento di database e moduli dell'applicazione* e fare clic su .

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Fare clic su **Modalità di esecuzione**.

4. Nella finestra visualizzata, selezionare la modalità di esecuzione dell'attività di aggiornamento:

   - Se si desidera che Kaspersky Endpoint Security esegua l'attività di aggiornamento indipendentemente dal fatto che un pacchetto di aggiornamento sia disponibile o meno nella sorgente degli aggiornamenti, selezionare **Automaticamente**. La frequenza dei controlli da parte di Kaspersky Endpoint Security dei pacchetti di aggiornamento aumenta durante gli attacchi di virus e si riduce in assenza di attacchi.

   - Se si desidera avviare manualmente un'attività di aggiornamento, selezionare **Manualmente**.

   - Se si desidera configurare una pianificazione per l'esecuzione dell'attività di aggiornamento, selezionare le altre opzioni. Configurare le impostazioni avanzate per avviare l'attività di aggiornamento:

     - Nel campo **Rimanda l'esecuzione dopo l'avvio dell'applicazione di N minuti**, immettere l'intervallo di tempo per cui rimandare l'inizio dell'attività di aggiornamento dopo l'avvio di Kaspersky Endpoint Security.

     - Selezionare **Esegui la scansione pianificata il giorno successivo se il computer è spento** se si desidera che Kaspersky Endpoint Security esegua attività di aggiornamento ignorate alla prima occasione. Quando l'applicazione ha l'opportunità di eseguire le attività non effettuate, esegue le attività in modo casuale entro un determinato intervallo di tempo per distribuire il carico sul computer.

5. Salvare le modifiche.

Aggiunta di una sorgente degli aggiornamenti

Una *sorgente degli aggiornamenti* è una risorsa che contiene gli aggiornamenti per i database e i moduli dell'applicazione di Kaspersky Endpoint Security.

Le sorgenti degli aggiornamenti includono il server Kaspersky Security Center, i server degli aggiornamenti Kaspersky e cartelle di rete o locali.

Se i server di aggiornamento Kaspersky non sono disponibili, Kaspersky Endpoint Security può utilizzare domini alternativi per aggiornare i database e i moduli del software applicativo. Per informazioni dettagliate, consultare la Knowledge Base dell'Assistenza tecnica.

L'elenco predefinito di sorgenti degli aggiornamenti include Kaspersky Security Center e i server degli aggiornamenti Kaspersky. È possibile aggiungere all'elenco altre sorgenti degli aggiornamenti. È possibile specificare server HTTP/FTP e cartelle condivise come sorgenti degli aggiornamenti.

Kaspersky Endpoint Security non supporta gli aggiornamenti dai server HTTPS, a meno che non si tratti dei server degli aggiornamenti Kaspersky.

Se sono state selezionate più risorse come sorgenti degli aggiornamenti, Kaspersky Endpoint Security tenta di connettersi a esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco e recupera gli aggiornamenti dalla prima disponibile.

Per impostazione predefinita, Kaspersky Endpoint Security utilizza il server Kaspersky Security Center come prima sorgente di aggiornamenti. Questo aiuta a conservare il traffico durante l'aggiornamento. Se un criterio non viene applicato al computer, i server Kaspersky vengono selezionati come prima sorgente degli aggiornamenti nelle impostazioni dell'attività locale *Aggiornamento di database e moduli dell'applicazione* perché l'applicazione potrebbe non avere accesso al server Kaspersky Security Center.

Se l'applicazione è in esecuzione in modalità Light Agent, una cartella nella SVM è selezionata come sorgente degli aggiornamenti.

Come aggiungere una sorgente degli aggiornamenti in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

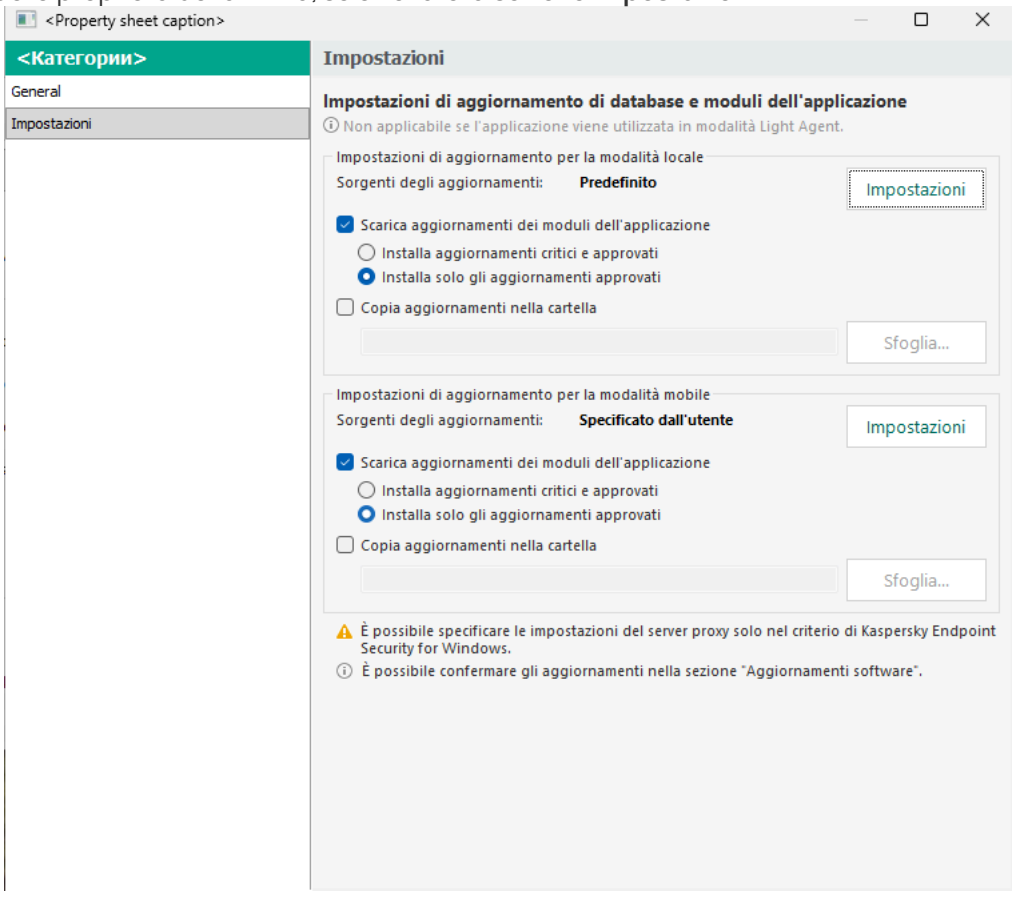
   Nella struttura della console, selezionare **Attività**.

2. Fare clic sull'attività **Aggiornamento di database e moduli dell'applicazione** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

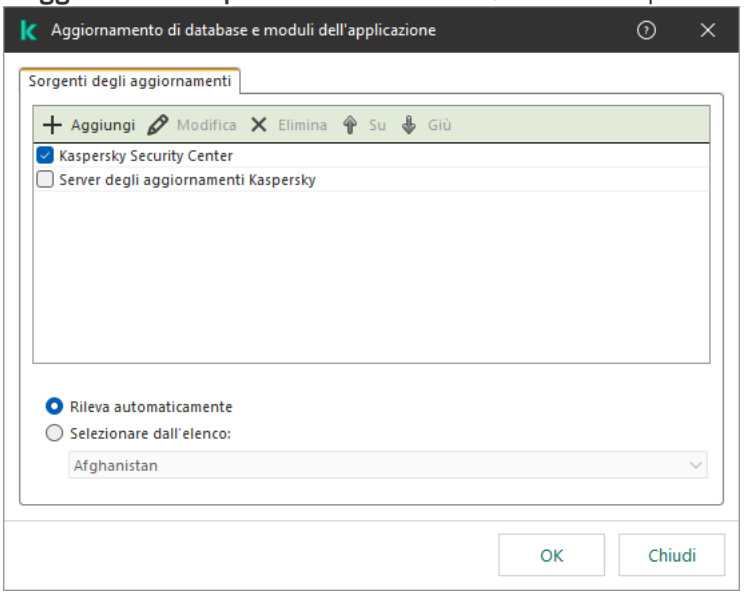
   L'attività *Aggiornamento di database e moduli dell'applicazione* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento di database e moduli dell'applicazione*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

3. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.



Impostazioni attività di Aggiornamento di database e moduli dell'applicazione

4. Nel blocco **Impostazioni di aggiornamento per la modalità locale**, fare clic sul pulsante **Impostazioni**.



Sorgenti dell'aggiornamento

5. Nell'elenco delle sorgenti degli aggiornamenti fare clic sul pulsante **Aggiungi**.

6. Nel campo **Sorgenti degli aggiornamenti** specificare l'indirizzo del server FTP o HTTP, la cartella di rete o la cartella locale che contiene il pacchetto di aggiornamento.

   Il formato dei percorsi per la sorgente degli aggiornamenti è il seguente:

   - Per un server FTP o HTTP, immettere l'indirizzo Web o l'indirizzo IP.

     Ad esempio, `http://dnl-01.geo.kaspersky.com/` o `93.191.13.103`.

     Per un server FTP è possibile specificare le impostazioni di autenticazione nell'indirizzo, nel seguente formato: `ftp://<user name>:<password>@<node>:<port>`.

   - Per una cartella di rete, immettere il percorso UNC.

     Ad esempio, `\\Server\Share\Update distribution`.

   - Per una cartella locale, immettere il percorso completo della cartella.

     Ad esempio, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   È possibile escludere la sorgente degli aggiornamenti senza rimuoverla nell'elenco delle sorgenti degli aggiornamenti. A tale scopo, deselezionare la casella di controllo accanto all'oggetto.

7. Fare clic su **OK**.

8. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

   Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.

9. Se necessario, aggiungere una sorgente degli aggiornamenti per la modalità mobile. La *modalità mobile* è la modalità di esecuzione di Kaspersky Endpoint Security quando un computer esce dal perimetro di rete dell'organizzazione (*computer offline*).

10. Salvare le modifiche.

Come aggiungere una sorgente degli aggiornamenti in Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

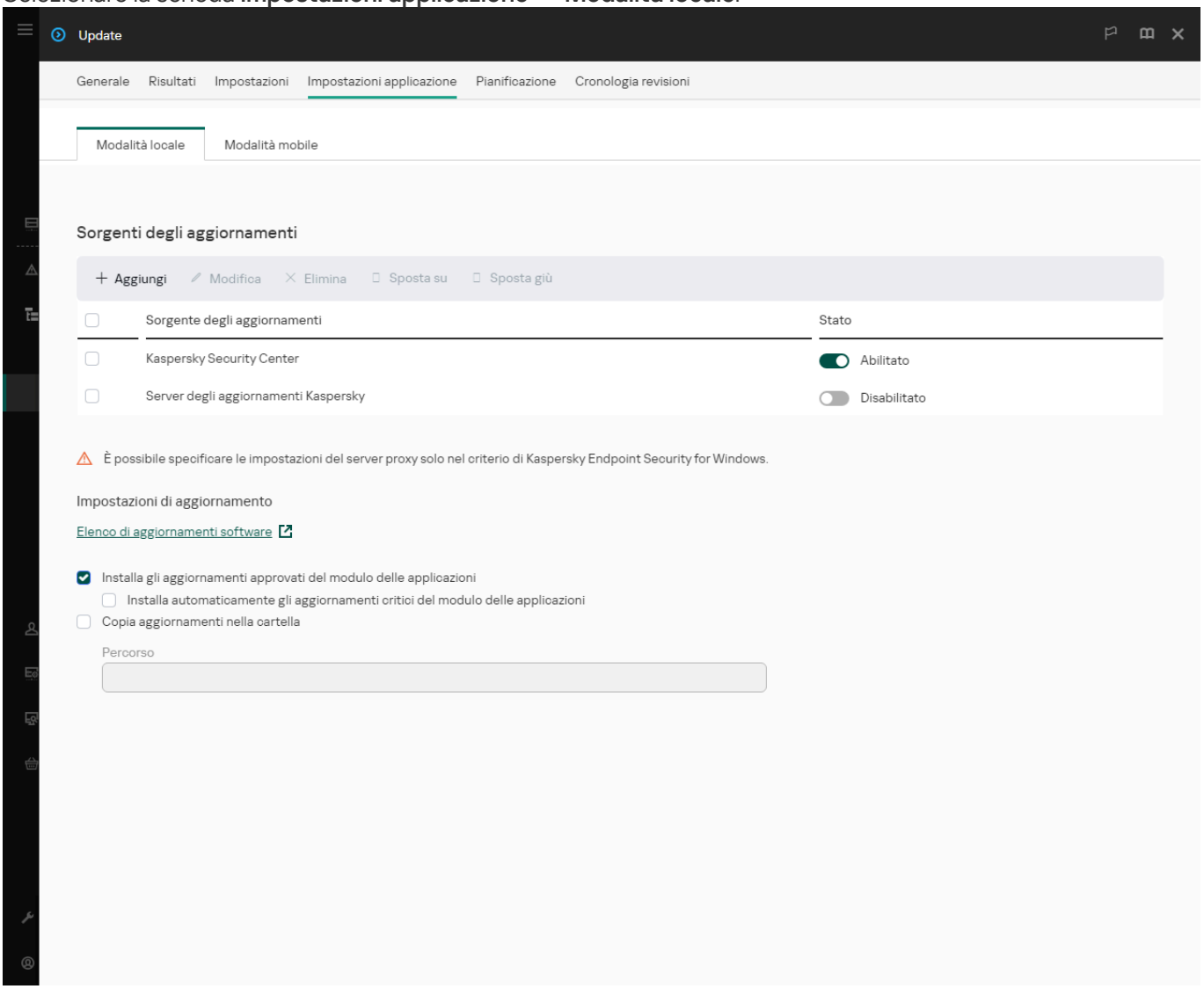
   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Aggiornamento** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   L'attività *Aggiornamento* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

3. Selezionare la scheda **Impostazioni applicazione** → **Modalità locale**.



Sorgenti dell'aggiornamento

4. Nell'elenco delle sorgenti degli aggiornamenti fare clic sul pulsante **Aggiungi**.

5. Nella finestra visualizzata, specificare l'indirizzo del server FTP o HTTP, la cartella di rete o la cartella locale che contiene il pacchetto di aggiornamento.

   Il formato dei percorsi per la sorgente degli aggiornamenti è il seguente:

   - Per un server FTP o HTTP, immettere l'indirizzo Web o l'indirizzo IP.

     Ad esempio, `http://dnl-01.geo.kaspersky.com/` o `93.191.13.103`.

Per un server FTP è possibile specificare le impostazioni di autenticazione nell'indirizzo, nel seguente formato: `ftp://<user name>:<password>@<node>:<port>`.

- Per una cartella di rete, immettere il percorso UNC.

  Ad esempio, `\\Server\Share\Update distribution`.

- Per una cartella locale, immettere il percorso completo della cartella.

  Ad esempio, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

È possibile escludere la sorgente degli aggiornamenti senza rimuoverla nell'elenco delle sorgenti degli aggiornamenti. A tale scopo, impostare l'interruttore accanto ad esso in posizione disattivato.

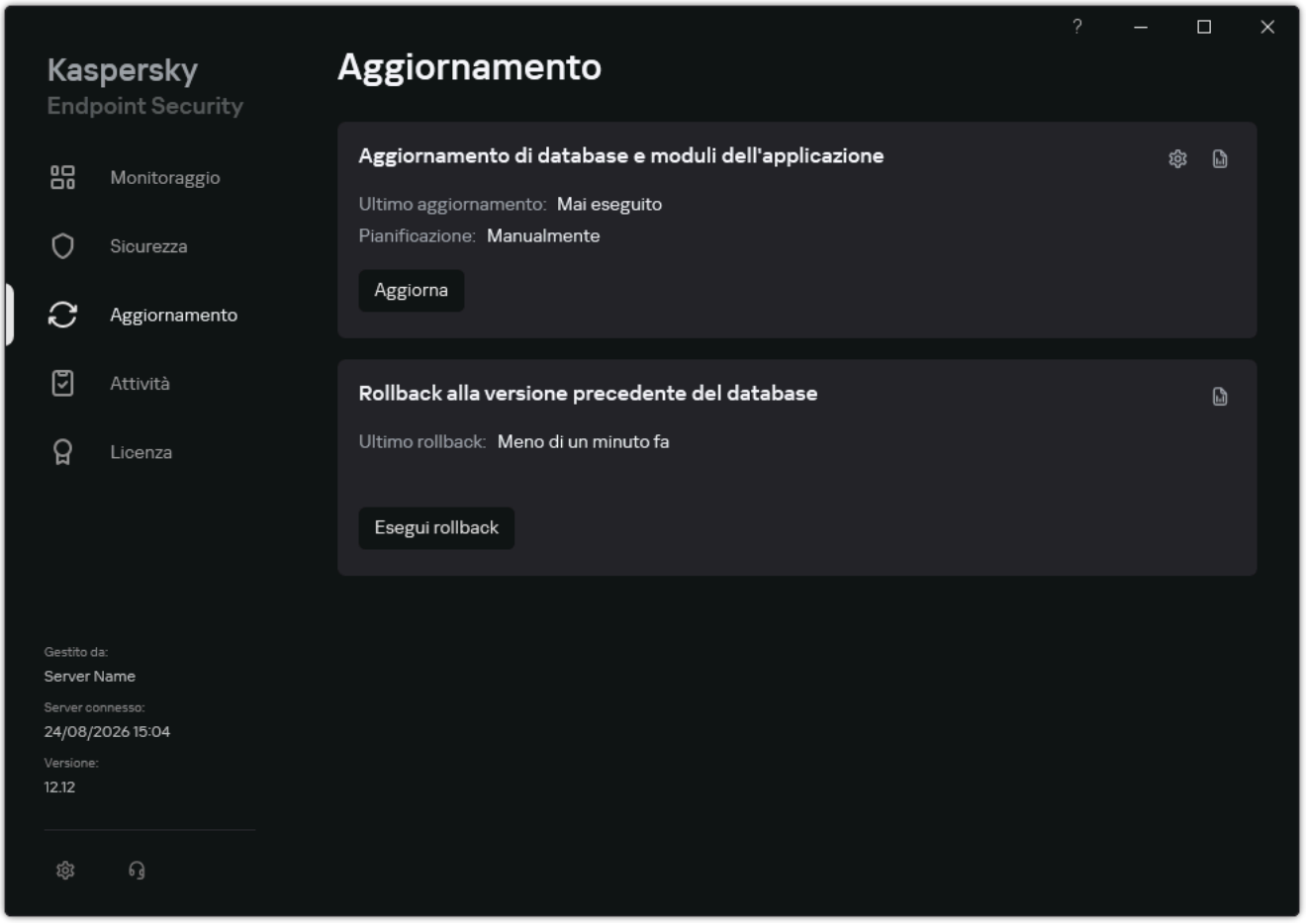
6. Fare clic su **OK**.
7. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Sposta su** e **Sposta giù**.

   Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.
8. Se necessario, aggiungere una sorgente degli aggiornamenti per la modalità mobile. La *modalità mobile* è la modalità di esecuzione di Kaspersky Endpoint Security quando un computer esce dal perimetro di rete dell'organizzazione (*computer offline*).
9. Salvare le modifiche.

Come aggiungere una sorgente degli aggiornamenti nell'interfaccia dell'applicazione

Non è possibile configurare l'attività di gruppo *Aggiornamento di database e moduli dell'applicazione* nell'interfaccia dell'applicazione. Solo un'attività di aggiornamento locale, *Aggiornamento di database e moduli dell'applicazione*, è disponibile per l'utente. Se l'attività *Aggiornamento di database e moduli dell'applicazione* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.



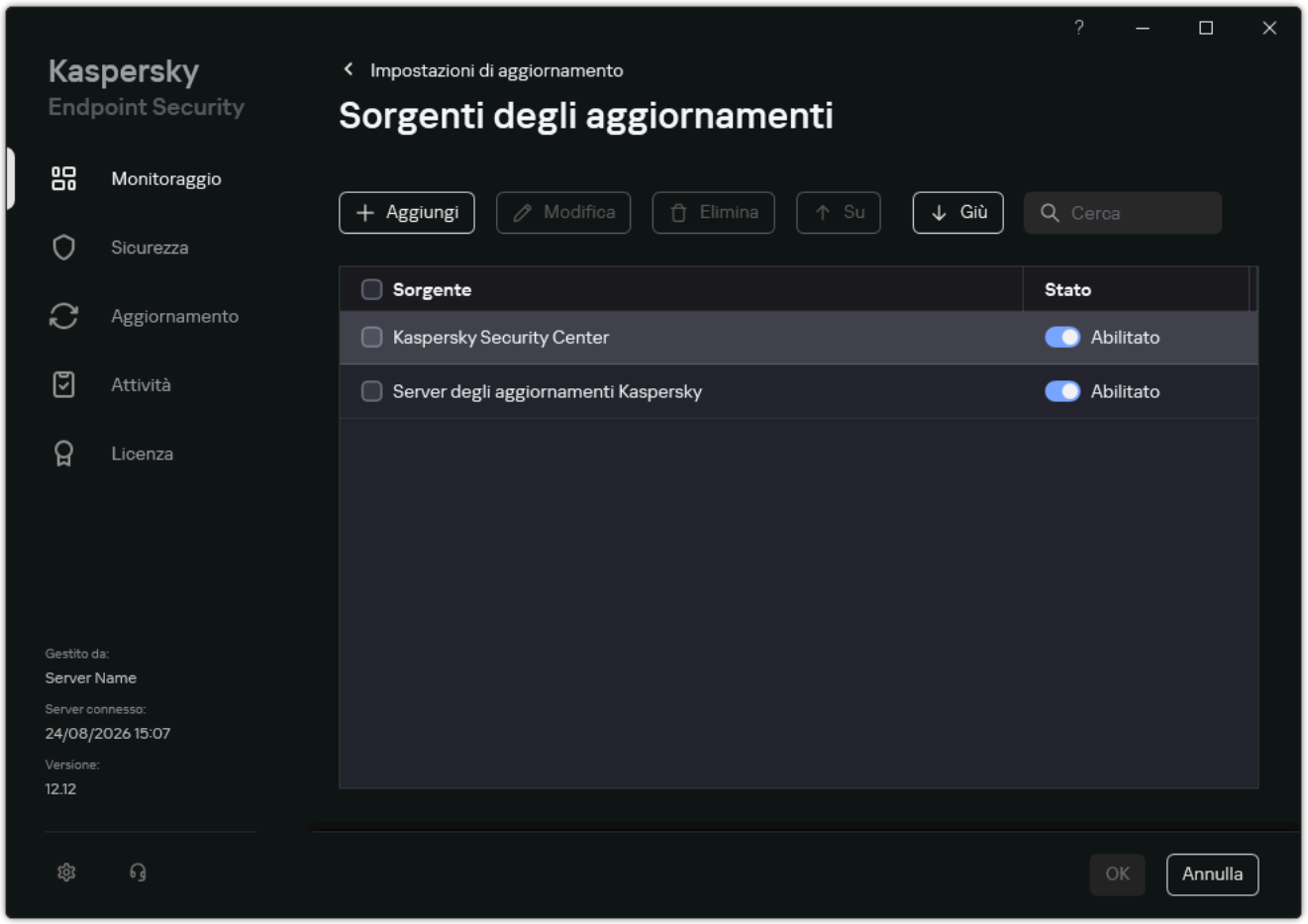
Attività di aggiornamento locali

2. Si apre l'elenco delle attività; selezionare l'attività *Aggiornamento di database e moduli dell'applicazione* e fare clic su ⚙.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Fare clic su **Seleziona sorgenti degli aggiornamenti**.

4. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.



Sorgenti dell'aggiornamento

5. Nella finestra visualizzata, specificare l'indirizzo del server FTP o HTTP, la cartella di rete o la cartella locale che contiene il pacchetto di aggiornamento.

   Il formato dei percorsi per la sorgente degli aggiornamenti è il seguente:

   - Per un server FTP o HTTP, immettere l'indirizzo Web o l'indirizzo IP.

     Ad esempio, `http://dnl-01.geo.kaspersky.com/` o `93.191.13.103`.

     Per un server FTP è possibile specificare le impostazioni di autenticazione nell'indirizzo, nel seguente formato: `ftp://<user name>:<password>@<node>:<port>`.

   - Per una cartella di rete, immettere il percorso UNC.

     Ad esempio, `\\Server\Share\Update distribution`.

   - Per una cartella locale, immettere il percorso completo della cartella.

     Ad esempio, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Fare clic su **Seleziona**.

7. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

8. Salvare le modifiche.

Aggiornamento dei moduli dell'applicazione

Gli aggiornamenti dei moduli delle applicazioni correggono errori, migliorano le prestazioni e aggiungono nuove funzionalità. Quando un nuovo aggiornamento dei moduli dell'applicazione diventa disponibile, è necessario confermare l'installazione dell'aggiornamento. È possibile confermare l'installazione di un aggiornamento dei moduli dell'applicazione nell'interfaccia dell'applicazione o in Kaspersky Security Center. Ogni volta che è disponibile un aggiornamento, l'applicazione mostra una notifica nella finestra principale di Kaspersky Endpoint Security: . Se gli aggiornamenti dei moduli dell'applicazione richiedono la lettura e l'accettazione delle condizioni del Contratto di licenza con l'utente finale, l'applicazione li installa una volta che il Contratto di licenza con l'utente finale è stato accettato.

Dopo l'installazione di un aggiornamento dell'applicazione, potrebbe essere necessario riavviare il computer.

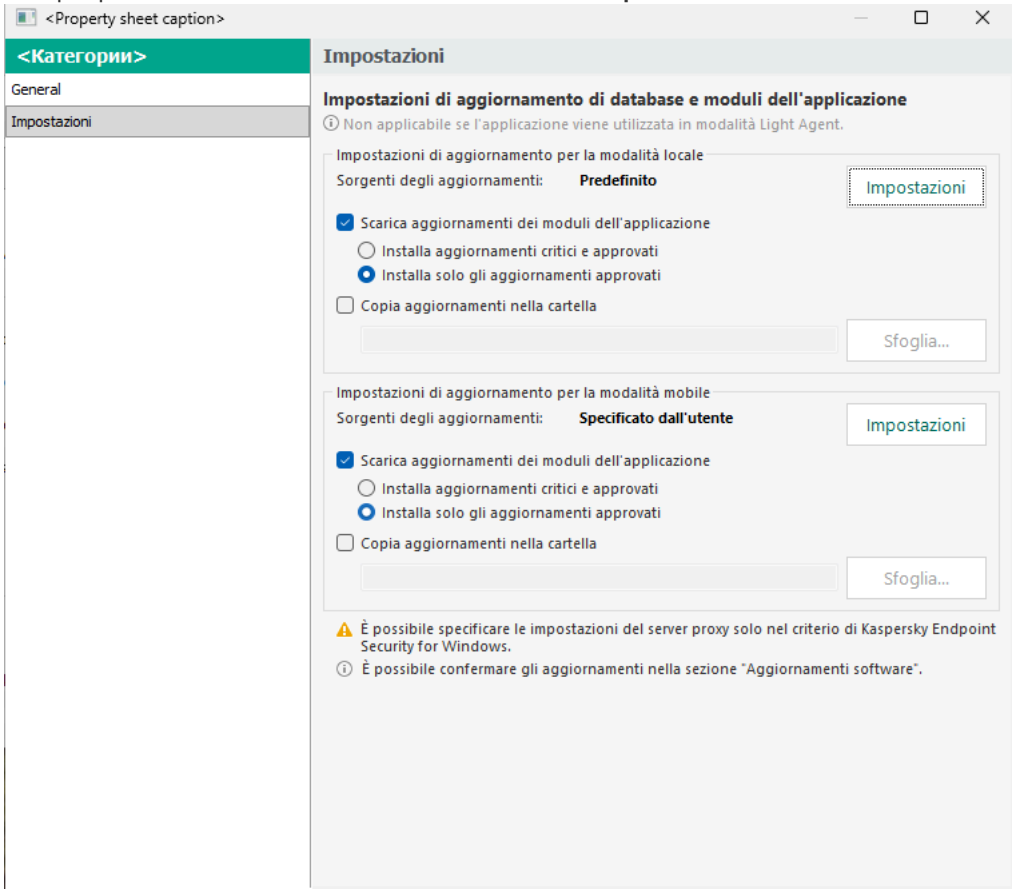
Come configurare il modulo dell'applicazione in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Attività**.
3. Fare clic sull'attività **Aggiornamento di database e moduli dell'applicazione** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   L'attività *Aggiornamento di database e moduli dell'applicazione* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento di database e moduli dell'applicazione*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

4. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.



Impostazioni attività di Aggiornamento di database e moduli dell'applicazione

5. Nella sezione **Impostazioni di aggiornamento per la modalità locale** selezionare la casella di controllo **Scarica aggiornamenti dei moduli dell'applicazione**.

   Se si desidera impedire il download degli aggiornamenti dei moduli dell'applicazione, deselezionare la casella di controllo **Scarica aggiornamenti dei moduli dell'applicazione** e vietare l'utilizzo delle attività locali da parte dell'utente.

6. Selezionare gli aggiornamenti dei moduli dell'applicazione da installare.

   - **Installa aggiornamenti critici e approvati**. Se questa opzione è selezionata, quando sono disponibili aggiornamenti dei moduli dell'applicazione, Kaspersky Endpoint Security installa automaticamente gli aggiornamenti critici e tutti gli altri aggiornamenti dei moduli dell'applicazione solo una volta che la relativa installazione viene approvata in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center.

   - **Installa solo gli aggiornamenti approvati**. Se questa opzione è selezionata, quando sono disponibili aggiornamenti dei moduli dell'applicazione, Kaspersky Endpoint Security li installa solo una volta che la relativa installazione viene approvata in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center. Questa opzione è selezionata per impostazione predefinita.

7. Se necessario, configurare gli aggiornamenti dei moduli dell'applicazione per la modalità mobile. La *modalità mobile* è la modalità di esecuzione di Kaspersky Endpoint Security quando un computer esce dal perimetro di rete dell'organizzazione (*computer offline*).

8. Salvare le modifiche.

Come configurare il modulo dell'applicazione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

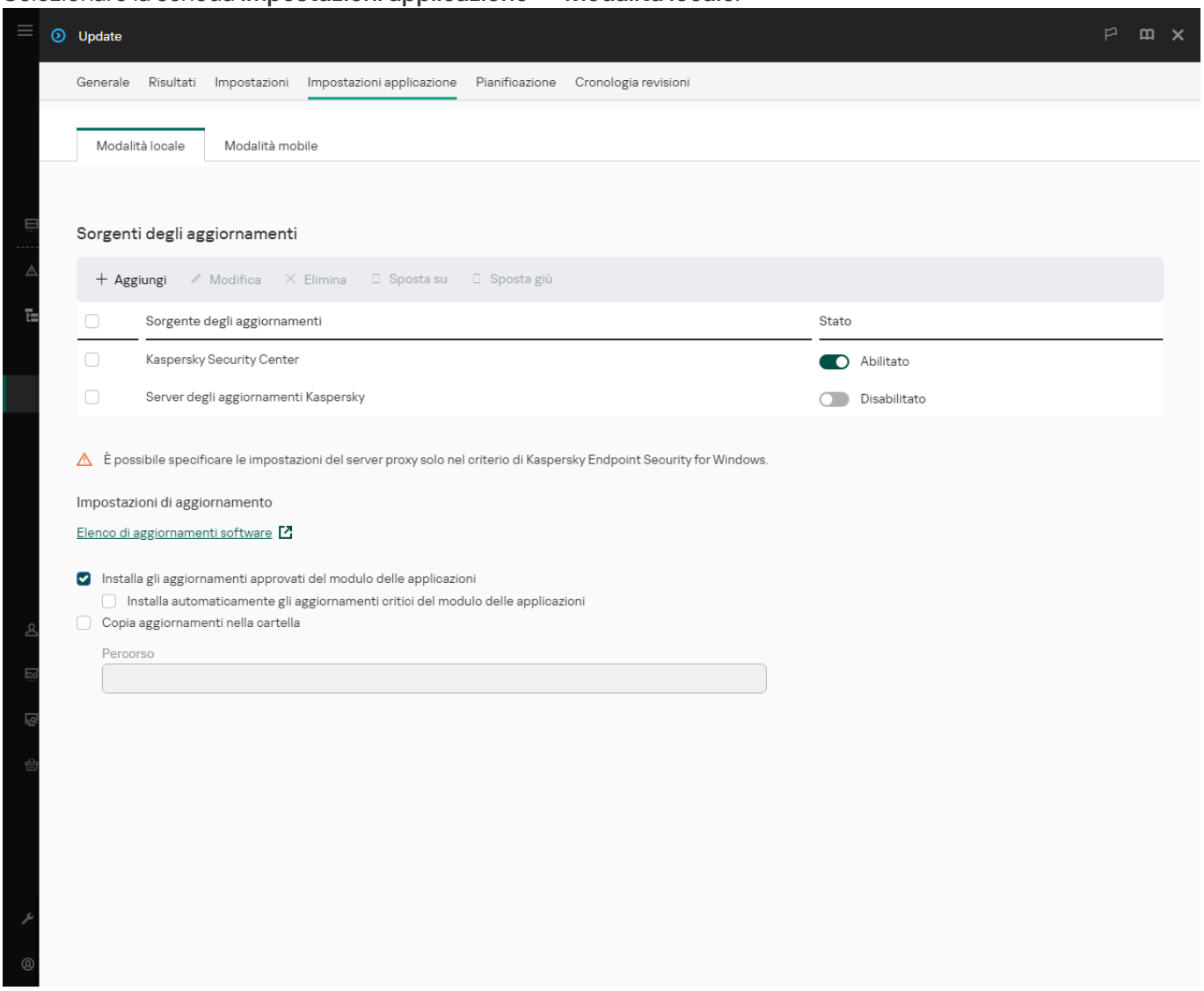
   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Aggiornamento di database e moduli dell'applicazione** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   L'attività *Aggiornamento di database e moduli dell'applicazione* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Per creare l'attività *Aggiornamento di database e moduli dell'applicazione*, installare il plug-in di gestione di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

3. Selezionare la scheda **Impostazioni applicazione** → **Modalità locale**.



Impostazioni attività di Aggiornamento

4. In **Aggiorna impostazioni**, selezionare gli aggiornamenti dei moduli dell'applicazione da installare:

   - **Installa aggiornamenti dei moduli applicativi approvati**. Se questa opzione è selezionata, quando sono disponibili aggiornamenti dei moduli dell'applicazione, Kaspersky Endpoint Security li installa solo una volta che la relativa installazione viene approvata in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center. Questa opzione è selezionata per impostazione predefinita.

   - **Installa automaticamente gli aggiornamenti critici dei moduli applicativi**. Se questa opzione è selezionata, quando sono disponibili aggiornamenti dei moduli dell'applicazione, Kaspersky Endpoint Security installa automaticamente gli aggiornamenti critici e tutti gli altri aggiornamenti dei moduli dell'applicazione solo una volta che la relativa installazione viene approvata in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center.

   Se si desidera impedire il download degli aggiornamenti dei moduli dell'applicazione, deselezionare le caselle di controllo **Installa aggiornamenti dei moduli applicativi approvati** e **Installa automaticamente gli aggiornamenti critici dei moduli applicativi** e vietare l'utilizzo delle attività locali da parte dell'utente.

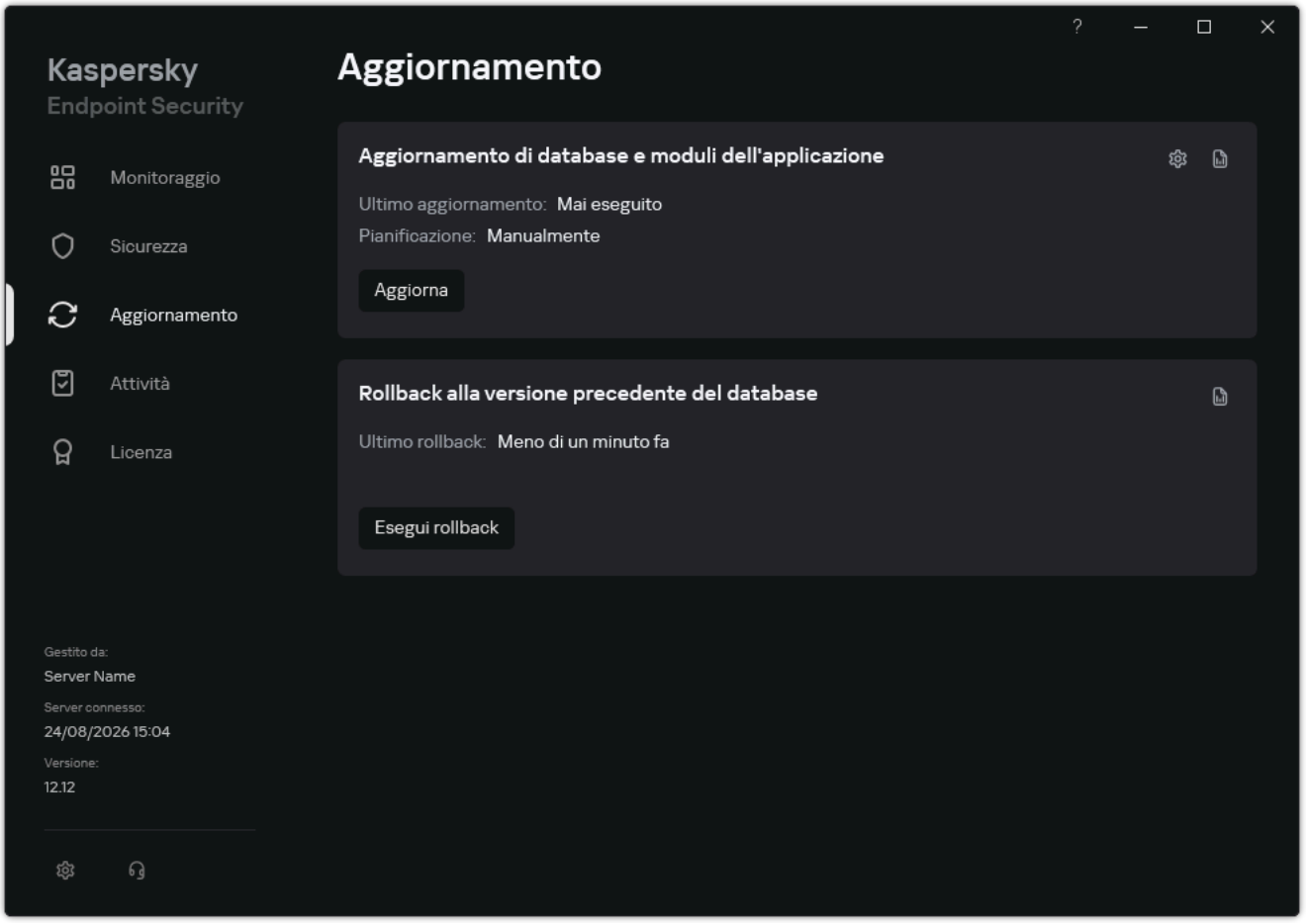
5. Se necessario, configurare gli aggiornamenti dei moduli dell'applicazione per la modalità mobile. La *modalità mobile* è la modalità di esecuzione di Kaspersky Endpoint Security quando un computer esce dal perimetro di rete dell'organizzazione (*computer offline*).

6. Salvare le modifiche.

Come configurare il modulo dell'applicazione nell'interfaccia dell'applicazione

Non è possibile configurare l'attività di gruppo *Aggiornamento di database e moduli dell'applicazione* nell'interfaccia dell'applicazione. Solo un'attività di aggiornamento locale, *Aggiornamento di database e moduli dell'applicazione*, è disponibile per l'utente. Se l'attività *Aggiornamento di database e moduli dell'applicazione* non viene visualizzata, significa che l'amministratore ha vietato l'uso delle attività locali nel criterio.

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.



Attività di aggiornamento locali

2. Si apre l'elenco delle attività; selezionare l'attività *Aggiornamento di database e moduli dell'applicazione* e fare clic su ⚙.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Nella sezione **Download e installazione degli aggiornamenti dei moduli dell'applicazione** selezionare la casella di controllo **Scarica aggiornamenti dei moduli dell'applicazione**.

4. Selezionare gli aggiornamenti dei moduli dell'applicazione da installare.

   - **Installa aggiornamenti critici e approvati**. Se questa opzione è selezionata, quando sono disponibili aggiornamenti dei moduli dell'applicazione, Kaspersky Endpoint Security installa automaticamente gli aggiornamenti critici e tutti gli altri aggiornamenti dei moduli dell'applicazione solo una volta che la relativa installazione viene approvata in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center.

   - **Installa solo gli aggiornamenti approvati**. Se questa opzione è selezionata, quando sono disponibili aggiornamenti dei moduli dell'applicazione, Kaspersky Endpoint Security li installa solo una volta che la relativa installazione viene approvata in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center. Questa opzione è selezionata per impostazione predefinita.

5. Salvare le modifiche.

Utilizzo di un server proxy per gli aggiornamenti

Può essere necessario specificare le impostazioni del server proxy per scaricare gli aggiornamenti dei database e dei moduli dell'applicazione dalla sorgente degli aggiornamenti. Se sono presenti più sorgenti degli aggiornamenti, le impostazioni del server proxy vengono applicate per tutte le sorgenti. Se un server proxy non è necessario per alcune sorgenti degli aggiornamenti, è possibile disabilitare l'utilizzo di un server proxy nelle proprietà del criterio. Kaspersky Endpoint Security utilizzerà inoltre un server proxy per accedere a Kaspersky Security Network e ai server di attivazione.

Per configurare una connessione alle sorgenti degli aggiornamenti tramite un server proxy:

1. Nella finestra principale di Web Console, fare clic su ⚙.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Passare alla sezione **Configurazione dell'accesso a Internet**.

3. Selezionare la casella di controllo **Usa server proxy**.

4. Configurare le impostazioni di connessione del server proxy: indirizzo del server proxy, porta e impostazioni di autenticazione del server proxy (nome utente e password).

5. Salvare le modifiche.

Per disabilitare l'utilizzo di un server proxy per un gruppo di amministrazione specifico:

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Impostazioni di rete**.

5. Nel blocco **Server proxy**, fare clic sul pulsante **Impostazioni**.

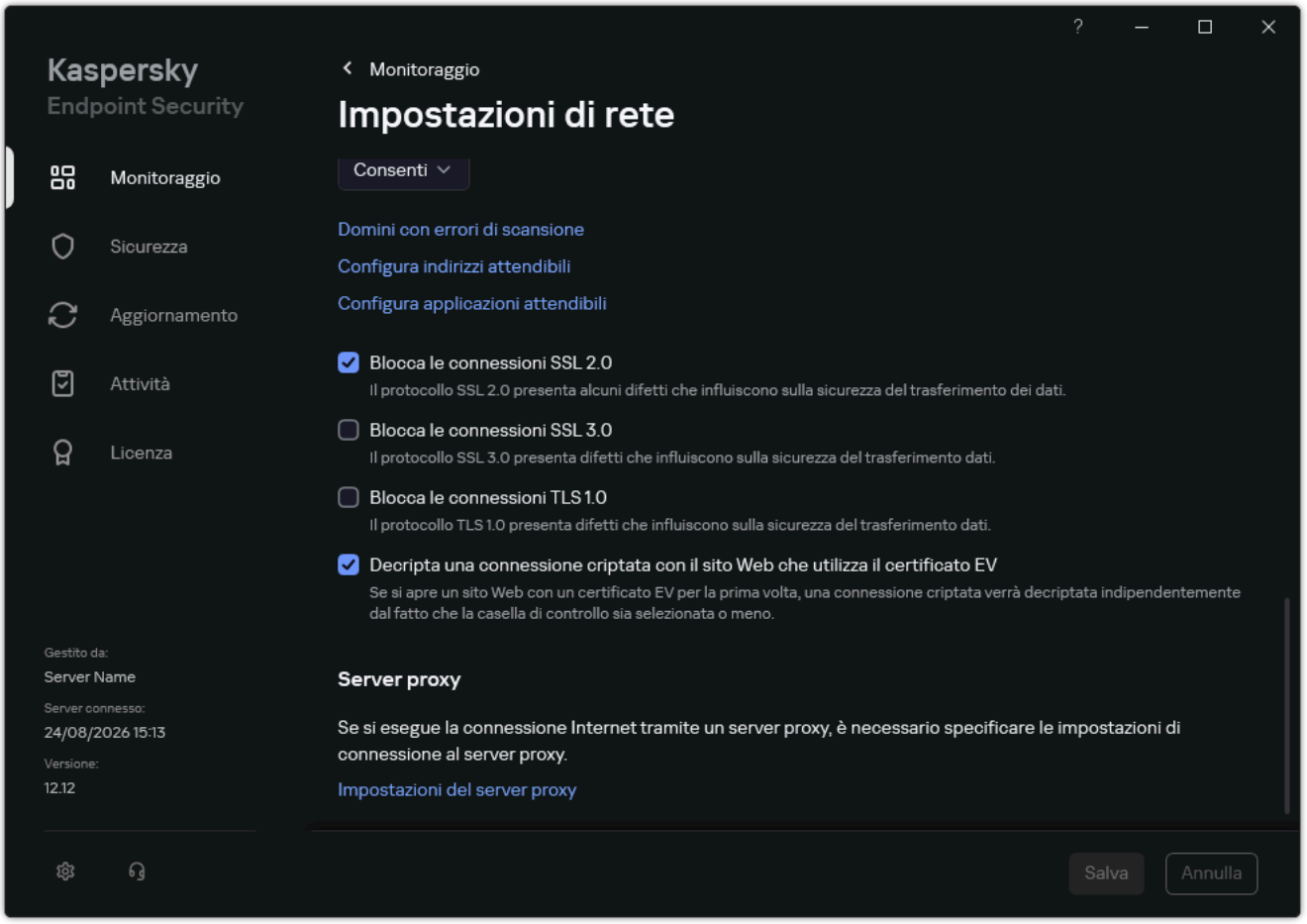
6. Nella finestra visualizzata, selezionare la casella di controllo **Ignora un server proxy per gli indirizzi locali**.

7. Salvare le modifiche.

Per configurare le impostazioni del server proxy nell'interfaccia dell'applicazione:

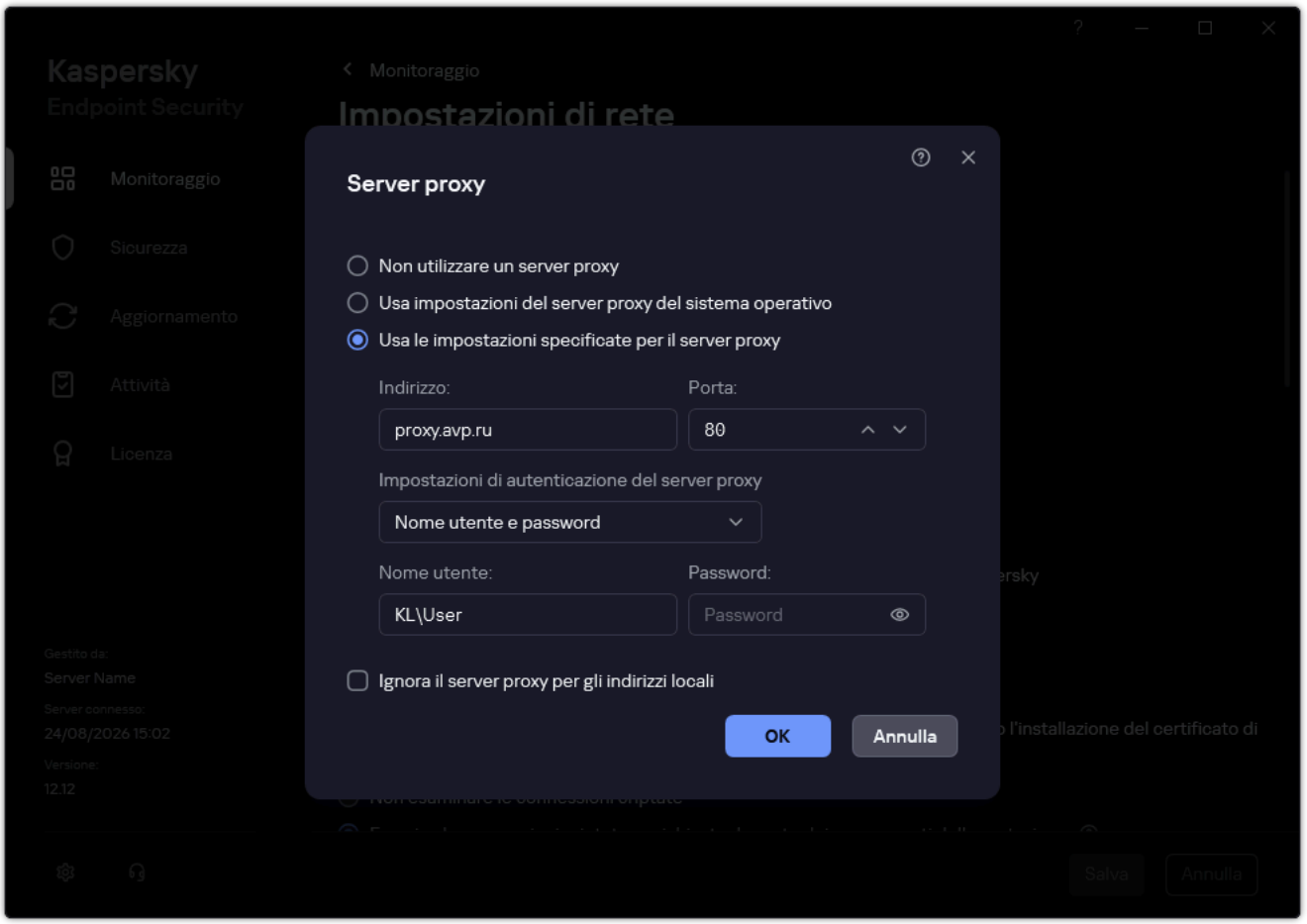
1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.



Impostazioni della rete delle applicazioni

3. Nella sezione **Server proxy**, fare clic sul collegamento **Impostazioni del server proxy**.



Impostazioni della connessione al server proxy

4. Nella finestra visualizzata, selezionare una delle seguenti opzioni per determinare l'indirizzo del server proxy:

   - **Usa impostazioni del server proxy del sistema operativo**.

     Questa opzione è selezionata per impostazione predefinita. Kaspersky Endpoint Security utilizza le impostazioni del server proxy definite nelle impostazioni del sistema operativo.

   - **Usa le impostazioni specificate per il server proxy**.

     Se è stata selezionata questa opzione, configurare le impostazioni per la connessione al server proxy: indirizzo e porta del server proxy.

5. Selezionare la modalità di autenticazione dell'applicazione nel server proxy. Per impostazione predefinita, l'applicazione utilizza l'autenticazione NTLM del dominio dell'utente corrente.

6. Se si desidera disabilitare l'utilizzo del server proxy durante l'aggiornamento dei database e dei moduli dell'applicazione da una cartella condivisa, selezionare la casella di controllo **Ignora il server proxy per gli indirizzi locali**.

7. Salvare le modifiche.

Di conseguenza, Kaspersky Endpoint Security utilizzerà il server proxy per scaricare il modulo dell'applicazione e gli aggiornamenti dei database. Kaspersky Endpoint Security utilizzerà inoltre il server proxy per accedere ai server KSN e ai server di attivazione Kaspersky. Se l'autenticazione è richiesta nel server proxy ma le credenziali dell'account utente non sono state fornite o non sono corrette, Kaspersky Endpoint Security richiederà il nome utente e la password.

Ultimo rollback degli aggiornamenti

Al termine del secondo aggiornamento dei database e dei moduli dell'applicazione, diventa disponibile la funzione di rollback dei database e dei moduli dell'applicazione alle versioni precedenti.

A ogni avvio del processo di aggiornamento, Kaspersky Endpoint Security crea una copia di backup dei database correnti e dei moduli dell'applicazione. In questo modo è possibile eseguire il rollback dei database e dei moduli dell'applicazione alla versione precedente, quando necessario. Ripristinare la versione precedente dell'ultimo aggiornamento può essere utile, ad esempio, se una nuova versione del database causa un falso positivo che porta Kaspersky Endpoint Security a bloccare un'applicazione sicura.

Kaspersky Endpoint Security in modalità Light Agent non supporta l'attività *Rollback degli aggiornamenti*.

Come eseguire il rollback dell'ultimo aggiornamento in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

1. Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Rollback degli aggiornamenti**.

Passaggio 2. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 3. Configurazione di una pianificazione di avvio dell'attività

Ad esempio, configurare manualmente la pianificazione dell'attività.

Passaggio 4. Definizione del nome dell'attività

Immettere un nome per l'attività.

Passaggio 7. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come eseguire il rollback dell'ultimo aggiornamento in Console Web

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Rollback**.

   c. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Rollback degli aggiornamenti*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Selezione dell'account per eseguire l'attività. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.

6. Terminare la procedura guidata.

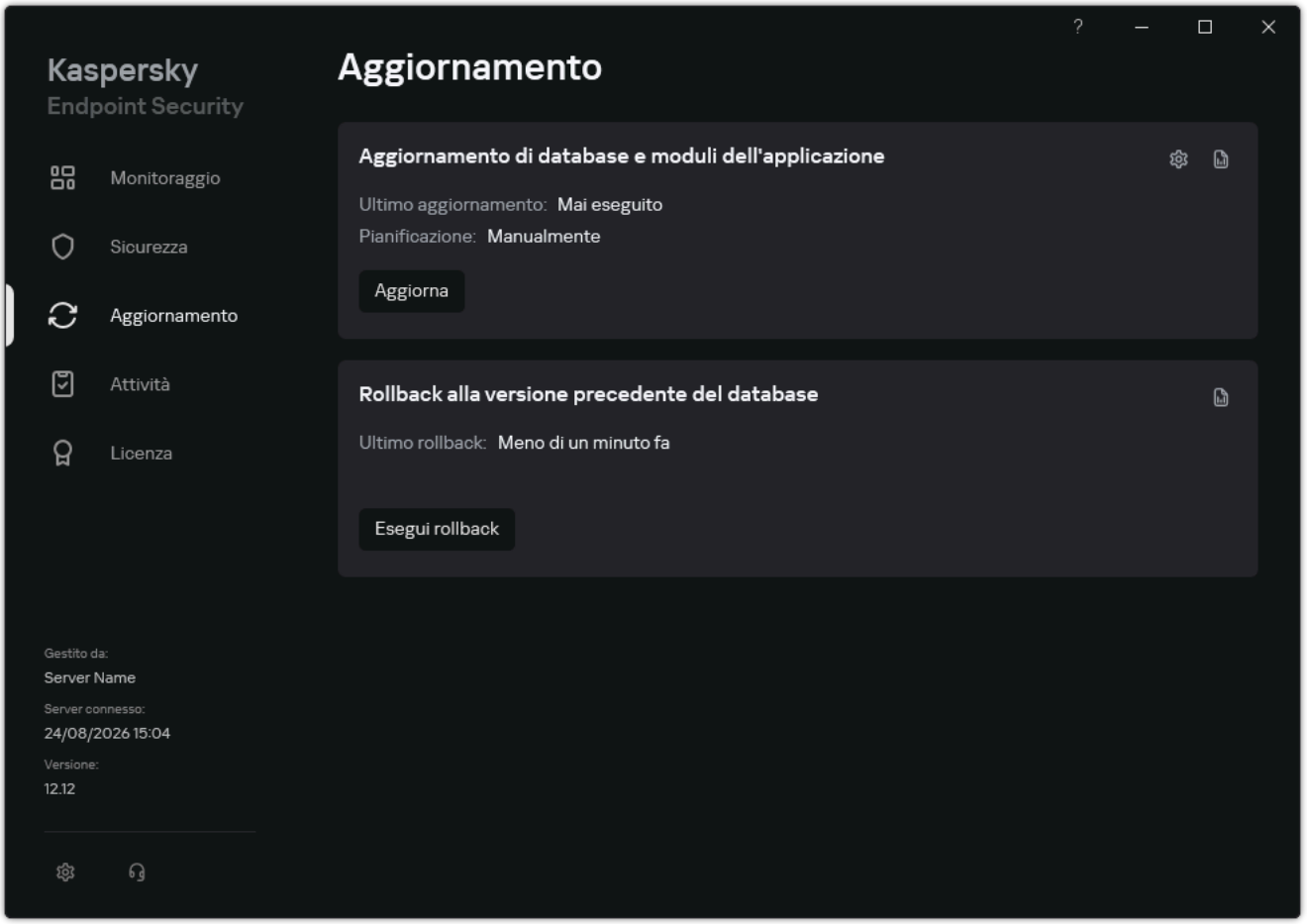
7. Verrà visualizzata una nuova attività nell'elenco delle attività.

8. Selezionare la casella di controllo accanto all'attività.

9. Fare clic su **Avvia**.

Come eseguire il rollback dell'ultimo aggiornamento nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiornamento**.



Attività di aggiornamento locali

2. Nel riquadro **Rollback alla versione precedente del database**, fare clic sul pulsante **Esegui rollback**.

Kaspersky Endpoint Security inizierà a eseguire il rollback dell'ultimo aggiornamento del database. L'applicazione visualizzerà lo stato di avanzamento del rollback, la dimensione dei file scaricati e l'origine degli aggiornamenti. È possibile interrompere l'attività in qualsiasi momento facendo clic sul pulsante **Interrompi aggiornamento**.

Tecnologia Disinfezione avanzata

Per contenere le minacce attive, Kaspersky Endpoint Security utilizza la tecnologia Disinfezione avanzata. Disinfezione avanzata funziona in modo diverso per le workstation e i server. È possibile configurare la disinfezione avanzata nelle impostazioni dell'attività *Scansione malware* e nelle impostazioni dell'applicazione.

Se Kaspersky Endpoint Security non riesce ad arrestare l'esecuzione di un malware, è possibile utilizzare la tecnologia Disinfezione avanzata. Per i computer a cui è applicato un criterio, la tecnologia Disinfezione avanzata è disabilitata per impostazione predefinita poiché utilizza una notevole quantità di risorse di elaborazione. Per i computer a cui non è applicato un criterio, Disinfezione avanzata è abilitata per impostazione predefinita.

Disinfezione avanzata funziona in modo diverso per le workstation e i server. Per utilizzare la tecnologia nei server, è necessario abilitare la Disinfezione avanzata immediata nelle proprietà dell'attività *Scansione malware*. Questo prerequisito non è necessario per utilizzare la tecnologia nelle workstation.

Come abilitare o disabilitare la tecnologia Disinfezione avanzata in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
4. Nel blocco **Generali**, selezionare o deselezionare la casella di controllo **Abilita la tecnologia Disinfezione avanzata** per abilitare o disabilitare la tecnologia Disinfezione avanzata.
5. Salvare le modifiche.

Come abilitare o disabilitare la tecnologia Disinfezione avanzata in Web Console e Cloud Console

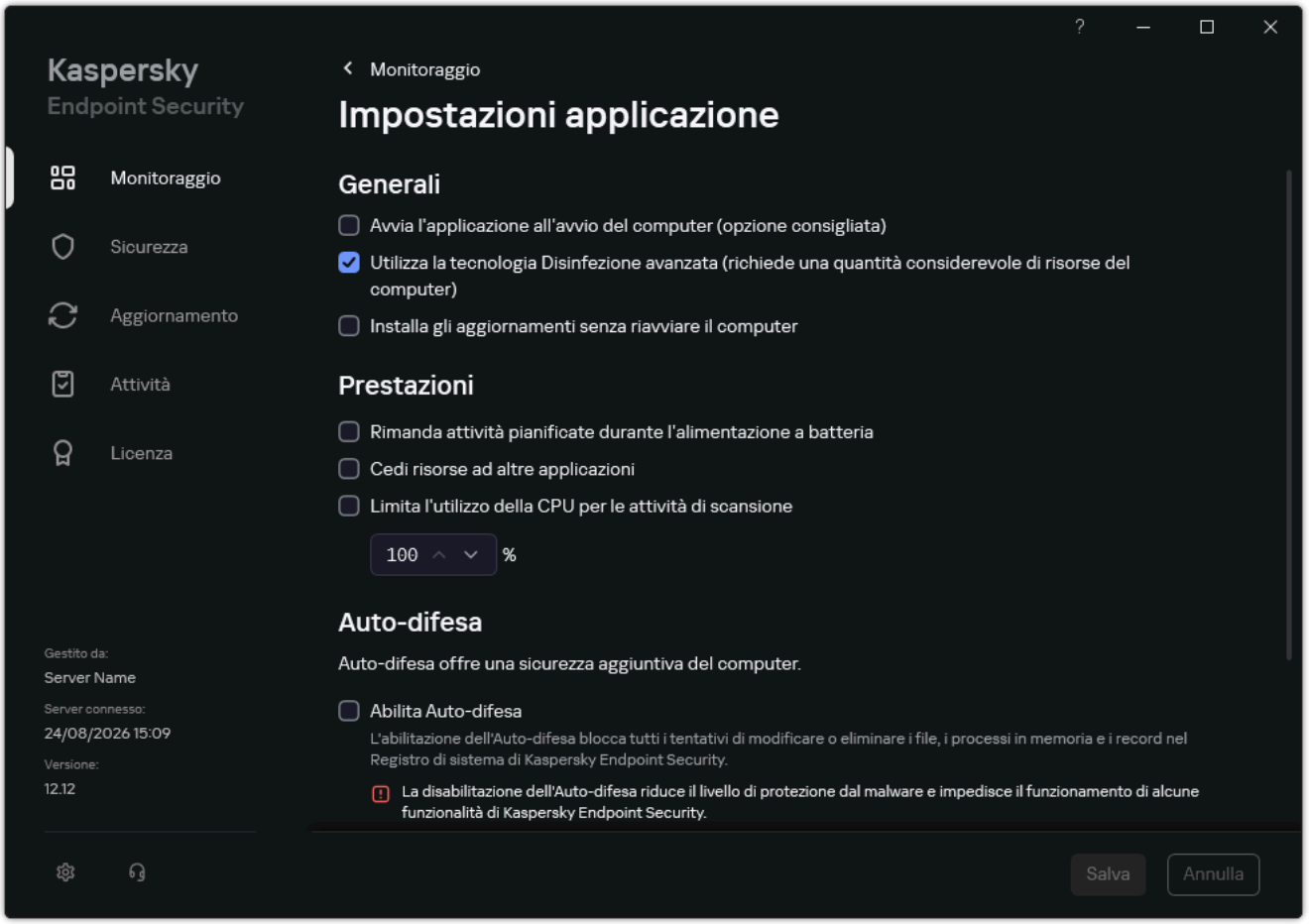
1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Selezionare **Impostazioni generali** → **Impostazioni di rilevamento**.
5. Nel blocco **Tecnologia Disinfezione avanzata**, attivare o disattivare l'interruttore **Tecnologia Disinfezione avanzata ABILITATA** per abilitare o disabilitare la tecnologia Disinfezione avanzata.
6. Salvare le modifiche.

Come abilitare o disabilitare la tecnologia Disinfezione avanzata nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.



Impostazioni di Kaspersky Endpoint Security for Windows

3. Nel blocco **Generali**, selezionare o deselezionare la casella di controllo **Utilizza la tecnologia Disinfezione avanzata (richiede una quantità considerevole di risorse del computer)** per abilitare o disabilitare la tecnologia Disinfezione avanzata.

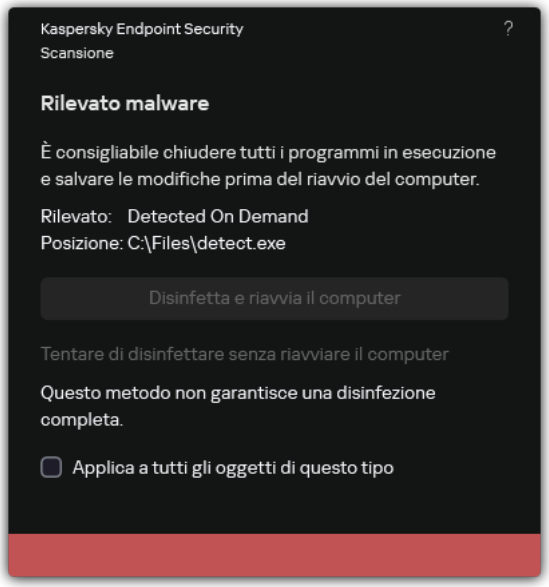
4. Salvare le modifiche.

Di conseguenza, l'utente non può utilizzare la maggior parte delle funzionalità del sistema operativo quando l'esecuzione di Disinfezione avanzata è in corso. Al termine della disinfezione, il computer verrà riavviato.

Disinfezione delle minacce attive nelle workstation

Per contenere le minacce attive nelle workstation, abilitare la tecnologia Disinfezione avanzata nelle impostazioni dell'applicazione. Successivamente, configurare l'esperienza utente nelle proprietà dell'attività *Scansione malware*. Nelle proprietà dell'attività è presente una casella di controllo **Esegui immediatamente Disinfezione avanzata**. Se il segno di spunta viene impostato, Kaspersky Endpoint Security eseguirà la disinfezione senza segnalarlo all'utente. Al termine della disinfezione, il computer verrà riavviato. Se il segno di spunta non viene impostato, Kaspersky Endpoint Security mostrerà una notifica sulle minacce attive (vedere la figura sotto). Non è possibile chiudere questa notifica senza elaborare il file.

La disinfezione avanzata durante un'attività di scansione virus in un computer viene eseguita solo se la funzionalità Disinfezione avanzata è abilitata nelle proprietà del criterio applicato al computer.



Notifica sulla minaccia attiva

Disinfezione delle minacce attive nei server

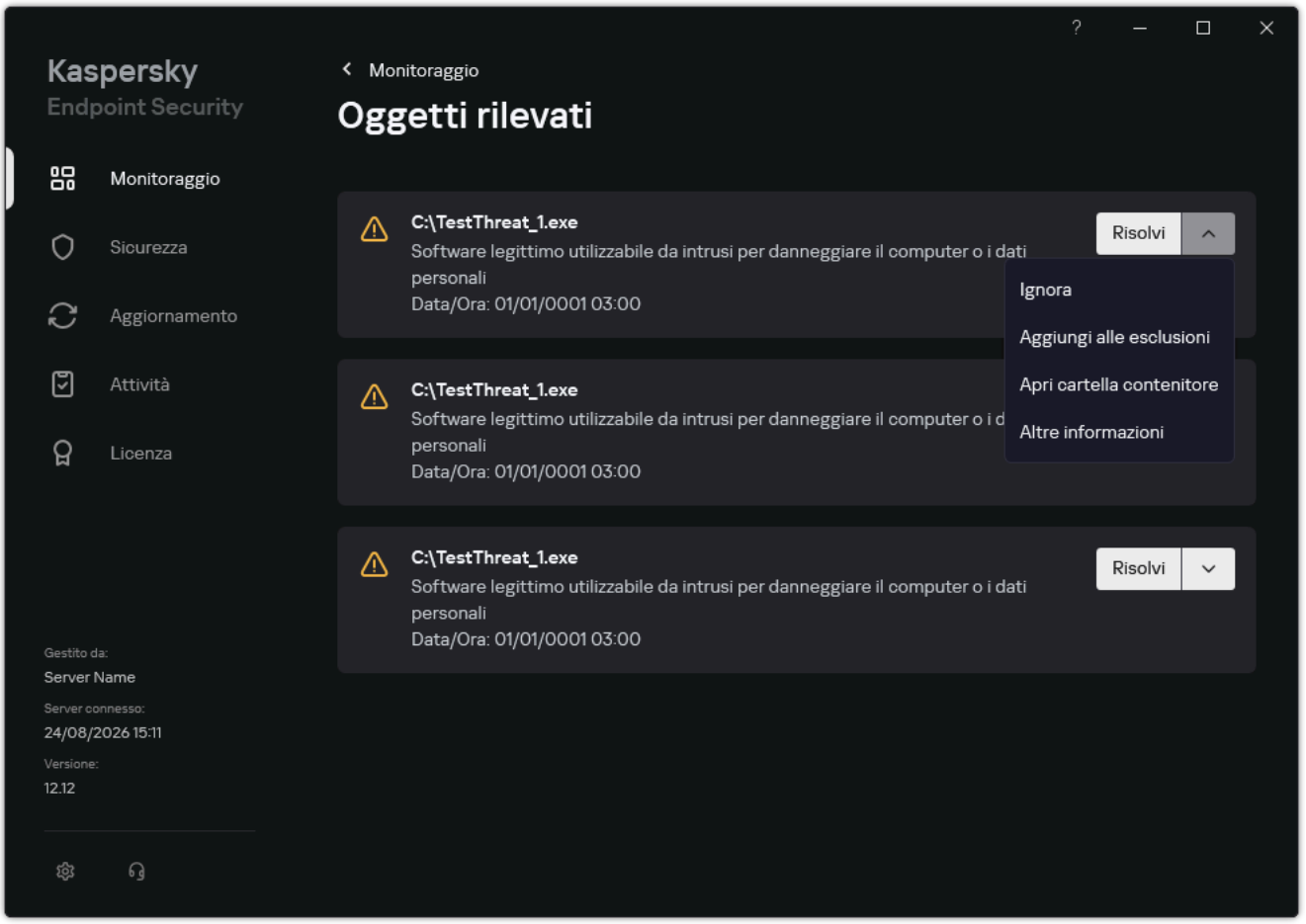
Per contenere le minacce attive nei server, è necessario procedere come segue:

- abilitare la tecnologia Disinfezione avanzata nelle impostazioni dell'applicazione;
- abilitare la Disinfezione avanzata immediata nelle proprietà dell'attività *Scansione malware*.

Se Kaspersky Endpoint Security è installato in un computer in cui viene eseguito Windows for Servers, Kaspersky Endpoint Security non mostra la notifica. Pertanto, l'utente non può selezionare un'azione per disinfettare una minaccia attiva. Per disinfettare una minaccia, è necessario abilitare la tecnologia Disinfezione avanzata nelle impostazioni dell'applicazione e abilitare immediatamente Disinfezione avanzata nelle impostazioni dell'attività *Scansione malware*. Quindi, è necessario avviare l'attività *Scansione malware*.

Eliminazione delle minacce non elaborate

Kaspersky Endpoint Security registra le informazioni sui file non elaborati. Queste informazioni vengono registrate sotto forma di eventi nell'elenco delle minacce attive (vedere la figura riportata di seguito).



Un elenco di minacce attive

Un file infetto viene considerato *elaborato* se Kaspersky Endpoint Security ha disinfettato il file o rimosso la minaccia come parte della scansione di virus e altro malware nel computer.

Kaspersky Endpoint Security sposta il file nell'elenco delle minacce attive se, per qualsiasi motivo, Kaspersky Endpoint Security non è in grado di eseguire un'azione sul file in base alle impostazioni dell'applicazione specificate durante la scansione del computer alla ricerca di virus e altre minacce.

Questa situazione è possibile nei seguenti casi:

- Il file da esaminare non è disponibile (ad esempio, è posizionato in un'unità di rete o in un'unità rimovibile senza privilegi di scrittura).
- Nelle impostazioni dell'attività *Scansione malware*, l'azione relativa al rilevamento delle minacce è impostata su **Informa**. Quindi, quando la notifica del file infetto è stata visualizzata sullo schermo, l'utente ha selezionato **Ignora**.

In caso di minacce non elaborate, Kaspersky Endpoint Security modifica l'icona in . Nella finestra principale dell'applicazione, viene visualizzata la notifica della minaccia (vedere la figura riportata di seguito). In Kaspersky Security Center Console, lo stato del computer viene modificato in *Critico* – .

Come elaborare una minaccia in Administration Console (MMC)

1. In Administration, Console passare alla cartella **Administration Server → Avanzate → Archivi → Minacce attive**.

   Verrà visualizzato l'elenco delle minacce attive.

2. Selezionare l'oggetto che si desidera elaborare.

3. Scegliere il modo in cui si desidera gestire la minaccia:

   - **Disinfetta**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato.

   - **Elimina**. Se questa opzione è selezionata, l'applicazione elimina i file infetti rilevati dall'archivio delle minacce attive. In questo caso, l'applicazione mantiene il file rilevato nella memoria del computer. Per eliminare la minaccia dal computer, selezionare **Disinfetta**.

Come elaborare una minaccia in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Operazioni → Archivi → Minacce attive**.

   Verrà visualizzato l'elenco delle minacce attive.

2. Selezionare l'oggetto che si desidera elaborare.

3. Scegliere il modo in cui si desidera gestire la minaccia:

   - **Disinfetta**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato.

   - **Elimina**. Se questa opzione è selezionata, l'applicazione elimina i file infetti rilevati dall'archivio delle minacce attive. In questo caso, l'applicazione mantiene il file rilevato nella memoria del computer. Per eliminare la minaccia dal computer, selezionare **Disinfetta**.

Come elaborare una minaccia nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **La protezione è a rischio**.

   Verrà visualizzato l'elenco delle minacce attive.

2. Selezionare l'oggetto che si desidera elaborare.

3. Scegliere il modo in cui si desidera gestire la minaccia:

   - **Risolvi**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato.

   - **Aggiungi alle esclusioni**. Se questa azione è selezionata, Kaspersky Endpoint Security consiglia di aggiungere il file all'elenco delle esclusioni dalla scansione. Le impostazioni dell'esclusione vengono configurate automaticamente. Se l'aggiunta di un'esclusione non è disponibile, significa che l'amministratore ha disattivato l'aggiunta di esclusioni nelle impostazioni dei criteri.

   - **Ignora**. Se questa opzione è selezionata, Kaspersky Endpoint Security elimina la voce dall'elenco delle minacce attive. Se nell'elenco non rimangono minacce attive, lo stato del computer verrà modificato in *OK*. Se l'oggetto viene rilevato nuovamente, Kaspersky Endpoint Security aggiungerà una nuova voce all'elenco delle minacce attive.

- **Apri cartella contenitore**. Se questa opzione è selezionata, Kaspersky Endpoint Security apre la cartella contenente l'oggetto in File Manager. È quindi possibile eliminare manualmente l'oggetto o spostare l'oggetto in una cartella che non rientra nell'ambito della protezione.

- **Altre informazioni**. Se questa opzione è selezionata, Kaspersky Endpoint Security apre il sito web del database delle vulnerabilità e delle minacce di Kaspersky.

Per elaborare le minacce attive nella console Kaspersky Security Center, è necessario abilitare il trasferimento delle informazioni sui file non elaborati ad Administration Server. Il trasferimento dei dati è abilitato per impostazione predefinita.

Come abilitare il trasferimento dei dati dei file non elaborati in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Rapporti e archivi**.
4. Nel blocco **Trasferimento dei dati ad Administration Server**, fare clic sul pulsante **Impostazioni**.
5. Selezionare la casella di controllo **File non elaborati**.
6. Salvare le modifiche.

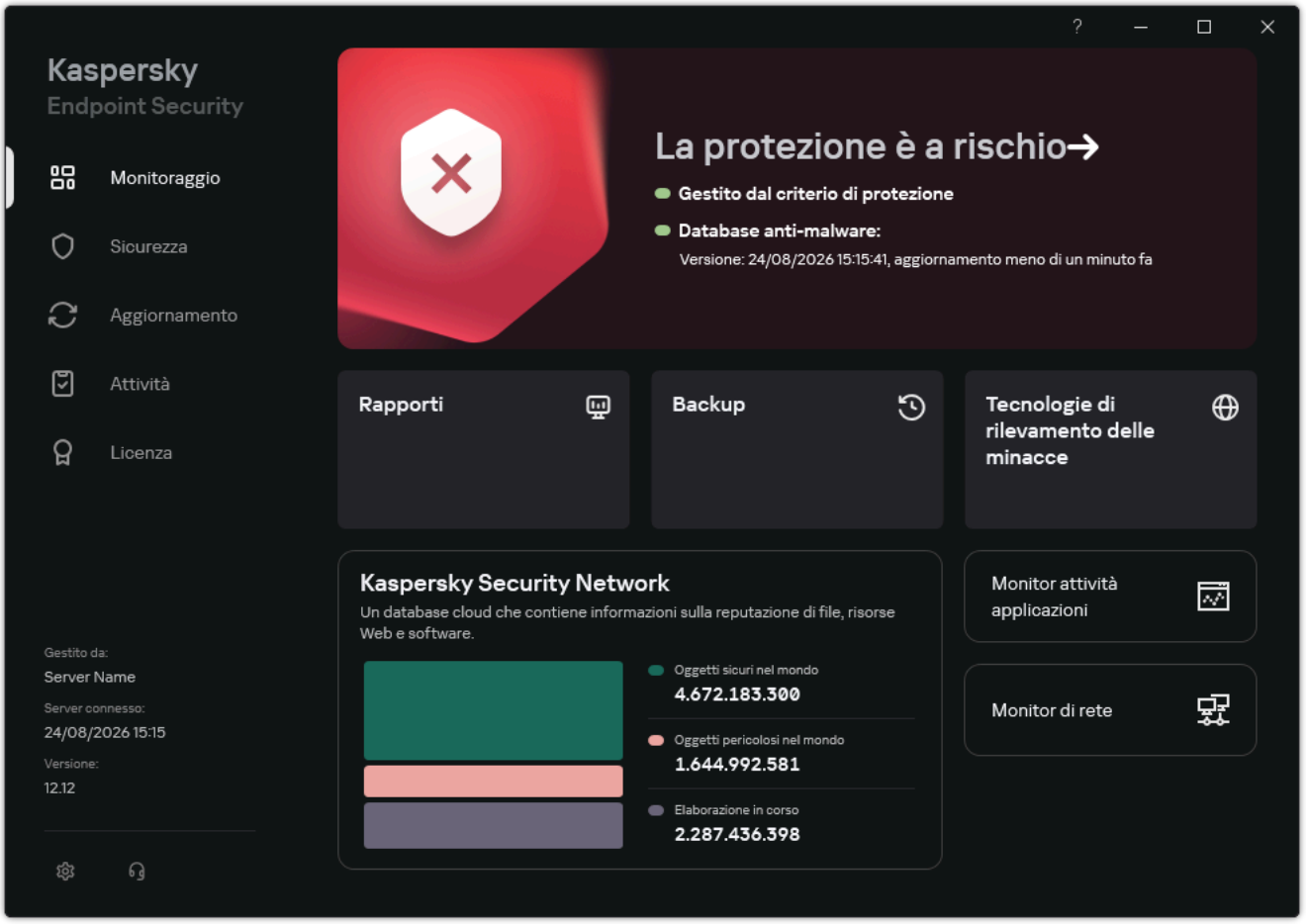
Come abilitare il trasferimento dei dati dei file non elaborati in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Integrazione KSC**.

5. Nella sezione **Trasferimento dei dati ad Administration Server** selezionare la casella di controllo **Informazioni sui file non elaborati**.

6. Salvare le modifiche.



Finestra principale dell'applicazione quando viene rilevata una minaccia

Protezione del computer

Stato della protezione in tempo reale

Kaspersky Endpoint Security invia l'impostazione **Stato protezione in tempo reale** a Kaspersky Security Center Administration Server; il valore di questa impostazione dipende dallo stato corrente dei componenti della protezione dell'applicazione nel computer protetto (vedere la tabella seguente).

Kaspersky Endpoint Security determina lo stato della protezione in tempo reale in base allo stato dei seguenti componenti dell'applicazione:

- Protezione minacce file.
- Protezione minacce Web.
- Protezione minacce di posta.
- Protezione AMSI.
- Prevenzione Attacchi BadUSB.
- Protezione minacce di rete.
- Firewall.
- Prevenzione Exploit.
- Rilevamento del Comportamento.
- Motore di Remediation.
- Prevenzione Intrusioni Host.

È possibile verificare lo stato della protezione in tempo reale dell'applicazione in una console di Kaspersky Security Center.

Come verificare lo stato della protezione in tempo reale in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi gestiti**.

Lo stato corrente della protezione in tempo reale viene visualizzato nell'elenco dei dispositivi, nella colonna **Stato protezione in tempo reale**. Se la colonna **Stato protezione in tempo reale** non è presente, gestire le impostazioni delle colonne facendo clic sul collegamento **Aggiungi/Rimuovi colonne**.

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi gestiti**.

Lo stato corrente della protezione in tempo reale viene visualizzato nell'elenco dei dispositivi, nella colonna **Stato protezione in tempo reale**. Se la colonna **Stato protezione in tempo reale** non è presente, gestire le impostazioni delle colonne facendo clic sul collegamento **Aggiungi/Rimuovi colonne**.

Come verificare la Protezione del computer in tempo reale in Web Console

Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Risorse (dispositivi)**.

Lo stato corrente della protezione in tempo reale viene visualizzato nell'elenco dei dispositivi, nella colonna **Stato protezione in tempo reale**. Se la colonna **Stato protezione in tempo reale** non è presente, gestire le impostazioni delle colonne (⚙).

Possibili valori dell'impostazione Stato protezione in tempo reale

Valore	Descrizione
Sconosciuto	Administration Server non dispone di informazioni sullo stato della protezione in tempo reale per questo computer.
Non installato	Nessun componente è installato.
Non supportato dalla licenza	L'applicazione non è attivata oppure la licenza non consente il funzionamento dei componenti installati.
Non riuscito	Uno o più componenti non funzionano correttamente.
Arrestata	Uno o più componenti sono disabilitati.
Sospesa	Uno o più componenti sono in pausa.
Avvio in corso	È in corso l'attivazione di uno o più componenti.
In esecuzione	I componenti dell'applicazione sono attivi e in esecuzione.

Se il valore dell'impostazione **Stato protezione in tempo reale** in Kaspersky Security Center è diverso da *In esecuzione*, verificare che i componenti installati di Kaspersky Endpoint Security presenti nell'elenco siano abilitati e che l'applicazione sia attivata.

Protezione minacce file

Il componente Protezione minacce file consente di impedire l'infezione del file system del computer. Per impostazione predefinita, il componente Protezione minacce file risiede permanentemente nella RAM del computer ed esegue la scansione di tutti i file aperti, salvati e avviati in tempo reale. Questo componente esegue la scansione dei file in tutte le unità del computer, incluse le unità collegate. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica.

Il componente esegue la scansione dei file a cui l'utente o l'applicazione ha eseguito l'accesso. Se viene rilevato un file dannoso, Kaspersky Endpoint Security blocca l'esecuzione del file. L'applicazione quindi disinfetta o elimina il file dannoso, a seconda delle impostazioni del componente Protezione minacce file.

Quando si tenta di accedere a un file i cui contenuti risiedono nell'archivio cloud OneDrive, Kaspersky Endpoint Security scarica ed esamina i contenuti dei file.

Abilitazione e disabilitazione di Protezione minacce file

Il componente Protezione minacce file è abilitato per impostazione predefinita e viene eseguito nella modalità consigliata dagli esperti Kaspersky. Per Protezione minacce file, Kaspersky Endpoint Security può applicare diversi gruppi di impostazioni. I gruppi di impostazioni archiviate nell'applicazione sono denominati *livelli di protezione*: **Alto**, **Consigliato**, **Basso**. Le impostazioni del livello di sicurezza **Consigliato** sono considerate le impostazioni ottimali consigliate dagli esperti di Kaspersky (vedere la tabella di seguito). È possibile selezionare uno dei livelli di protezione preimpostati o configurare manualmente le impostazioni del livello di protezione. Se si modificano le impostazioni del livello di sicurezza dei file, è possibile ripristinare in qualsiasi momento le impostazioni consigliate.

Il componente Protezione minacce file utilizza i dati ricevuti da altri componenti dell'applicazione. L'abilitazione di tali componenti è facoltativa. I componenti che forniscono ulteriori dati includono:

- Kaspersky Security Network.
- Prevenzione Intrusioni Host.
- Rilevamento del Comportamento.

Come abilitare o disabilitare il componente Protezione minacce file in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce file**.
4. Utilizzare la casella di controllo **Protezione minacce file** per abilitare o disabilitare il componente.
5. Se il componente è stato abilitato, eseguire una delle seguenti operazioni nel blocco **Livello di sicurezza**:
   - Se si desidera applicare uno dei livelli di protezione preimpostati, selezionarlo con il dispositivo di scorrimento:
     - **Alto**. Quando si seleziona questo livello di sicurezza dei file, il componente Protezione minacce file esegue il controllo più approfondito di tutti i file aperti, salvati e avviati. Il componente Protezione minacce file esamina tutti i tipi di file in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer. Vengono inoltre esaminati archivi, pacchetti di installazione e oggetti OLE incorporati.
     - **Consigliato**. Questo livello di sicurezza dei file è consigliato dagli esperti di Kaspersky Lab. Il componente Protezione minacce file esamina solo i formati di file specificati in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer, oltre agli oggetti OLE incorporati. Il componente Protezione minacce file non esamina gli archivi o i pacchetti di installazione.
     - **Basso**. Le impostazioni di questo livello di sicurezza dei file garantiscono la massima velocità di scansione. Il componente Protezione minacce file esamina solo i file con determinate estensioni in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer. Il componente Protezione minacce file non esamina i file compositi.
   - Se si desidera configurare un livello di sicurezza personalizzato, fare clic sul pulsante **Impostazioni** e definire le proprie impostazioni del componente (vedere la tabella seguente).

     È possibile ripristinare i valori dei livelli di sicurezza preimpostati facendo clic sul pulsante **Predefinito**.

6. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi:

   - **Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato.
   - **Disinfetta (se non è possibile, blocca)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, l'applicazione blocca questo file.
   - **Blocca**. Se questa opzione è selezionata, l'applicazione blocca automaticamente il file infetto senza tentare di disinfettarlo o eliminarlo.
   - **Informa**. Se questa opzione è selezionata, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti all'elenco delle minacce attive in caso di rilevamento di tali file.

   Prima di tentare di disinfettare o eliminare un file infetto, l'applicazione crea una copia di backup del file nel caso in cui sia necessario ripristinare il file o se può essere disinfettato in futuro.

7. Salvare le modifiche.

Come abilitare o disabilitare il componente Protezione minacce file in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Protezione minacce file**.
5. Utilizzare l'interruttore **Protezione minacce file ABILITATA** per abilitare o disabilitare il componente.
6. Per aggiungere un nuovo oggetto all'ambito di protezione:
   a. In **Impostazioni avanzate**, selezionare la scheda **Ambito della protezione**.
   b. Fare clic su **Aggiungi**.
   c. Viene visualizzata una finestra, in cui è possibile selezionare gli oggetti che si desidera aggiungere all'ambito della protezione.

Utilizzare le maschere:

- Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

- Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

- Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

È possibile usare le maschere ovunque in un percorso di file o cartella. Ad esempio, se si desidera che l'ambito della scansione includa la cartella Downloads per tutti gli account utente sul computer, immettere la maschera `C:\Users\*\Downloads\`.

È possibile escludere un oggetto dalla protezione senza rimuoverlo dall'elenco degli oggetti nell'ambito della protezione. A tale scopo, impostare l'interruttore accanto ad esso in posizione disattivato.

d. Salvare le modifiche.

7. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi:

   - **Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato.

   - **Disinfetta (se non è possibile, blocca)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, l'applicazione blocca questo file.

   - **Blocca**. Se questa opzione è selezionata, l'applicazione blocca automaticamente il file infetto senza tentare di disinfettarlo o eliminarlo.

   Prima di tentare di disinfettare o eliminare un file infetto, l'applicazione crea una copia di backup del file nel caso in cui sia necessario ripristinare il file o se può essere disinfettato in futuro.

8. Se necessario, modificare le impostazioni avanzate di Protezione minacce file.

9. Salvare le modifiche.

Come abilitare o disabilitare il componente Protezione minacce file nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce file**.

3. Utilizzare l'interruttore **Protezione minacce file** per abilitare o disabilitare il componente.

4. Se il componente è stato abilitato, eseguire una delle seguenti operazioni nel blocco **Livello di sicurezza**:

   - Se si desidera applicare uno dei livelli di protezione preimpostati, selezionarlo con il dispositivo di scorrimento:

     - **Alto**. Quando si seleziona questo livello di sicurezza dei file, il componente Protezione minacce file esegue il controllo più approfondito di tutti i file aperti, salvati e avviati. Il componente Protezione minacce file esamina tutti i tipi di file in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer. Vengono inoltre esaminati archivi, pacchetti di installazione e oggetti OLE incorporati.

     - **Consigliato**. Questo livello di sicurezza dei file è consigliato dagli esperti di Kaspersky Lab. Il componente Protezione minacce file esamina solo i formati di file specificati in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer, oltre agli oggetti OLE incorporati. Il componente Protezione minacce file non esamina gli archivi o i pacchetti di installazione.

     - **Basso**. Le impostazioni di questo livello di sicurezza dei file garantiscono la massima velocità di scansione. Il componente Protezione minacce file esamina solo i file con determinate estensioni in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer. Il componente Protezione minacce file non esamina i file compositi.

   - Se si desidera configurare un livello di sicurezza personalizzato, fare clic sul pulsante **Impostazioni avanzate** e definire le proprie impostazioni del componente (vedere la tabella seguente).

     È possibile ripristinare i valori dei livelli di sicurezza preimpostati facendo clic sul pulsante **Ripristina il livello di sicurezza consigliato**.

5. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi:

   - **Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato.

   - **Disinfetta (se non è possibile, blocca)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, l'applicazione blocca questo file.

   - **Blocca**. Se questa opzione è selezionata, l'applicazione blocca automaticamente il file infetto senza tentare di disinfettarlo o eliminarlo.

   - **Informa**. Se questa opzione è selezionata, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti all'elenco delle minacce attive in caso di rilevamento di tali file.

   Prima di tentare di disinfettare o eliminare un file infetto, l'applicazione crea una copia di backup del file nel caso in cui sia necessario ripristinare il file o se può essere disinfettato in futuro.

6. Salvare le modifiche.

Impostazioni di Protezione minacce file consigliate dagli esperti Kaspersky (livello di sicurezza consigliato)

Parametro	Valore	Descrizione
Tipi di file	**File esaminati per formato**	Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Prima di esaminare un file alla ricerca di codice dannoso, viene analizzata l'intestazione interna del file per determinarne il formato (ad esempio, .txt, .doc o .exe). La scansione cerca inoltre i file con estensioni file particolari.
Analisi euristica	**Superficiale**	Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto. Durante la scansione dei file alla ricerca di codice dannoso, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.
Esamina solo i file nuovi e modificati	**Attivato**	Esamina solo i nuovi file e i file che sono stati modificati dopo l'ultima scansione. Questo consente di ridurre la durata di una scansione. Questa modalità si applica sia ai file semplici che compositi.
Usa Tecnologia iSwift	**Attivato**	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.
Usa Tecnologia iChecker	**Attivato**	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
Esamina i file nei formati Microsoft Office	**Attivato**	Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE. L'applicazione analizza i file in formato Office di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Esamina i file in formato e-mail	**Attivato**	Scansiona i file in formato e-mail. L'applicazione esegue la scansione dei file MSG ed EML. I file in formato e-mail includono anche gli oggetti OLE e i file MHT. Kaspersky Endpoint Security analizza i file in formato e-mail di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Modalità di scansione	**Modalità Smart**	In questa modalità Protezione minacce file esamina un oggetto in base a un'analisi delle azioni eseguite sull'oggetto. Ad esempio, quando si utilizza un documento di Microsoft Office, Kaspersky Endpoint Security esegue la scansione del file quando viene aperto per la prima volta e chiuso per l'ultima volta. Le operazioni intermedie di sovrascrittura del file non ne determinano la scansione.
Azione se viene rilevata una minaccia	**Disinfetta (se non è possibile, elimina)**	Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato.

Sospensione automatica di Protezione minacce file

È possibile configurare la sospensione automatica di Protezione minacce file a un orario specificato o durante l'utilizzo di applicazioni specifiche.

Protezione minacce file deve essere sospeso solo in caso di estrema necessità se si verificano conflitti con alcune applicazioni. In caso di conflitto durante l'esecuzione di un componente, è consigliabile contattare l'Assistenza tecnica di Kaspersky. Gli esperti dell'assistenza forniranno supporto per la configurazione dell'esecuzione del componente Protezione minacce file simultaneamente ad altre applicazioni nel computer.

Per configurare la sospensione automatica di Protezione minacce file:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce file**.

3. Fare clic su **Impostazioni avanzate**.

4. Nella sezione **Sospendi Protezione minacce file**, fare clic sul collegamento **Sospendi Protezione minacce file**.

5. Nella finestra visualizzata, configurare le impostazioni per sospendere Protezione minacce file:

   a. Configurare una pianificazione per sospendere automaticamente Protezione minacce file.

   b. Creare un elenco di applicazioni il cui funzionamento dovrebbe causare la sospensione delle attività di Protezione minacce file.

6. Salvare le modifiche.

Modifica dell'azione eseguita sui file infetti dal componente Protezione minacce file

Per impostazione predefinita, il componente Protezione minacce file tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, il componente Protezione minacce file elimina questi file.

Per modificare l'azione eseguita sui file infetti dal componente Protezione minacce file:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce file**.

3. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'opzione pertinente:

   - **Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato.

   - **Disinfetta (se non è possibile, blocca)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, l'applicazione blocca questo file.

   - **Blocca**. Se questa opzione è selezionata, l'applicazione blocca automaticamente il file infetto senza tentare di disinfettarlo o eliminarlo.

   Prima di tentare di disinfettare o eliminare un file infetto, l'applicazione crea una copia di backup del file nel caso in cui sia necessario ripristinare il file o se può essere disinfettato in futuro.

4. Salvare le modifiche.

Creazione dell'ambito di protezione del componente Protezione minacce file

L'ambito di protezione si riferisce agli oggetti che vengono esaminati dal componente quando è abilitato. Gli ambiti di protezione dei vari componenti dispongono di differenti proprietà. La posizione e il tipo di file da esaminare sono proprietà dell'ambito di protezione del componente Protezione minacce file. Per impostazione predefinita, il componente Protezione minacce file esamina solo i file potenzialmente infettabili eseguiti da dischi rigidi, unità rimovibili e unità di rete.

Durante la selezione del tipo di file da esaminare, tenere presenti i seguenti elementi:

1. Esiste una bassa probabilità in merito all'introduzione di codice dannoso nei file di determinati formati e alla successiva attivazione (ad esempio il formato TXT). Altri formati di file, al contrario, contengono codice eseguibile (ad esempio exe, dll). È inoltre possibile che il codice eseguibile sia contenuto in formati di file che non sono destinati a questo scopo (ad esempio il formato DOC). Il rischio di penetrazione e attivazione di codice dannoso in tali file è alto.

2. Un utente malintenzionato potrebbe inviare un virus o un'altra applicazione dannosa al computer dell'utente in un file eseguibile rinominato con estensione txt. Se si seleziona la scansione dei file in base all'estensione, l'applicazione ignora il file durante la scansione. Se è selezionata la scansione dei file in base al formato, Kaspersky Endpoint Security analizza l'intestazione del file indipendentemente dall'estensione. Se l'analisi rivela che il file presenta il formato di un file eseguibile (ad esempio EXE), l'applicazione lo esamina.

Per creare l'ambito di protezione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce file**.

3. Fare clic su **Impostazioni avanzate**.

4. Nel blocco **Tipi di file**, specificare il tipo di file che deve essere esaminato dal componente Protezione minacce file:

   - **Tutti i file**. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina tutti i file senza eccezioni (tutti i formati e le estensioni).

   - **File esaminati per formato**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Prima di esaminare un file alla ricerca di codice dannoso, viene analizzata l'intestazione interna del file per determinarne il formato (ad esempio, .txt, .doc o .exe). La scansione cerca inoltre i file con estensioni file particolari.

   - **File esaminati per estensione**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Il formato del file viene quindi determinato in base all'estensione.

5. Fare clic sul collegamento **Modifica ambito della protezione**.

6. Nella finestra visualizzata, selezionare gli oggetti che si desidera aggiungere o escludere dall'ambito della protezione.

   Non è possibile rimuovere o modificare gli oggetti che sono inclusi nell'ambito di protezione predefinito.

7. Per aggiungere un nuovo oggetto all'ambito di protezione:

   a. Fare clic su **Aggiungi**.

      Verrà visualizzata la struttura di cartelle.

   b. Nel campo **Percorso**, immettere il percorso del file o della cartella.

      Utilizzare le maschere:

      - Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

      - Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

      - Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

      È possibile usare le maschere ovunque in un percorso di file o cartella. Ad esempio, se si desidera che l'ambito della scansione includa la cartella Downloads per tutti gli account utente sul computer, immettere la maschera `C:\Users\*\Downloads\`.

      L'oggetto **Questo PC** nell'elenco delle risorse file del computer include i seguenti oggetti: **Tutti i dischi rigidi**, **Tutte le unità di rete** e **Tutte le unità rimovibili**.

   È possibile escludere un oggetto dalle scansioni senza eliminarlo dall'elenco degli oggetti nell'ambito della scansione. A tale scopo, deselezionare la casella di controllo accanto all'oggetto.

8. Salvare le modifiche.

Utilizzo dei metodi di scansione

Kaspersky Endpoint Security utilizza una tecnica di scansione denominata Machine Learning e analisi delle firme. Durante l'analisi delle firme, Kaspersky Endpoint Security confronta l'oggetto rilevato con i record nel proprio database. In base ai suggerimenti degli esperti Kaspersky, il metodo Machine Learning e analisi delle firme è sempre abilitato.

Per aumentare l'efficacia della protezione, è possibile utilizzare l'analisi euristica. Durante la scansione dei file alla ricerca di codice dannoso, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.

Per configurare l'utilizzo dell'analisi euristica durante l'esecuzione del componente Protezione minacce file:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Protezione minacce file**.
3. Fare clic su **Impostazioni avanzate**.
4. Se si desidera che l'applicazione utilizzi l'analisi euristica per la protezione contro le minacce file, selezionare la casella di controllo **Analisi euristica** nella sezione **Metodi di scansione**. Quindi utilizzare il dispositivo di scorrimento per impostare il livello di analisi euristica: **Superficiale**, **Media** o **Approfondita**.
5. Salvare le modifiche.

Utilizzo delle tecnologie di scansione durante l'esecuzione del componente Protezione minacce file

Per configurare l'utilizzo delle tecnologie di scansione durante l'esecuzione del componente Protezione minacce file:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Protezione minacce file**.
3. Fare clic su **Impostazioni avanzate**.
4. Nella sezione **Tecnologie di scansione** selezionare le caselle di controllo accanto ai nomi delle tecnologie da utilizzare per la protezione dalle minacce file:
   - **Usa Tecnologia iSwift**. Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.
   - **Usa Tecnologia iChecker**. Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
5. Salvare le modifiche.

Ottimizzazione della scansione dei file

È possibile ottimizzare la scansione dei file eseguita dal componente Protezione minacce file riducendo il tempo di scansione e aumentando la velocità di esecuzione di Kaspersky Endpoint Security. Per ottenere questo risultato, è possibile eseguire la scansione solo dei file nuovi e modificati dopo l'ultima scansione. Questa modalità si applica sia ai file semplici che compositi.

È inoltre possibile abilitare l'utilizzo delle tecnologie iChecker e iSwift, che ottimizzano la velocità di scansione dei file escludendo i file che non sono stati modificati dall'ultima scansione.

Per ottimizzare la scansione dei file:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce file**.
3. Fare clic su **Impostazioni avanzate**.
4. Nella sezione **Ottimizzazione** selezionare la casella di controllo **Esamina solo i file nuovi e modificati**.
5. Salvare le modifiche.

Scansione dei file compositi

Una tecnica comune per nascondere virus e altro malware è inserirli in file compositi, come ad esempio archivi o database. Per rilevare i virus e il malware nascosti in questo modo, è necessario decomprimere il file composito, cosa che può rallentare la scansione. È possibile limitare i tipi di file compositi da esaminare, velocizzando la scansione.

Il metodo elabora un file composito infetto (disinfezione o eliminazione) a seconda del tipo di file.

Il componente Protezione minacce file disinfetta i file compositi nei formati ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR e ICE ed elimina i file in tutti gli altri formati (ad eccezione dei database di posta).

Per configurare la scansione dei file compositi:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce file**.
3. Fare clic su **Impostazioni avanzate**.
4. Nel blocco **Scansione dei file compositi**, specificare i tipi di file compositi di cui eseguire la scansione: archivi, pacchetti di distribuzione, posto o file in formato Office.

5. Se la scansione dei soli file nuovi e modificati è disabilitata, configurare le impostazioni per la scansione di ogni tipo di file composito: esamina tutti i file di questo tipo o solo i nuovi file.

   Se è abilitata la scansione dei soli file nuovi e modificati, Kaspersky Endpoint Security esamina solo i file nuovi e modificati di tutti i tipi di file compositi.

6. Configurare le impostazioni avanzate per la scansione dei file compositi.

   - **Non decomprimere i file compositi di grandi dimensioni**.

     Se la casella di controllo è selezionata, Kaspersky Endpoint Security non esegue la scansione dei file compositi se la loro dimensione supera il valore specificato.

     Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esamina i file compositi di qualsiasi dimensione.

     > Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi, indipendentemente dal fatto che la casella di controllo **Non decomprimere i file compositi di grandi dimensioni** sia selezionata o meno.

   - **Decomprimi file compositi in background**.

     Se la casella di controllo è selezionata, Kaspersky Endpoint Security consente di accedere ai file compositi di dimensioni superiori al valore specificato prima della scansione dei file. In questo caso, Kaspersky Endpoint Security decomprime ed esamina i file compositi in background.

     Kaspersky Endpoint Security consente di accedere ai file compositi di dimensioni inferiori a questo valore solo dopo la decompressione e la scansione dei file.

     Se la casella di controllo non è selezionata, Kaspersky Endpoint Security consente di accedere ai file compositi solo dopo la decompressione e la scansione di file di qualsiasi dimensione.

7. Salvare le modifiche.

Modifica della modalità di scansione

Modalità di scansione fa riferimento alla condizione che attiva la scansione dei file da parte del componente Protezione minacce file. Per impostazione predefinita, Kaspersky Endpoint Security esegue la scansione dei file in modalità Smart. In questa modalità di scansione file, il componente Protezione minacce file stabilisce se eseguire o meno la scansione dei file dopo aver analizzato le operazioni eseguite con il file da parte dell'utente, di un'applicazione per conto dell'utente (tramite l'account con cui è stato eseguito l'accesso o un account utente differente) o del sistema operativo. Ad esempio, quando si lavora con un documento di Microsoft Office Word, Kaspersky Endpoint Security esegue la scansione del file quando viene aperto per la prima volta e chiuso per l'ultima volta. Le operazioni intermedie di sovrascrittura del file non ne determinano la scansione.

Per modificare la modalità di scansione dei file:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce file**.

3. Fare clic su **Impostazioni avanzate**.

4. Nel blocco **Modalità di scansione**, selezionare la modalità desiderata:

   - **Modalità Smart**. In questa modalità Protezione minacce file esamina un oggetto in base a un'analisi delle azioni eseguite sull'oggetto. Ad esempio, quando si utilizza un documento di Microsoft Office, Kaspersky Endpoint Security esegue la scansione del file quando viene aperto per la prima volta e chiuso per l'ultima volta. Le operazioni intermedie di sovrascrittura del file non ne determinano la scansione.

   - **In fase di accesso e modifica**. In questa modalità Protezione minacce file esamina gli oggetti in caso di tentativo di apertura o modifica.

   - **In fase di accesso**. In questa modalità Protezione minacce file esamina gli oggetti solo in caso di tentativo di apertura.

   - **In fase di esecuzione**. In questa modalità Protezione minacce file esamina gli oggetti solo in caso di tentativo di esecuzione.

5. Salvare le modifiche.

Scansione dei contenitori

Un *contenitore* è un ambiente isolato in cui un'applicazione può essere eseguita senza interagire direttamente con il sistema operativo. L'utilizzo di contenitori comporta i seguenti rischi:

- Gli hacker potrebbero essere in grado di sfruttare le vulnerabilità della containerizzazione per compromettere le applicazioni all'interno del contenitore.

- Gli hacker possono sfruttare una configurazione non protetta dell'ambiente dei contenitori per ottenere l'accesso non autorizzato ai dati nel computer o per compromettere l'integrità del sistema.

- Un attacco a un contenitore sferrato con successo può consentire a un hacker di ottenere l'accesso ai dati nel computer.

- Gli hacker possono sfruttare le vulnerabilità della rete per intercettare il traffico di rete.

Kaspersky Endpoint Security analizza i file non solo nei dischi, ma anche all'interno dei contenitori. Kaspersky Endpoint Security è uno strumento esterno per il rilevamento di attività dannose all'interno dei contenitori. Questo consente di mantenere le prestazioni dei contenitori e previene conflitti con altre applicazioni all'interno del contenitore. L'installazione di Kaspersky Endpoint Security all'interno del contenitore non è supportata.

Oltre a fornire la protezione dei contenitori, Kaspersky Endpoint Security consente di gestire le applicazioni all'interno di contenitori tramite Controllo applicazioni. Controllo applicazioni viene configurato per i contenitori allo stesso modo delle applicazioni installate nel computer. Monitoraggio integrità di sistema supporta anche i contenitori.

Requisiti dei contenitori

- Il contenitore deve essere un contenitore Docker. Gli altri strumenti di containerizzazione non sono supportati.

- Il contenitore deve essere eseguito in modalità di isolamento dei processi. La modalità di isolamento Hyper-V non è supportata.

- Il contenitore deve essere ubicato in un server Windows Server 2016, 2019 o 2022 (Docker Host).
- Il contenitore deve includere un'immagine Windows (Docker Image). Windows 10 e 11 non sono supportati. Le immagini Linux non sono supportate.

Azione se viene rilevata una minaccia

Se viene rilevata una minaccia all'interno di un contenitore, l'applicazione applica l'azione selezionata per il componente Protezione minacce file. La scansione dei contenitori ha impostazioni aggiuntive (vedere le istruzioni di seguito). Se viene rilevata una minaccia, l'applicazione blocca l'attività dannosa ed esegue l'azione selezionata (ad esempio, i tentativi di disinfezione dell'oggetto). Kaspersky Endpoint Security può arrestare il contenitore se l'oggetto rilevato non può essere disinfettato. Per impostazione predefinita, la funzionalità di arresto dei contenitori è disabilitata.

Come configurare i contenitori in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce file**.
4. Fare clic su **Impostazioni**.
5. Viene visualizzata una finestra, che consente di selezionare la scheda **Avanzate**.
6. Nel blocco **Scansione delle operazioni sui file eseguite nei contenitori Windows**, configurare le impostazioni di scansione dei contenitori:
   - **Arresta il contenitore se la disinfezione non riesce**. L'applicazione potrebbe non disporre di diritti di lettura e scrittura sufficienti per l'oggetto rilevato. In tal caso, la disinfezione o l'eliminazione dell'oggetto rilevato non è possibile. Se questa casella di controllo è selezionata, l'applicazione blocca l'oggetto rilevato e arresta il contenitore. Se questa casella di controllo è deselezionata, l'applicazione blocca solo l'oggetto rilevato.
   - **Non eseguire la scansione delle operazioni sui file eseguite nei contenitori Windows**. Se la casella di controllo è selezionata, l'applicazione esegue la scansione del contenitore solo all'avvio del contenitore. Se la casella di controllo è deselezionata, l'applicazione esegue la scansione del contenitore costantemente in tempo reale.
7. Salvare le modifiche.

Come configurare la scansione dei contenitori in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Protezione minacce file**.
5. In **Impostazioni avanzate**, selezionare la scheda **Prestazioni**.

6. Nel blocco **Ottimizzazione della scansione**, configurare le impostazioni di scansione dei contenitori:

   - **Arresta il contenitore se la disinfezione non riesce**. L'applicazione potrebbe non disporre di diritti di lettura e scrittura sufficienti per l'oggetto rilevato. In tal caso, la disinfezione o l'eliminazione dell'oggetto rilevato non è possibile. Se questa casella di controllo è selezionata, l'applicazione blocca l'oggetto rilevato e arresta il contenitore. Se questa casella di controllo è deselezionata, l'applicazione blocca solo l'oggetto rilevato.

   - **Non eseguire la scansione delle operazioni sui file eseguite nei contenitori Windows**. Se la casella di controllo è selezionata, l'applicazione esegue la scansione del contenitore solo all'avvio del contenitore. Se la casella di controllo è deselezionata, l'applicazione esegue la scansione del contenitore costantemente in tempo reale.

7. Salvare le modifiche.

Come configurare la scansione dei contenitori nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce file**.

3. Nel blocco **Scansione delle operazioni sui file eseguite nei contenitori Windows**, configurare le impostazioni di scansione dei contenitori:

   - **Arresta il contenitore se la disinfezione non riesce**. L'applicazione potrebbe non disporre di diritti di lettura e scrittura sufficienti per l'oggetto rilevato. In tal caso, la disinfezione o l'eliminazione dell'oggetto rilevato non è possibile. Se questa casella di controllo è selezionata, l'applicazione blocca l'oggetto rilevato e arresta il contenitore. Se questa casella di controllo è deselezionata, l'applicazione blocca solo l'oggetto rilevato.

   - **Non eseguire la scansione delle operazioni sui file eseguiti nei contenitori Windows**. Se la casella di controllo è selezionata, l'applicazione esegue la scansione del contenitore solo all'avvio del contenitore. Se la casella di controllo è deselezionata, l'applicazione esegue la scansione del contenitore costantemente in tempo reale.

4. Salvare le modifiche.

Prevenzione Intrusioni Host

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server.

Il componente Prevenzione Intrusioni Host impedisce alle applicazioni di eseguire azioni che possono essere pericolose per il sistema operativo, assicurando il controllo dell'accesso alle risorse del sistema operativo e ai dati personali. Il componente garantisce la protezione del computer mediante database anti-virus e il servizio cloud Kaspersky Security Network.

Il componente controlla l'esecuzione delle applicazioni utilizzando *i diritti delle applicazioni*. I diritti delle applicazioni includono i seguenti parametri di accesso:

- Accesso alle risorse del sistema operativo (ad esempio opzioni di avvio automatico, chiavi di registro)
- Accesso ai dati personali (ad esempio file e applicazioni)

L'attività di rete delle applicazioni è controllata dal componente Firewall mediante le *regole di rete*.

Durante il primo avvio dell'applicazione, il componente Prevenzione Intrusioni Host esegue le seguenti azioni:

1. Verifica la sicurezza dell'applicazione utilizzando i database anti-virus scaricati.
2. Verifica la sicurezza dell'applicazione in Kaspersky Security Network.

   È consigliabile partecipare a Kaspersky Security Network per un miglior funzionamento del componente Prevenzione Intrusioni Host.

3. Colloca l'applicazione in uno dei gruppi di attendibilità: *Attendibili*, *Restrizione bassa*, *Restrizione alta*, *Non attendibili*.

   Un gruppo di attendibilità definisce i diritti a cui Kaspersky Endpoint Security fa riferimento durante il controllo delle attività delle applicazioni. Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità in base al livello di pericolosità che l'applicazione può rappresentare per il computer.

   Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità per i componenti Firewall e Prevenzione Intrusioni Host. Non è possibile modificare il gruppo di attendibilità solo per Firewall o Prevenzione Intrusioni Host.

   Se si rifiuta di partecipare a KSN o non è disponibile alcuna rete, Kaspersky Endpoint Security inserisce l'applicazione in un gruppo di attendibilità in base alle impostazioni del componente Prevenzione Intrusioni Host. Dopo la ricezione della reputazione dell'applicazione da KSN, il gruppo di attendibilità può essere modificato automaticamente.

4. Blocca le azioni dell'applicazione in base al gruppo di attendibilità. Ad esempio, alle applicazioni del gruppo di attendibilità *Restrizione alta* viene negato l'accesso ai moduli del sistema operativo.

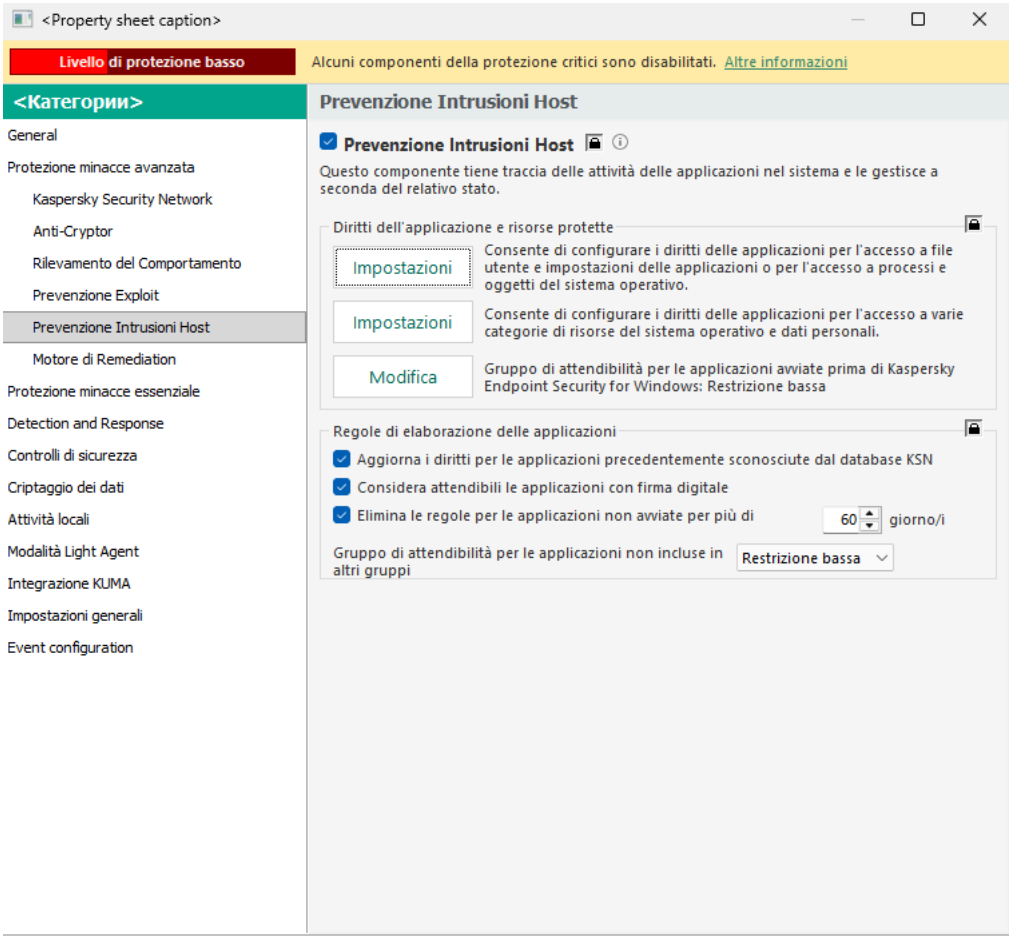
Al successivo avvio dell'applicazione, Kaspersky Endpoint Security verifica l'integrità dell'applicazione. Se l'applicazione non è stata modificata, il componente utilizza i diritti delle applicazioni correnti. Se l'applicazione è stata modificata, Kaspersky Endpoint Security la analizza come se si trattasse del primo avvio.

Abilitazione e disabilitazione di Prevenzione Intrusioni Host

Il componente Prevenzione Intrusioni Host è abilitato per impostazione predefinita e viene eseguito nella modalità consigliata dagli esperti Kaspersky.

Come abilitare o disabilitare il componente Prevenzione Intrusioni Host in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.



Impostazioni di Prevenzione intrusioni

4. Utilizzare la casella di controllo **Prevenzione Intrusioni Host** per abilitare o disabilitare il componente.
5. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare il componente Prevenzione Intrusioni Host in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host → Prevenzione Intrusioni Host**.
5. Utilizzare l'interruttore **Prevenzione Intrusioni Host ABILITATA** per abilitare o disabilitare il componente.
6. Salvare le modifiche.

Come abilitare o disabilitare il componente Prevenzione Intrusioni Host nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.
3. Utilizzare l'interruttore **Prevenzione Intrusioni Host** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Se il componente Prevenzione Intrusioni Host è abilitato, Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità in base al livello di pericolosità che l'applicazione può rappresentare per il computer. Kaspersky Endpoint Security bloccherà quindi le azioni dell'applicazione a seconda del gruppo di attendibilità.

Gestione dei gruppi di attendibilità delle applicazioni

Quando ogni applicazione viene avviata per la prima volta, il componente Prevenzione Intrusioni Host controlla la sicurezza dell'applicazione e la inserisce in uno dei gruppi di attendibilità.

Durante la prima fase della scansione delle applicazioni, Kaspersky Endpoint Security esegue una ricerca nel database interno delle applicazioni note per determinare se è presente una voce corrispondente e contemporaneamente invia una richiesta al database di Kaspersky Security Network (se è disponibile una connessione Internet). In base ai risultati di ricerca nel database interno e nel database di Kaspersky Security Network, l'applicazione viene inserita in un gruppo di attendibilità. Ogni volta che l'applicazione viene successivamente avviata, Kaspersky Endpoint Security invia una nuova query al database KSN e inserisce l'applicazione in un gruppo di attendibilità diverso se la reputazione dell'applicazione nel database KSN è cambiata.

È possibile selezionare un gruppo di attendibilità in cui si desidera che Kaspersky Endpoint Security assegni automaticamente tutte le applicazioni sconosciute. Le applicazioni in esecuzione prima dell'avvio di Kaspersky Endpoint Security vengono automaticamente inserite nel gruppo di attendibilità impostato nelle impostazioni di Prevenzione Intrusioni Host.

Per le applicazioni avviate prima di Kaspersky Endpoint Security, verrà controllata solo l'attività di rete. Il controllo viene eseguito in base alle regole di rete definite nelle impostazioni di Firewall.

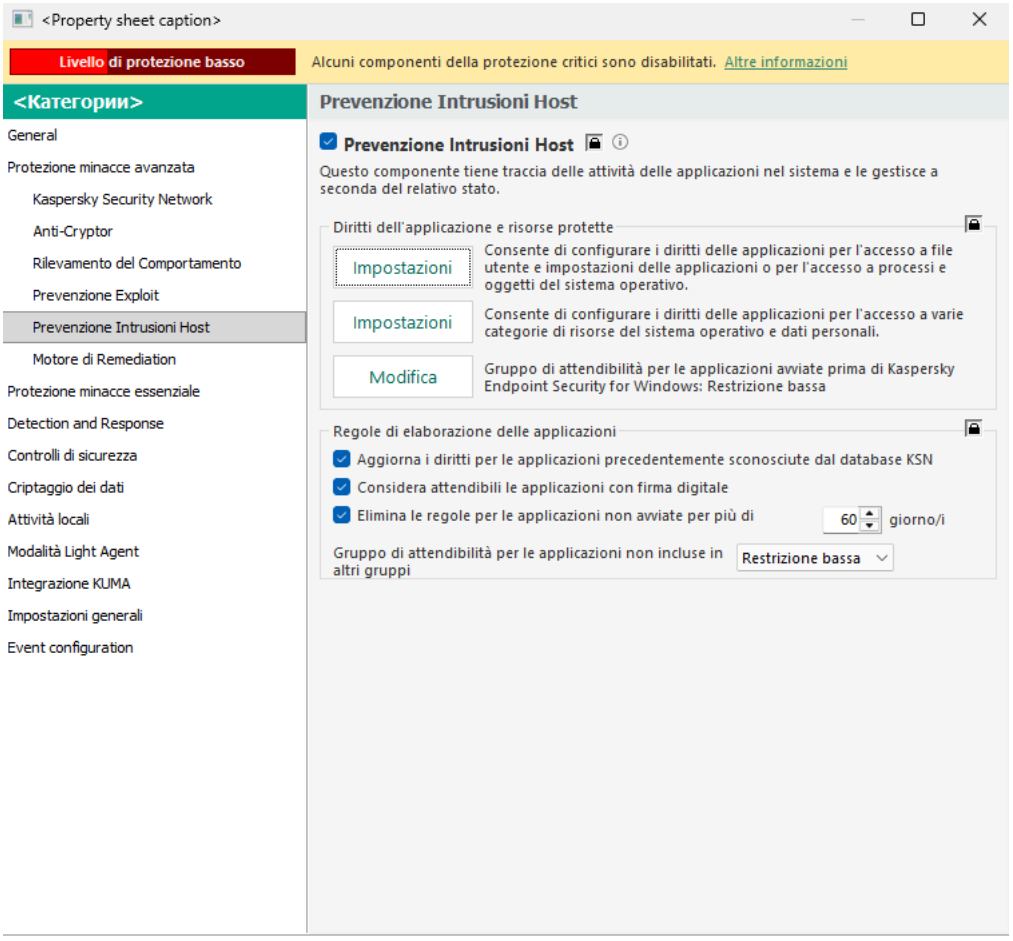
Modifica del gruppo di attendibilità di un'applicazione

Quando ogni applicazione viene avviata per la prima volta, il componente Prevenzione Intrusioni Host controlla la sicurezza dell'applicazione e la inserisce in uno dei gruppi di attendibilità.

Gli specialisti di Kaspersky consigliano di non spostare le applicazioni dal gruppo di attendibilità a cui sono assegnate automaticamente. In alternativa, è possibile modificare i diritti per una singola applicazione, se necessario.

Come modificare il gruppo di attendibilità di un'applicazione in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.



Impostazioni di Prevenzione intrusioni

4. Nel blocco **Diritti dell'applicazione e risorse protette**, fare clic sul pulsante **Impostazioni**.

   Verranno visualizzati la finestra di configurazione dei diritti dell'applicazione e l'elenco delle risorse protette.
5. Selezionare la scheda **Diritti applicazione**.
6. Fare clic su **Aggiungi**.
7. Nella finestra visualizzata, immettere i criteri per cercare l'applicazione di cui di desidera modificare il gruppo di attendibilità.

   È possibile immettere il nome dell'applicazione o il nome del fornitore. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.
8. Fare clic su **Aggiorna**.

   Kaspersky Endpoint Security cercherà l'applicazione nell'elenco consolidato di applicazioni installate nei computer gestiti. Kaspersky Endpoint Security mostrerà un elenco di applicazioni che soddisfano i criteri di ricerca.
9. Selezionare l'applicazione desiderata.

10. Nell'elenco a discesa **Aggiungi l'applicazione selezionata al gruppo di attendibilità**, selezionare il gruppo di attendibilità necessario per l'applicazione.

11. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come modificare il gruppo di attendibilità di un'applicazione in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Protezione minacce host** → **Prevenzione Intrusioni Host**.

5. Nella sezione **Diritti dell'applicazione e risorse protette**, fare clic sul collegamento **Diritti dell'applicazione e risorse protette**.

   Verranno visualizzati la finestra di configurazione dei diritti dell'applicazione e l'elenco delle risorse protette.

6. Selezionare la scheda **Diritti applicazione**.

   Verrà visualizzato un elenco di gruppi di attendibilità sul lato sinistro della finestra e le relative proprietà sul lato destro.

7. Fare clic su **Aggiungi**.

   Verrà avviata la procedura guidata per l'aggiunta di un'applicazione a un gruppo di attendibilità.

8. Selezionare il gruppo di attendibilità pertinente per l'applicazione.

9. Selezionare il tipo **Applicazione**. Procedere con il passaggio successivo.

   Se si desidera modificare il gruppo di attendibilità per più applicazioni, selezionare il tipo **Gruppo** e definire un nome per il gruppo di applicazioni.

10. Nell'elenco delle applicazioni visualizzato selezionare le applicazioni per le quali si desidera modificare il gruppo di attendibilità.

    Utilizzare un filtro. È possibile immettere il nome dell'applicazione o il nome del fornitore. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

11. Terminare la procedura guidata.

    L'applicazione verrà aggiunta al gruppo di attendibilità.

12. Salvare le modifiche.

Come modificare il gruppo di attendibilità di un'applicazione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.

3. Fare clic su **Gestisci applicazioni**.

   Verrà visualizzato l'elenco delle applicazioni installate.

4. Selezionare l'applicazione desiderata.

5. Nel menu di scelta rapida dell'applicazione, file clic su **Restrizioni** → **<gruppo di attendibilità>**.

6. Salvare le modifiche.

Di conseguenza, l'applicazione verrà inserita nell'altro gruppo di attendibilità. Kaspersky Endpoint Security bloccherà quindi le azioni dell'applicazione a seconda del gruppo di attendibilità. All'applicazione verrà assegnato lo stato *(definita dall'utente)*. Se la reputazione dell'applicazione viene modificata in Kaspersky Security Network, il componente Prevenzione Intrusioni Host lascerà invariato il gruppo di attendibilità dell'applicazione.

Configurazione dei diritti dei gruppi di attendibilità

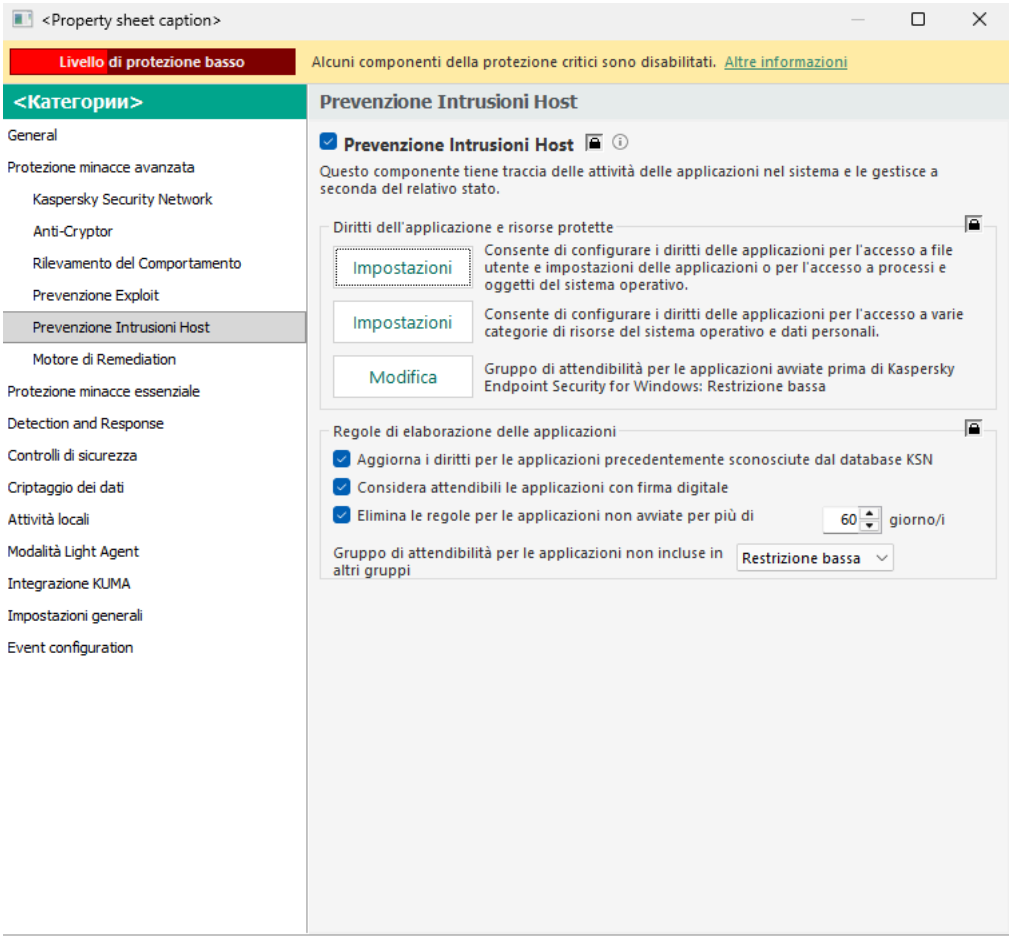
I diritti ottimali delle applicazioni vengono creati per diversi gruppi di attendibilità per impostazione predefinita. Le impostazioni dei diritti per i gruppi di applicazioni che si trovano in un gruppo di attendibilità ereditano i valori dalle impostazioni dei diritti dei gruppi di attendibilità.

Come modificare i diritti dei gruppi di attendibilità in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.



Impostazioni di Prevenzione intrusioni

4. Nel blocco **Diritti dell'applicazione e risorse protette**, fare clic sul pulsante **Impostazioni**.

   Verranno visualizzati la finestra di configurazione dei diritti dell'applicazione e l'elenco delle risorse protette.

5. Passare alla scheda **Diritti applicazione**.

6. Selezionare il gruppo di attendibilità necessario.

7. Nel menu di scelta rapida del gruppo di attendibilità, selezionare **Diritti del gruppo**.

   Verranno visualizzate le proprietà del gruppo di attendibilità.

8. Eseguire una delle seguenti operazioni:

   - Se si desidera modificare i diritti del gruppo di attendibilità che regolano le operazioni con il registro del sistema operativo, i file utente e le impostazioni dell'applicazione, selezionare **File e Registro di sistema**.
   - Se si desidera modificare i diritti del gruppo di attendibilità che regolano l'accesso ai processi e agli oggetti del sistema operativo, selezionare **Diritti**.

   L'attività di rete delle applicazioni è controllata dal componente Firewall mediante le *regole di rete*.

9. Per la risorsa opportuna, nella colonna dell'azione corrispondente, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida e selezionare l'opzione necessaria: **Eredita**, **Consenti** (✓) o **Blocca** (⊘).

10. Se si desidera monitorare l'utilizzo delle risorse del computer, selezionare **Registra eventi** (✓ / ⊘).

    Kaspersky Endpoint Security registrerà le informazioni sul funzionamento del componente Prevenzione Intrusioni Host. I rapporti contengono informazioni sulle operazioni con le risorse del computer eseguite dall'applicazione (consentite o vietate). I rapporti contengono anche informazioni sulle applicazioni che utilizzano ciascuna risorsa.

11. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come modificare i diritti del gruppo di attendibilità in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Protezione minacce host** → **Prevenzione Intrusioni Host**.

5. Nella sezione **Diritti dell'applicazione e risorse protette**, fare clic sul collegamento **Diritti dell'applicazione e risorse protette**.

   Verranno visualizzati la finestra di configurazione dei diritti dell'applicazione e l'elenco delle risorse protette.

6. Passare alla scheda **Diritti applicazione**.

   Verrà visualizzato un elenco di gruppi di attendibilità sul lato sinistro della finestra e le relative proprietà sul lato destro.

7. Nella parte sinistra della finestra selezionare il gruppo di attendibilità opportuno.

8. Nella parte destra della finestra, nell'elenco a discesa, eseguire una delle seguenti operazioni:

   - Se si desidera modificare i diritti del gruppo di attendibilità che regolano le operazioni con il registro del sistema operativo, i file utente e le impostazioni dell'applicazione, selezionare **File e Registro di sistema**.
   - Se si desidera modificare i diritti del gruppo di attendibilità che regolano l'accesso ai processi e agli oggetti del sistema operativo, selezionare **Diritti**.

   L'attività di rete delle applicazioni è controllata dal componente Firewall mediante le *regole di rete*.

9. Per la risorsa opportuna, nella colonna dell'azione corrispondente selezionare l'opzione necessaria: **Eredita**, **Consenti** (), **Blocca** ().

10. Se si desidera monitorare l'utilizzo delle risorse del computer, selezionare **Registra eventi** (/).

    Kaspersky Endpoint Security registrerà le informazioni sul funzionamento del componente Prevenzione Intrusioni Host. I rapporti contengono informazioni sulle operazioni con le risorse del computer eseguite dall'applicazione (consentite o vietate). I rapporti contengono anche informazioni sulle applicazioni che utilizzano ciascuna risorsa.

11. Salvare le modifiche.

Come modificare i diritti del gruppo di attendibilità nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.

3. Fare clic su **Gestisci applicazioni**.

   Verrà visualizzato l'elenco delle applicazioni installate.

4. Selezionare il gruppo di attendibilità necessario.

5. Nel menu di scelta rapida del gruppo di attendibilità, selezionare **Dettagli e regole**.

   Verranno visualizzate le proprietà del gruppo di attendibilità.

6. Eseguire una delle seguenti operazioni:

   - Se si desidera modificare i diritti del gruppo di attendibilità che regolano le operazioni con il registro del sistema operativo, i file utente e le impostazioni dell'applicazione, selezionare **File e Registro di sistema**.
   - Se si desidera modificare i diritti del gruppo di attendibilità che regolano l'accesso ai processi e agli oggetti del sistema operativo, selezionare **Diritti**.

   L'attività di rete delle applicazioni è controllata dal componente Firewall mediante le *regole di rete*.

7. Per la risorsa opportuna, nella colonna dell'azione corrispondente, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida e selezionare l'opzione necessaria: **Eredita**, **Consenti** () o **Nega** ().

8. Se si desidera monitorare l'utilizzo delle risorse del computer, selezionare **Registra eventi** ( ).

   Kaspersky Endpoint Security registrerà le informazioni sul funzionamento del componente Prevenzione Intrusioni Host. I rapporti contengono informazioni sulle operazioni con le risorse del computer eseguite dall'applicazione (consentite o vietate). I rapporti contengono anche informazioni sulle applicazioni che utilizzano ciascuna risorsa.

9. Salvare le modifiche.

I diritti del gruppo di attendibilità verranno modificati. Kaspersky Endpoint Security bloccherà quindi le azioni dell'applicazione a seconda del gruppo di attendibilità. Lo stato (*Impostazioni personalizzate*) verrà assegnato al gruppo di attendibilità.

Selezione di un gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security

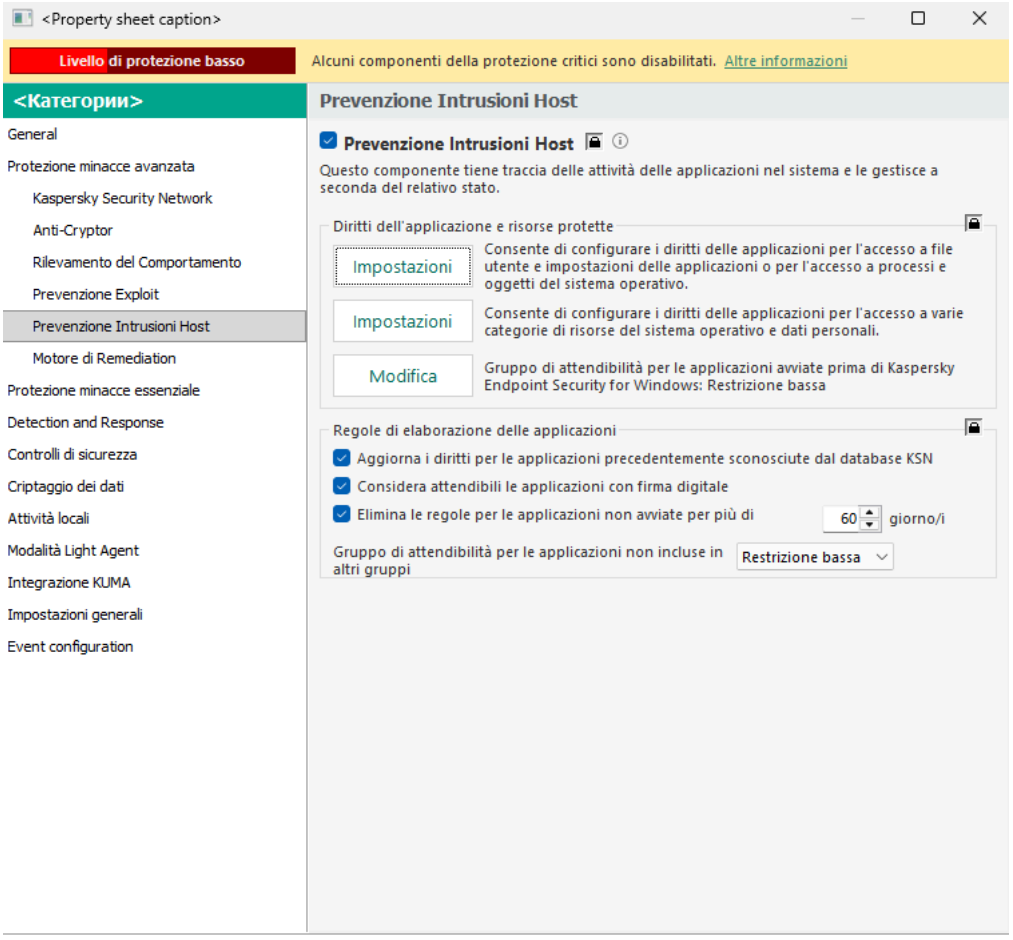
Per le applicazioni avviate prima di Kaspersky Endpoint Security, verrà controllata solo l'attività di rete. Il controllo viene eseguito in base alle regole di rete definite nelle impostazioni di Firewall. Per specificare le regole di rete che devono essere applicate per il monitoraggio dell'attività di rete per tali applicazioni, è necessario selezionare un gruppo di attendibilità.

Come selezionare un gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.



Impostazioni di Prevenzione intrusioni

4. Nel blocco **Diritti dell'applicazione e risorse protette**, fare clic sul pulsante **Modifica**.

5. Per l'impostazione **Gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security**, selezionare il gruppo di attendibilità appropriato.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come selezionare un gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Protezione minacce host → Prevenzione Intrusioni Host**.

5. Per l'impostazione **Gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security**, selezionare il gruppo di attendibilità appropriato.

6. Salvare le modifiche.

Come selezionare un gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.
3. Nel blocco **Gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security**, selezionare il gruppo di attendibilità appropriato.
4. Salvare le modifiche.

Di conseguenza, un'applicazione avviata prima di Kaspersky Endpoint Security verrà inserita nell'altro gruppo di attendibilità. Kaspersky Endpoint Security bloccherà quindi le azioni dell'applicazione a seconda del gruppo di attendibilità.

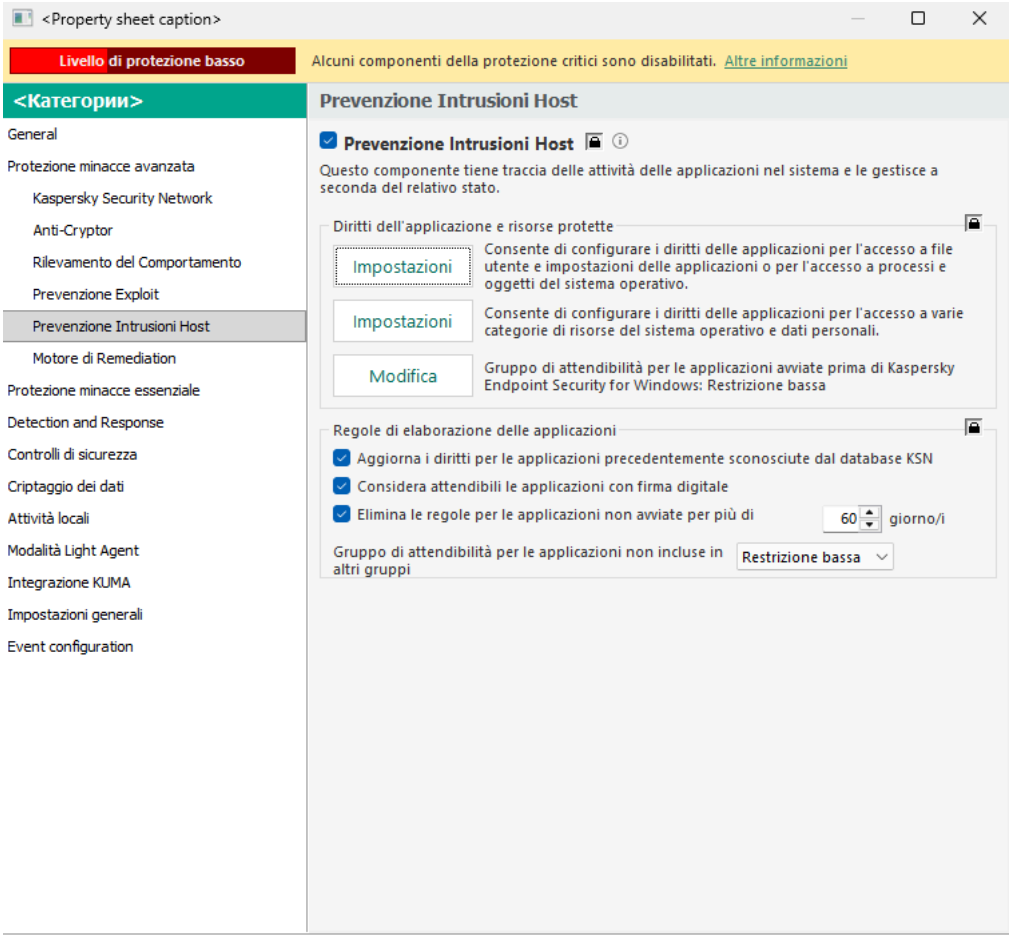
Selezione di un gruppo di attendibilità per le applicazioni sconosciute

Durante il primo avvio di un'applicazione, il componente Prevenzione Intrusioni Host determina il gruppo di attendibilità per l'applicazione. Se non si dispone dell'accesso a Internet o se Kaspersky Security Network non dispone di informazioni sull'applicazione, Kaspersky Endpoint Security collocherà l'applicazione nel gruppo *Restrizione bassa* per impostazione predefinita. Quando vengono rilevate informazioni su un'applicazione precedentemente sconosciuta in KSN, Kaspersky Endpoint Security aggiornerà i diritti dell'applicazione. È quindi possibile modificare manualmente i diritti delle applicazioni.

Come selezionare un gruppo di attendibilità per le applicazioni sconosciute in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.



Impostazioni di Prevenzione intrusioni

4. Nella sezione **Regole di elaborazione delle applicazioni**, utilizzare l'elenco a discesa **Gruppo di attendibilità per le applicazioni non incluse in altri gruppi** per selezionare il gruppo di attendibilità necessario.

   Se la partecipazione a Kaspersky Security Network è abilitata, Kaspersky Endpoint Security invia a KSN una richiesta per conoscere la reputazione di un'applicazione ogni volta che l'applicazione viene avviata. In base alla risposta ricevuta, l'applicazione può essere spostata in un gruppo di attendibilità diverso da quello specificato nelle impostazioni del componente Prevenzione Intrusioni Host.

5. Utilizzare la casella di controllo **Aggiorna i diritti per le applicazioni precedentemente sconosciute dal database KSN** per configurare l'aggiornamento automatico dei diritti delle applicazioni sconosciute.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come selezionare un gruppo di attendibilità per le applicazioni sconosciute in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Protezione minacce host → Prevenzione Intrusioni Host**.

5. Nella sezione **Regole di elaborazione delle applicazioni**, utilizzare l'elenco a discesa **Gruppo di attendibilità per le applicazioni non incluse in altri gruppi** per selezionare il gruppo di attendibilità necessario.

   Se la partecipazione a Kaspersky Security Network è abilitata, Kaspersky Endpoint Security invia a KSN una richiesta per conoscere la reputazione di un'applicazione ogni volta che l'applicazione viene avviata. In base alla risposta ricevuta, l'applicazione può essere spostata in un gruppo di attendibilità diverso da quello specificato nelle impostazioni del componente Prevenzione Intrusioni Host.

6. Utilizzare la casella di controllo **Aggiorna i diritti per le applicazioni precedentemente sconosciute dal database KSN** per configurare l'aggiornamento automatico dei diritti delle applicazioni sconosciute.

7. Salvare le modifiche.

Come selezionare un gruppo di attendibilità per le applicazioni sconosciute nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.

3. Nel blocco **Regole di elaborazione delle applicazioni**, selezionare il gruppo di attendibilità appropriato.

   Se la partecipazione a Kaspersky Security Network è abilitata, Kaspersky Endpoint Security invia a KSN una richiesta per conoscere la reputazione di un'applicazione ogni volta che l'applicazione viene avviata. In base alla risposta ricevuta, l'applicazione può essere spostata in un gruppo di attendibilità diverso da quello specificato nelle impostazioni del componente Prevenzione Intrusioni Host.

4. Utilizzare la casella di controllo **Aggiorna le regole per le applicazioni precedentemente sconosciute da KSN** per configurare l'aggiornamento automatico dei diritti delle applicazioni sconosciute.

5. Salvare le modifiche.

Selezione di un gruppo di attendibilità per le applicazioni firmate digitalmente

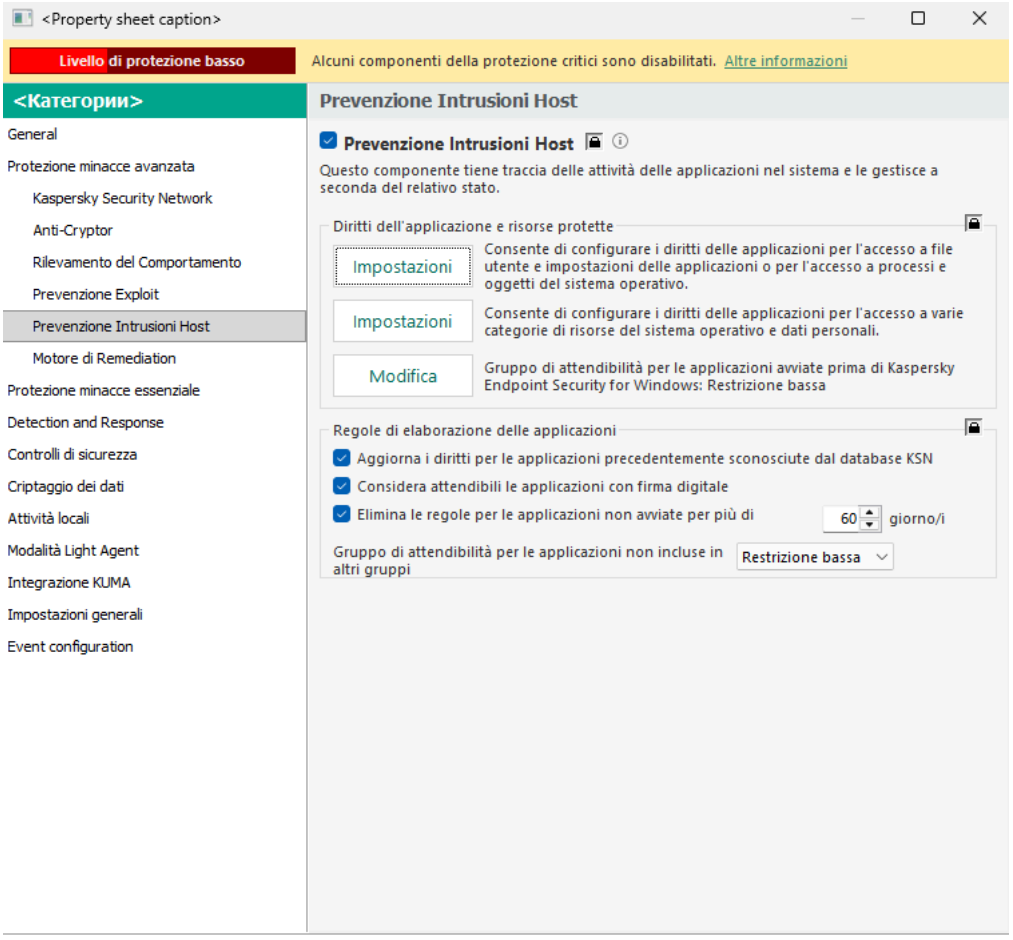
Kaspersky Endpoint Security inserisce sempre le applicazioni firmate da certificati Microsoft o certificati Kaspersky nel gruppo *Attendibili*.

Come selezionare un gruppo di attendibilità per applicazioni firmate digitalmente in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.



Impostazioni di Prevenzione intrusioni

4. Nella sezione **Regole di elaborazione delle applicazioni**, utilizzare la casella di controllo **Considera attendibili le applicazioni con firma digitale** per abilitare o disabilitare l'assegnazione automatica al gruppo di attendibilità per le applicazioni contenenti la firma digitale dei produttori attendibili.

   Per *Produttori attendibili* si intendono i produttori di software inclusi nel gruppo Attendibili da Kaspersky. È inoltre possibile aggiungere manualmente il certificato del produttore all'archivio di certificati di sistema attendibili.

   Se la casella di controllo è deselezionata, il componente Prevenzione Intrusioni Host non considera attendibili le applicazioni dotate di una firma digitale e utilizza altri parametri per determinarne il gruppo di attendibilità.

5. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come selezionare un gruppo di attendibilità per applicazioni con firma digitale in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Protezione minacce host → Prevenzione Intrusioni Host**.

5. Nella sezione **Regole di elaborazione delle applicazioni**, utilizzare la casella di controllo **Considera attendibili le applicazioni con firma digitale** per abilitare o disabilitare l'assegnazione automatica al gruppo di attendibilità per le applicazioni contenenti la firma digitale dei produttori attendibili.

Per *Produttori attendibili* si intendono i produttori di software inclusi nel gruppo Attendibili da Kaspersky. È inoltre possibile aggiungere manualmente il certificato del produttore all'archivio di certificati di sistema attendibili.

Se la casella di controllo è deselezionata, il componente Prevenzione Intrusioni Host non considera attendibili le applicazioni dotate di una firma digitale e utilizza altri parametri per determinarne il gruppo di attendibilità.

6. Salvare le modifiche.

Come selezionare un gruppo di attendibilità per applicazioni con firma digitale nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.
3. Nella sezione **Regole di elaborazione delle applicazioni**, utilizzare la casella di controllo **Considera attendibili le applicazioni con firma digitale** per abilitare o disabilitare l'assegnazione automatica al gruppo di attendibilità per le applicazioni contenenti la firma digitale dei produttori attendibili.

   Per *Produttori attendibili* si intendono i produttori di software inclusi nel gruppo Attendibili da Kaspersky. È inoltre possibile aggiungere manualmente il certificato del produttore all'archivio di certificati di sistema attendibili.

   Se la casella di controllo è deselezionata, il componente Prevenzione Intrusioni Host non considera attendibili le applicazioni dotate di una firma digitale e utilizza altri parametri per determinarne il gruppo di attendibilità.

4. Salvare le modifiche.

Gestione dei diritti delle applicazioni

Per impostazione predefinita, l'attività dell'applicazione viene controllata in base ai diritti dell'applicazione definiti per il gruppo di attendibilità specifico che Kaspersky Endpoint Security ha assegnato all'applicazione al primo avvio. Se necessario, è possibile modificare i diritti delle applicazioni per un intero gruppo di attendibilità, per una singola applicazione o per un gruppo di applicazioni all'interno di un gruppo di attendibilità.

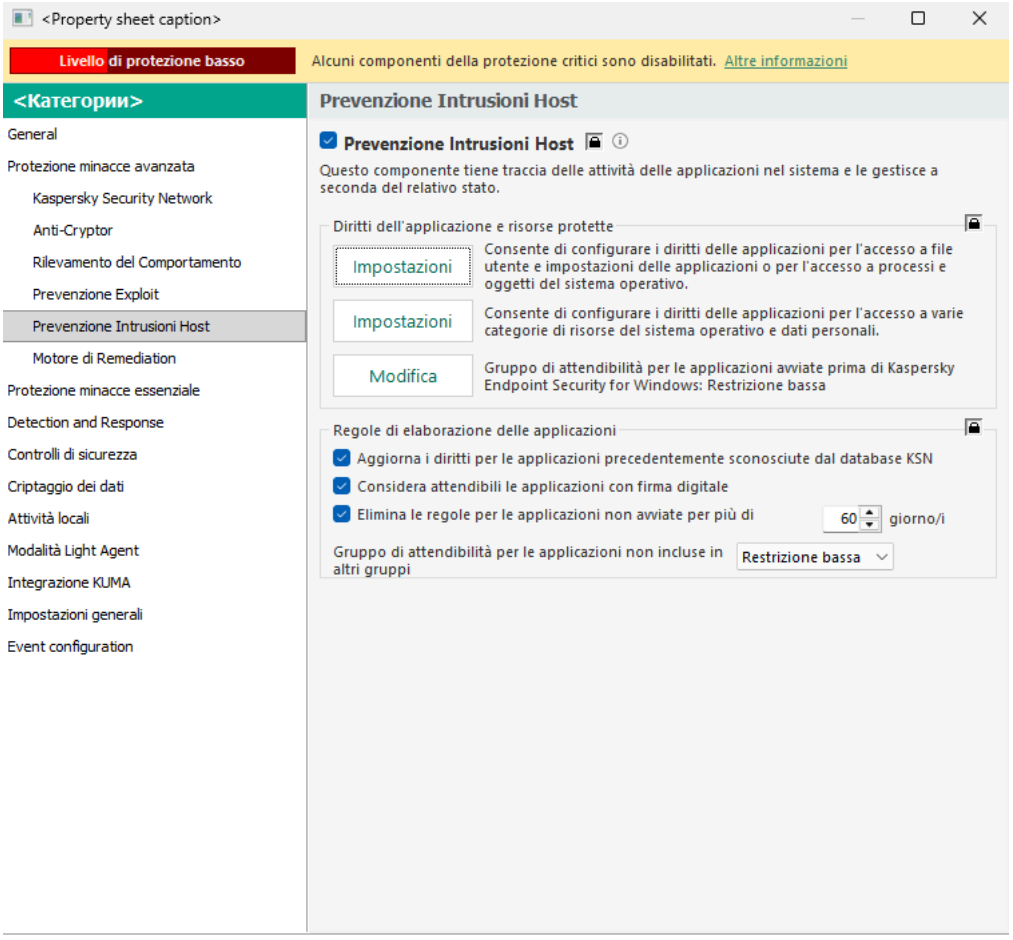
I diritti dell'applicazione definiti manualmente hanno una priorità più elevata rispetto ai diritti dell'applicazione determinati per un gruppo di attendibilità. In altre parole, se i diritti dell'applicazione definiti manualmente differiscono dai diritti dell'applicazione determinati per un gruppo di attendibilità, il componente Prevenzione Intrusioni Host controlla l'attività dell'applicazione in base ai diritti dell'applicazione definiti manualmente.

Le regole create per le applicazioni vengono ereditate dalle applicazioni figlio. Se ad esempio si negano tutte le attività di rete per cmd.exe, verranno negate anche tutte le attività di rete per notepad.exe se questa viene avviata utilizzando cmd.exe. Quando un'applicazione non è figlia dell'applicazione da cui viene eseguita, le regole non vengono ereditate.

Come modificare i diritti delle applicazioni in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.



Impostazioni di Prevenzione intrusioni

4. Nel blocco **Diritti dell'applicazione e risorse protette**, fare clic sul pulsante **Impostazioni**.

   Verranno visualizzati la finestra di configurazione dei diritti dell'applicazione e l'elenco delle risorse protette.

5. Passare alla scheda **Diritti applicazione**.

6. Fare clic su **Aggiungi**.

7. Nella finestra visualizzata, immettere i criteri per cercare l'applicazione di cui di desidera modificare i diritti dell'applicazione.

   È possibile immettere il nome dell'applicazione o il nome del fornitore. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

8. Fare clic su **Aggiorna**.

   Kaspersky Endpoint Security cercherà l'applicazione nell'elenco consolidato di applicazioni installate nei computer gestiti. Kaspersky Endpoint Security mostrerà un elenco di applicazioni che soddisfano i criteri di ricerca.

9. Selezionare l'applicazione desiderata.

10. Nell'elenco a discesa **Aggiungi l'applicazione selezionata al gruppo di attendibilità**, selezionare **Gruppi predefiniti** e fare clic su **OK**.

    L'applicazione verrà aggiunta al gruppo predefinito.

11. Selezionare l'applicazione opportuna, quindi selezionare **Diritti applicazione** dal menu di scelta rapida dell'applicazione.

    Verranno visualizzate le proprietà dell'applicazione.

12. Eseguire una delle seguenti operazioni:

    - Se si desidera modificare i diritti del gruppo di attendibilità che regolano le operazioni con il registro del sistema operativo, i file utente e le impostazioni dell'applicazione, selezionare **File e Registro di sistema**.
    - Se si desidera modificare i diritti del gruppo di attendibilità che regolano l'accesso ai processi e agli oggetti del sistema operativo, selezionare **Diritti**.

    L'attività di rete delle applicazioni è controllata dal componente Firewall mediante le *regole di rete*.

13. Per la risorsa opportuna, nella colonna dell'azione corrispondente, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida e selezionare l'opzione necessaria: **Eredita**, **Consenti** (✓) o **Blocca** (⊘).

14. Se si desidera monitorare l'utilizzo delle risorse del computer, selezionare **Registra eventi** (✓ / ⊘).

    Kaspersky Endpoint Security registrerà le informazioni sul funzionamento del componente Prevenzione Intrusioni Host. I rapporti contengono informazioni sulle operazioni con le risorse del computer eseguite dall'applicazione (consentite o vietate). I rapporti contengono anche informazioni sulle applicazioni che utilizzano ciascuna risorsa.

15. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come modificare i diritti dell'applicazione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Prevenzione Intrusioni Host**.
5. Nella sezione **Diritti dell'applicazione e risorse protette**, fare clic sul collegamento **Diritti dell'applicazione e risorse protette**.

   Verranno visualizzati la finestra di configurazione dei diritti dell'applicazione e l'elenco delle risorse protette.
6. Passare alla scheda **Diritti applicazione**.

   Verrà visualizzato un elenco di gruppi di attendibilità sul lato sinistro della finestra e le relative proprietà sul lato destro.
7. Fare clic su **Aggiungi**.

   Verrà avviata la procedura guidata per l'aggiunta di un'applicazione a un gruppo di attendibilità.
8. Selezionare il gruppo di attendibilità pertinente per l'applicazione.
9. Selezionare il tipo **Applicazione**. Procedere con il passaggio successivo.

   Se si desidera modificare il gruppo di attendibilità per più applicazioni, selezionare il tipo **Gruppo** e definire un nome per il gruppo di applicazioni.

10. Nell'elenco delle applicazioni visualizzato selezionare le applicazioni per le quali si desidera modificare i diritti dell'applicazione.

    Utilizzare un filtro. È possibile immettere il nome dell'applicazione o il nome del fornitore. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

11. Terminare la procedura guidata.

    L'applicazione verrà aggiunta al gruppo di attendibilità.

12. Nella parte sinistra della finestra selezionare l'applicazione attinente.

13. Nella parte destra della finestra, nell'elenco a discesa, eseguire una delle seguenti operazioni:

    - Se si desidera modificare i diritti del gruppo di attendibilità che regolano le operazioni con il registro del sistema operativo, i file utente e le impostazioni dell'applicazione, selezionare **File e Registro di sistema**.
    - Se si desidera modificare i diritti del gruppo di attendibilità che regolano l'accesso ai processi e agli oggetti del sistema operativo, selezionare **Diritti**.

    L'attività di rete delle applicazioni è controllata dal componente Firewall mediante le *regole di rete*.

14. Per la risorsa opportuna, nella colonna dell'azione corrispondente selezionare l'opzione necessaria: **Eredita**, **Consenti** ( ), **Blocca** ( ).

15. Se si desidera monitorare l'utilizzo delle risorse del computer, selezionare **Registra eventi** (/).

    Kaspersky Endpoint Security registrerà le informazioni sul funzionamento del componente Prevenzione Intrusioni Host. I rapporti contengono informazioni sulle operazioni con le risorse del computer eseguite dall'applicazione (consentite o vietate). I rapporti contengono anche informazioni sulle applicazioni che utilizzano ciascuna risorsa.

16. Salvare le modifiche.

Come modificare i diritti dell'applicazione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.

3. Fare clic su **Gestisci applicazioni**.

   Verrà visualizzato l'elenco delle applicazioni installate.

4. Selezionare l'applicazione desiderata.

5. Dal menu di scelta rapida dell'applicazione selezionare **Dettagli e regole**.

   Verranno visualizzate le proprietà dell'applicazione.

6. Eseguire una delle seguenti operazioni:

   - Se si desidera modificare i diritti del gruppo di attendibilità che regolano le operazioni con il registro del sistema operativo, i file utente e le impostazioni dell'applicazione, selezionare **File e Registro di sistema**.
   - Se si desidera modificare i diritti del gruppo di attendibilità che regolano l'accesso ai processi e agli oggetti del sistema operativo, selezionare **Diritti**.

7. Per la risorsa opportuna, nella colonna dell'azione corrispondente, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida e selezionare l'opzione necessaria: **Eredita**, **Consenti** (✓) o **Nega** (!).

8. Se si desidera monitorare l'utilizzo delle risorse del computer, selezionare **Registra eventi** (📊).

   Kaspersky Endpoint Security registrerà le informazioni sul funzionamento del componente Prevenzione Intrusioni Host. I rapporti contengono informazioni sulle operazioni con le risorse del computer eseguite dall'applicazione (consentite o vietate). I rapporti contengono anche informazioni sulle applicazioni che utilizzano ciascuna risorsa.

9. Selezionare la scheda **Esclusioni** e configurare le impostazioni avanzate dell'applicazione (vedere la tabella di seguito).

10. Salvare le modifiche.

Impostazioni avanzate dell'applicazione

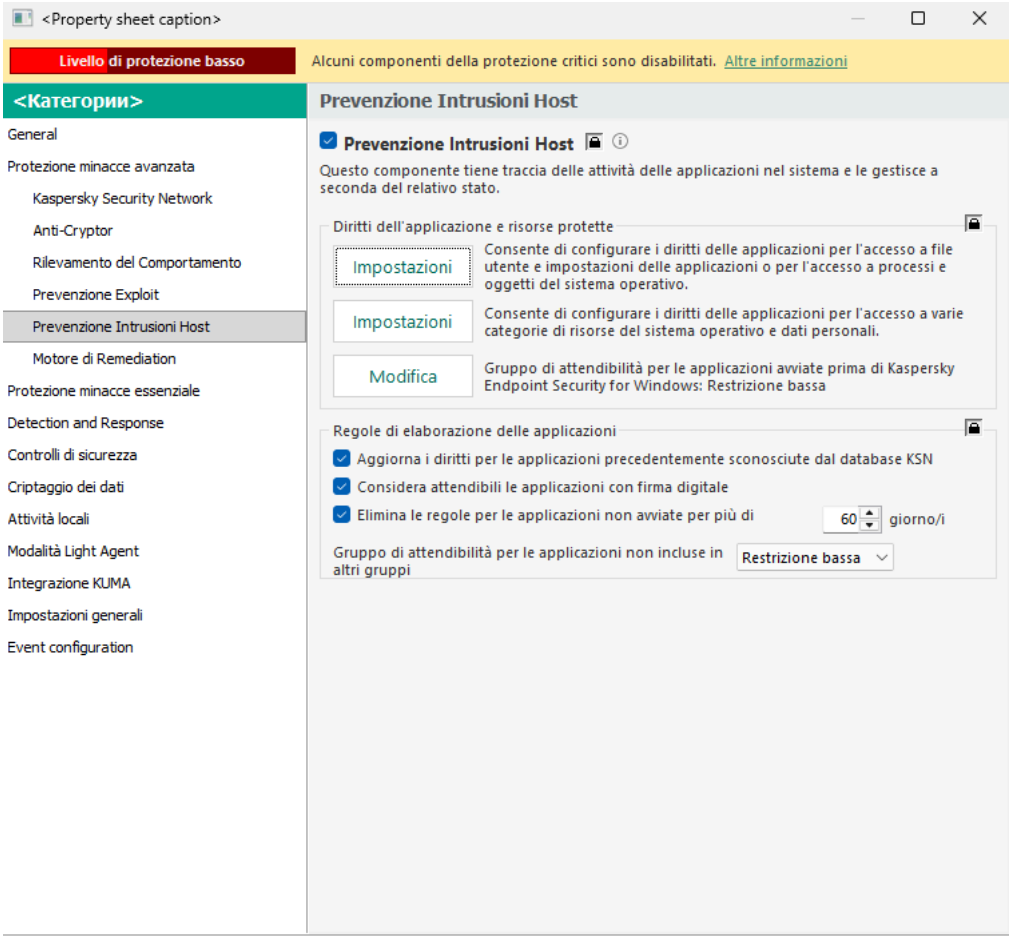
Parametro	Descrizione
Non esaminare i file aperti dall'applicazione	Tutti i file aperti dall'applicazione sono esclusi dalle scansioni di Kaspersky Endpoint Security. Se ad esempio si utilizzano applicazioni per eseguire il backup dei file, questa funzionalità consente di ridurre l'utilizzo di risorse da parte di Kaspersky Endpoint Security.
Non monitorare le attività dell'applicazione	Kaspersky Endpoint Security non monitorerà l'attività file e rete dell'applicazione nel sistema operativo. È possibile configurare il monitoraggio delle attività delle applicazioni per diversi componenti di Kaspersky Endpoint Security: • **Non monitorare i componenti di protezione e controllo**. L'attività dell'applicazione è monitorata dai seguenti componenti: Rilevamento del Comportamento, Prevenzione Exploit, Prevenzione Intrusioni Host, Motore di Remediation e Firewall. • **Non monitorare per Managed Detection and Response ed Endpoint Detection and Response**. Le attività dell'applicazione sono monitorate dall'agente MDR integrato e dall'agente EDR (KATA) integrato. • **Non intercettare l'input interattivo della console per Endpoint Detection and Response**. Kaspersky Endpoint Security non invia dati di telemetria sulla gestione dell'applicazione nella console. I dati di telemetria vengono utilizzati da Kaspersky Anti Targeted Attack Platform (EDR).
Non ereditare le restrizioni dal processo entità superiore (applicazione)	Le restrizioni configurate per il processo principale non verranno applicate da Kaspersky Endpoint Security a un processo secondario. Il processo principale viene avviato da un'applicazione per la quale sono configurati i diritti dell'applicazione (Prevenzione Intrusioni Host) e le regole di rete delle applicazioni (Firewall).
Non monitorare le attività dell'applicazione secondaria	Kaspersky Endpoint Security non monitorerà l'attività file o l'attività di rete delle applicazioni avviate dall'applicazione. È possibile applicare l'esclusione in modo ricorsivo. In modo che l'applicazione non monitori le attività dell'intera catena di applicazioni secondarie.
Consenti interazione con l'interfaccia di Kaspersky Endpoint Security	Auto-difesa di Kaspersky Endpoint Security blocca tutti i tentativi di gestire i servizi delle applicazioni da un computer remoto. Se la casella di controllo è selezionata, l'applicazione di accesso remoto può gestire le impostazioni di Kaspersky Endpoint Security tramite l'interfaccia di Kaspersky Endpoint Security.
Non esaminare il traffico di rete criptato/Non esaminare tutto il traffico	Il traffico di rete avviato dall'applicazione verrà escluso dalle scansioni di Kaspersky Endpoint Security. È possibile escludere tutto il traffico o solo il traffico criptato dalle scansioni. È inoltre possibile escludere singoli indirizzi IP e numeri di porta dalle scansioni. Kaspersky Endpoint Security versione 14.0 o precedente non supporta l'esclusione del traffico di rete se viene specificato un hash per un'applicazione attendibile anziché un percorso.

Protezione delle risorse del sistema operativo e dei dati di identità

Il componente Prevenzione Intrusioni Host gestisce i diritti delle applicazioni per intervenire sulle diverse categorie di risorse del sistema operativo e sui dati personali. Le categorie preimpostate di risorse protette sono state definite dagli specialisti di Kaspersky. Ad esempio, la categoria *Sistema operativo* dispone di una sottocategoria *Impostazioni di avvio* che elenca tutte le chiavi di registro associate all'esecuzione automatica delle applicazioni. Non è possibile modificare o eliminare le categorie preimpostate di risorse protette o le risorse protette in queste categorie.

Come aggiungere una risorsa protetta in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.



Impostazioni di Prevenzione intrusioni

4. Nel blocco **Diritti dell'applicazione e risorse protette**, fare clic sul pulsante **Impostazioni**.

   Verranno visualizzati la finestra di configurazione dei diritti dell'applicazione e l'elenco delle risorse protette.

5. Passare alla scheda **Risorse protette**.

   Verrà visualizzato un elenco di risorse protette nella parte sinistra della finestra e i diritti corrispondenti per l'accesso a tali risorse a seconda del gruppo di attendibilità specifico.

6. Selezionare la categoria di risorse protette alla quale si desidera aggiungere una nuova risorsa protetta.

   Se si desidera aggiungere una sottocategoria, fare clic su **Aggiungi** → **Categoria**.

7. Fare clic sul pulsante **Aggiungi**. Nell'elenco a discesa, selezionare il tipo di risorsa che si desidera aggiungere: **File o cartella** o **Chiave del Registro di sistema**.

8. Nella finestra visualizzata, selezionare un file, una cartella o una chiave del Registro di sistema.

   È possibile visualizzare i diritti delle applicazioni per accedere alle risorse aggiunte. A tale scopo, selezionare una risorsa aggiunta nella parte sinistra della finestra e Kaspersky Endpoint Security mostrerà i diritti di accesso per ciascun gruppo di attendibilità. È inoltre possibile disabilitare il controllo dell'attività delle applicazioni con le risorse utilizzando la casella di controllo accanto a una nuova risorsa.

9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come aggiungere una risorsa protetta in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Protezione minacce host** → **Prevenzione Intrusioni Host**.

5. Nella sezione **Diritti dell'applicazione e risorse protette**, fare clic sul collegamento **Diritti dell'applicazione e risorse protette**.

   Verranno visualizzati la finestra di configurazione dei diritti dell'applicazione e l'elenco delle risorse protette.

6. Passare alla scheda **Risorse protette**.

   Verrà visualizzato un elenco di risorse protette nella parte sinistra della finestra e i diritti corrispondenti per l'accesso a tali risorse a seconda del gruppo di attendibilità specifico.

7. Fare clic su **Aggiungi**.

   Verrà avviata la creazione guidata della nuova risorsa.

8. Nel blocco **Nome gruppo**, selezionare la categoria di risorse protette alla quale si desidera aggiungere una nuova risorsa protetta.

   Se si desidera aggiungere una sottocategoria, selezionare l'opzione **Categoria di risorse protette**.

9. Selezionare il tipo di risorsa che si desidera aggiungere: **File o cartella** o **Chiave del Registro di sistema**.

10. Selezionare un file, una cartella o una chiave di registro.

11. Terminare la procedura guidata.

    È possibile visualizzare i diritti delle applicazioni per accedere alle risorse aggiunte. A tale scopo, selezionare una risorsa aggiunta nella parte sinistra della finestra e Kaspersky Endpoint Security mostrerà i diritti di accesso per ciascun gruppo di attendibilità. È inoltre possibile utilizzare la casella di controllo nella colonna **Stato** per disabilitare il controllo dell'attività delle applicazioni con le risorse.

12. Salvare le modifiche.

Come aggiungere una risorsa protetta nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
3. Fare clic su **Gestisci risorse**.

   Verrà visualizzato l'elenco delle risorse protette.
4. Selezionare la categoria di risorse protette alla quale si desidera aggiungere una nuova risorsa protetta.

   Se si desidera aggiungere una sottocategoria, fare clic su **Aggiungi** → **Categoria**.
5. Fare clic sul pulsante **Aggiungi**. Nell'elenco a discesa, selezionare il tipo di risorsa che si desidera aggiungere: **File o cartella** o **Chiave del Registro di sistema**.
6. Nella finestra visualizzata, selezionare un file, una cartella o una chiave del Registro di sistema.

   È possibile visualizzare i diritti delle applicazioni per accedere alle risorse aggiunte. A tale scopo, selezionare una risorsa aggiunta nella parte sinistra della finestra e Kaspersky Endpoint Security mostrerà un elenco di applicazioni e i diritti di accesso per ciascuna applicazione. È inoltre possibile disabilitare il controllo dell'attività delle applicazioni con le risorse utilizzando il pulsante **Abilita controllo** nella colonna **Stato**.
7. Salvare le modifiche.

Kaspersky Endpoint Security controllerà l'accesso alle risorse del sistema operativo aggiunte e ai dati personali. Kaspersky Endpoint Security controlla l'accesso di un'applicazione alle risorse in base al gruppo di attendibilità assegnato all'applicazione. È inoltre possibile modificare il gruppo di attendibilità di un'applicazione.

Eliminazione delle informazioni relative alle applicazioni inutilizzate

Kaspersky Endpoint Security utilizza i diritti dell'applicazione per controllare le attività delle applicazioni. I diritti dell'applicazione sono determinati in base al relativo gruppo di attendibilità. Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità al primo avvio dell'applicazione. È possibile modificare manualmente il gruppo di attendibilità di un'applicazione. È inoltre possibile configurare manualmente i diritti di una singola applicazione. Kaspersky Endpoint Security memorizza le seguenti informazioni su un'applicazione: gruppo di attendibilità dell'applicazione e diritti dell'applicazione.

Kaspersky Endpoint Security elimina automaticamente le informazioni sulle applicazioni inutilizzate per ottimizzare le risorse del computer. Kaspersky Endpoint Security elimina le informazioni sull'applicazione in base alle seguenti regole:

- Se il gruppo di attendibilità e i diritti di un'applicazione sono stati determinati automaticamente, Kaspersky Endpoint Security elimina le informazioni sull'applicazione dopo 30 giorni. Non è possibile modificare il periodo di archiviazione per le informazioni dell'applicazione o disattivare l'eliminazione automatica.
- Se si inserisce manualmente un'applicazione in un gruppo di attendibilità o si configurano i diritti di accesso, Kaspersky Endpoint Security elimina le informazioni su questa applicazione dopo 60 giorni (periodo di archiviazione predefinito). È possibile modificare il periodo di archiviazione per le informazioni sull'applicazione o disattivare l'eliminazione automatica (vedere le istruzioni di seguito).

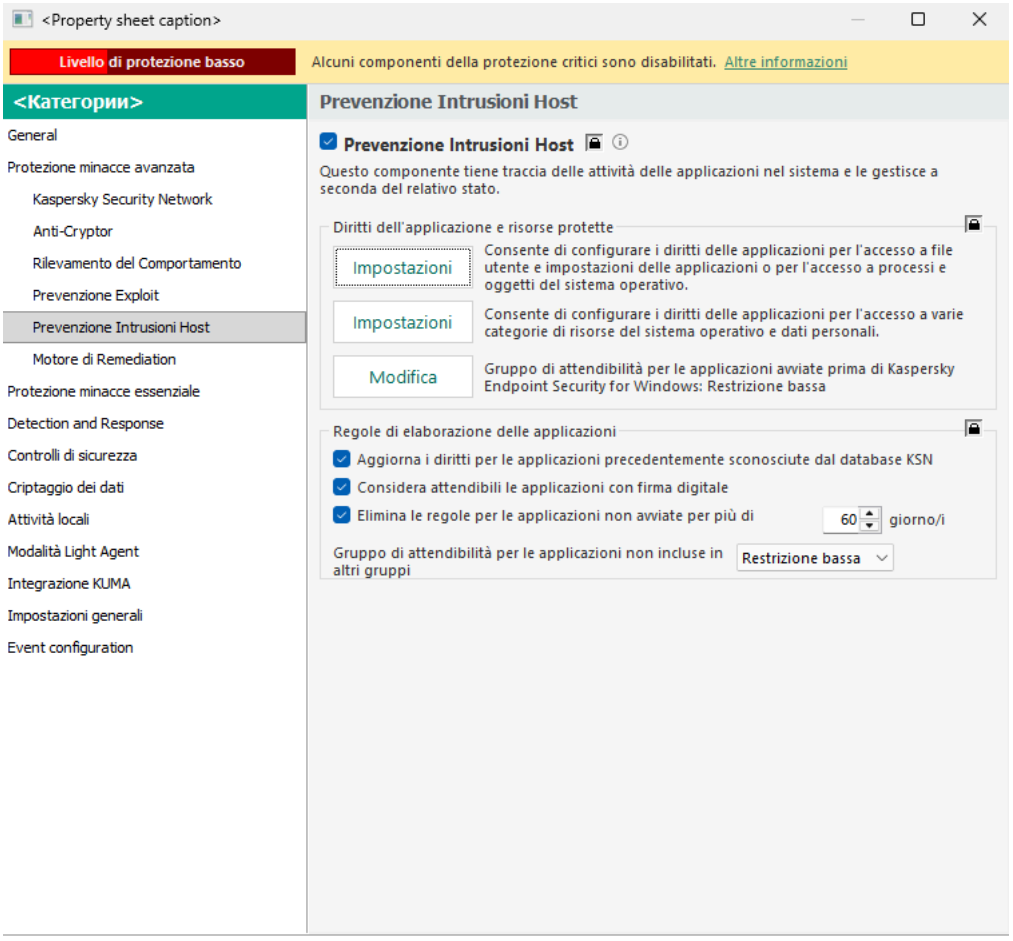
Quando si avvia un'applicazione le cui informazioni sono state eliminate, Kaspersky Endpoint Security analizza l'applicazione come se venisse avviata per la prima volta.

Come configurare l'eliminazione automatica delle informazioni sulle applicazioni inutilizzate in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Prevenzione Intrusioni Host**.



Impostazioni di Prevenzione intrusioni

4. Nel blocco **Regole di elaborazione delle applicazioni**, eseguire una delle seguenti operazioni:

   - Se si desidera configurare l'eliminazione automatica, selezionare la casella di controllo **Elimina le regole per le applicazioni non avviate per più di N giorno/i** e immettere il numero di giorni.

     Le informazioni sulle applicazioni inserite manualmente in un gruppo di attendibilità o i cui diritti di accesso sono stati configurati manualmente verranno eliminate da Kaspersky Endpoint Security dopo il numero di giorni definito. Anche le informazioni sulle applicazioni per cui il gruppo di attendibilità e i diritti dell'applicazione sono stati determinati automaticamente verranno eliminate da Kaspersky Endpoint Security dopo 30 giorni.

   - Se si desidera disattivare l'eliminazione automatica, deselezionare la casella di controllo **Elimina le regole per le applicazioni non avviate per più di N giorno/i**.

     Le informazioni sulle applicazioni inserite manualmente in un gruppo di attendibilità o i cui diritti di accesso sono stati configurati manualmente verranno archiviate da Kaspersky Endpoint Security in modo indefinito, senza limiti relativi al periodo di archiviazione. Kaspersky Endpoint Security eliminerà solo le informazioni sulle applicazioni per cui il gruppo di attendibilità e i diritti dell'applicazione sono stati determinati automaticamente dopo 30 giorni.

5. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare l'eliminazione automatica delle informazioni sulle applicazioni inutilizzate in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Prevenzione Intrusioni Host**.
5. Nel blocco **Regole di elaborazione delle applicazioni**, eseguire una delle seguenti operazioni:

   - Se si desidera configurare l'eliminazione automatica, selezionare la casella di controllo **Elimina le regole per le applicazioni non avviate da più di (giorni, da 1 a 90)** e immettere il numero di giorni.

     Le informazioni sulle applicazioni inserite manualmente in un gruppo di attendibilità o i cui diritti di accesso sono stati configurati manualmente verranno eliminate da Kaspersky Endpoint Security dopo il numero di giorni definito. Anche le informazioni sulle applicazioni per cui il gruppo di attendibilità e i diritti dell'applicazione sono stati determinati automaticamente verranno eliminate da Kaspersky Endpoint Security dopo 30 giorni.

   - Se si desidera disattivare l'eliminazione automatica, deselezionare la casella di controllo **Elimina le regole per le applicazioni non avviate da più di (giorni, da 1 a 90)**.

     Le informazioni sulle applicazioni inserite manualmente in un gruppo di attendibilità o i cui diritti di accesso sono stati configurati manualmente verranno archiviate da Kaspersky Endpoint Security in modo indefinito, senza limiti relativi al periodo di archiviazione. Kaspersky Endpoint Security eliminerà solo le informazioni sulle applicazioni per cui il gruppo di attendibilità e i diritti dell'applicazione sono stati determinati automaticamente dopo 30 giorni.
6. Salvare le modifiche.

Come configurare l'eliminazione automatica delle informazioni sulle applicazioni inutilizzate nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
3. Nel blocco **Regole di elaborazione delle applicazioni**, eseguire una delle seguenti operazioni:

   - Se si desidera configurare l'eliminazione automatica, selezionare la casella di controllo **Elimina le regole per le applicazioni non avviate per più di N giorni (da 1 a 90)** e immettere il numero di giorni.

     Le informazioni sulle applicazioni inserite manualmente in un gruppo di attendibilità o i cui diritti di accesso sono stati configurati manualmente verranno eliminate da Kaspersky Endpoint Security dopo il numero di giorni definito. Anche le informazioni sulle applicazioni per cui il gruppo di attendibilità e i diritti dell'applicazione sono stati determinati automaticamente verranno eliminate da Kaspersky Endpoint Security dopo 30 giorni.

- Se si desidera disattivare l'eliminazione automatica, deselezionare la casella di controllo **Elimina le regole per le applicazioni non avviate per più di N giorni (da 1 a 90)**.

  Le informazioni sulle applicazioni inserite manualmente in un gruppo di attendibilità o i cui diritti di accesso sono stati configurati manualmente verranno archiviate da Kaspersky Endpoint Security in modo indefinito, senza limiti relativi al periodo di archiviazione. Kaspersky Endpoint Security eliminerà solo le informazioni sulle applicazioni per cui il gruppo di attendibilità e i diritti dell'applicazione sono stati determinati automaticamente dopo 30 giorni.

4. Salvare le modifiche.

Monitoraggio di Prevenzione Intrusioni Host

È possibile ricevere rapporti sul funzionamento del componente Prevenzione Intrusioni Host. I rapporti contengono informazioni sulle operazioni con le risorse del computer eseguite dall'applicazione (consentite o vietate). I rapporti contengono anche informazioni sulle applicazioni che utilizzano ciascuna risorsa.

Per monitorare le operazioni di Prevenzione Intrusioni Host, è necessario abilitare la scrittura dei rapporti. È ad esempio possibile abilitare l'inoltro dei rapporti per singole applicazioni nelle impostazioni del componente Prevenzione Intrusioni Host.

Quando si configura il monitoraggio di Prevenzione Intrusioni Host, tenere in considerazione il potenziale carico di rete durante l'inoltro degli eventi a Kaspersky Security Center. È inoltre possibile abilitare il salvataggio dei rapporti solo nel registro locale di Kaspersky Endpoint Security.

Protezione dell'accesso ad audio e video

La funzionalità di protezione del segnale audio e la funzionalità di protezione dell'accesso alla webcam non è supportata nei computer basati su Arm.

I criminali informatici possono utilizzare programmi speciali per tentare di accedere a dispositivi che registrano audio e video (come microfoni o webcam). Kaspersky Endpoint Security controlla quando le applicazioni ricevono un flusso audio o video e protegge i dati da intercettazioni non autorizzate.

Per impostazione predefinita, Kaspersky Endpoint Security consente di ricevere flussi audio e video solo per le applicazioni dal gruppo *Attendibili*. Le applicazioni dai gruppi *Restrizione bassa*, *Restrizione alta* e *Non attendibili* non sono autorizzate a ricevere il flusso audio e il flusso video dai dispositivi. È possibile consentire manualmente alle applicazioni di ricevere il flusso audio e video.

Funzionalità speciali della protezione del flusso audio

La protezione del flusso audio prevede le seguenti caratteristiche speciali:

- Per poter utilizzare questa funzionalità, il componente Prevenzione Intrusioni Host deve essere abilitato.
- Se l'applicazione ha iniziato a ricevere il flusso audio prima dell'avvio del componente Prevenzione Intrusioni Host, Kaspersky Endpoint Security consente all'applicazione di ricevere il flusso audio e non visualizza alcuna notifica.
- Se l'applicazione è stata spostata nel gruppo *Non attendibili* o *Restrizione alta* dopo che l'applicazione ha iniziato a ricevere il flusso audio, Kaspersky Endpoint Security consente all'applicazione di ricevere il flusso audio e non visualizza alcuna notifica.
- Dopo la modifica delle impostazioni per l'accesso dell'applicazione ai dispositivi di registrazione audio (ad esempio se la ricezione del flusso audio da parte dell'applicazione è stata bloccata), è necessario riavviare l'applicazione per impedire che riceva il flusso audio.
- Il controllo dell'accesso al flusso audio dai dispositivi di registrazione audio non dipende dalle impostazioni di accesso alla webcam di un'applicazione.
- Kaspersky Endpoint Security protegge l'accesso solo per i microfoni incorporati e i microfoni esterni. Altri dispositivi di streaming audio non sono supportati.
- Kaspersky Endpoint Security non può garantire la protezione di un flusso audio da dispositivi come fotocamere DSLR, videocamere portatili e action camera.
- Quando si eseguono applicazioni di riproduzione o di registrazione audio e video per la prima volta dopo l'installazione di Kaspersky Endpoint Security, la riproduzione o la registrazione audio e video potrebbero essere interrotte. Questo è necessario per abilitare la funzionalità che controlla l'accesso ai dispositivi di registrazione audio da parte delle applicazioni. Il servizio di sistema che controlla l'hardware audio verrà riavviato quando Kaspersky Endpoint Security viene eseguito per la prima volta.

Funzionalità speciali della protezione dell'accesso alla webcam delle applicazioni

Per la funzionalità di protezione dell'accesso alla webcam tenere presenti le seguenti limitazioni e considerazioni speciali:

- L'applicazione controlla il video e le immagini derivati dall'elaborazione dei dati della webcam.
- L'applicazione controlla il flusso audio se fa parte del flusso video ricevuto della webcam.
- L'applicazione controlla solo le webcam connesse tramite USB o IEEE1394 che sono visualizzate come Dispositivi di acquisizione immagini in Gestione dispositivi di Windows.
- Kaspersky Endpoint Security supporta le seguenti webcam:
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310

- Logitech Webcam C210
- Logitech Webcam Pro 9000
- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

Kaspersky non può garantire il supporto per le webcam che non sono specificate in questo elenco.

Prevenzione Attacchi BadUSB

Alcuni virus modificano il firmware dei dispositivi USB per indurre il sistema operativo a rilevare il dispositivo USB come una tastiera. Di conseguenza, il virus potrebbe eseguire comandi con l'account dell'utente per scaricare malware, ad esempio.

Il componente Prevenzione Attacchi BadUSB impedisce la connessione al computer di dispositivi USB infetti che emulano una tastiera.

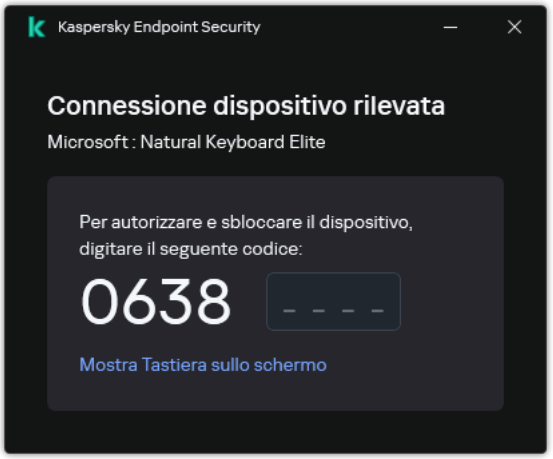
Quando un dispositivo USB viene connesso al computer e identificato dal sistema operativo come una tastiera, l'applicazione richiede all'utente di immettere un codice numerico generato dall'applicazione da questa tastiera o utilizzando Tastiera sullo schermo (vedere la figura di seguito). Questa procedura è denominata autorizzazione della tastiera.

Se il codice è stato immesso correttamente, l'applicazione salva i parametri di identificazione (VID/PID della tastiera e numero della porta a cui è stata connessa) nell'elenco delle tastiere autorizzate. L'autorizzazione delle tastiera non deve essere ripetuta quando la tastiera viene connessa di nuovo o dopo il riavvio del sistema operativo.

> Quando la tastiera autorizzata viene connessa a una diversa porta USB del computer, l'applicazione visualizza nuovamente una richiesta di autorizzazione della tastiera.

Se il codice numerico è stato immesso in modo errato, l'applicazione genera un nuovo codice. È possibile configurare il numero di tentativi di immissione del codice numerico. Se il codice numerico viene immesso più volte in modo errato o la finestra dell'autorizzazione della tastiera viene chiusa (vedere la figura riportata di seguito), l'applicazione blocca l'input dalla tastiera. Quando la durata di blocco del dispositivo USB termina o il sistema operativo viene riavviato, l'applicazione richiede all'utente di eseguire nuovamente l'autorizzazione della tastiera.

L'applicazione consente l'utilizzo di una tastiera autorizzata e blocca una tastiera che non è stata autorizzata.



Autorizzazione tastiera

Abilitazione e disabilitazione di Prevenzione Attacchi BadUSB

I dispositivi USB identificati dal sistema operativo come tastiere e connessi al computer prima dell'installazione del componente Prevenzione Attacchi BadUSB sono considerati autorizzati dopo l'installazione del componente.

Come abilitare o disabilitare il componente Prevenzione Attacchi BadUSB in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Prevenzione Attacchi BadUSB**.
4. Utilizzare la casella di controllo **Prevenzione Attacchi BadUSB** per abilitare o disabilitare il componente.
5. Nel blocco **Autorizzazione dispositivo USB alla connessione**, modificare le impostazioni di sicurezza per l'immissione del codice di autorizzazione:
   - **Numero massimo di tentativi di autorizzazione del dispositivo USB**. Blocco automatico del dispositivo USB se il codice di autorizzazione viene immesso in modo errato per il numero di volte specificato. I valori validi sono compresi tra 1 e 10. Ad esempio, se si consentono cinque tentativi di immissione del codice di autorizzazione, l'applicazione blocca il dispositivo USB dopo il quinto tentativo non riuscito. Kaspersky Endpoint Security mostra la durata del blocco per il dispositivo USB. Trascorso questo tempo, sono di nuovo disponibili cinque tentativi di immissione del codice di autorizzazione.
   - **Timeout al raggiungimento del numero massimo di tentativi (minuti)**. Durata del blocco del dispositivo USB dopo il numero specificato di tentativi non riusciti di immissione del codice di autorizzazione. I valori validi sono compresi tra 1 e 180 (minuti).
6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare il componente Prevenzione Attacchi BadUSB in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Prevenzione Attacchi BadUSB**.
5. Utilizzare l'interruttore **Prevenzione Attacchi BadUSB ABILITATA** per abilitare o disabilitare il componente.
6. Nel blocco **Autorizzazione dei dispositivi USB**, modificare le impostazioni di sicurezza per l'immissione del codice di autorizzazione:

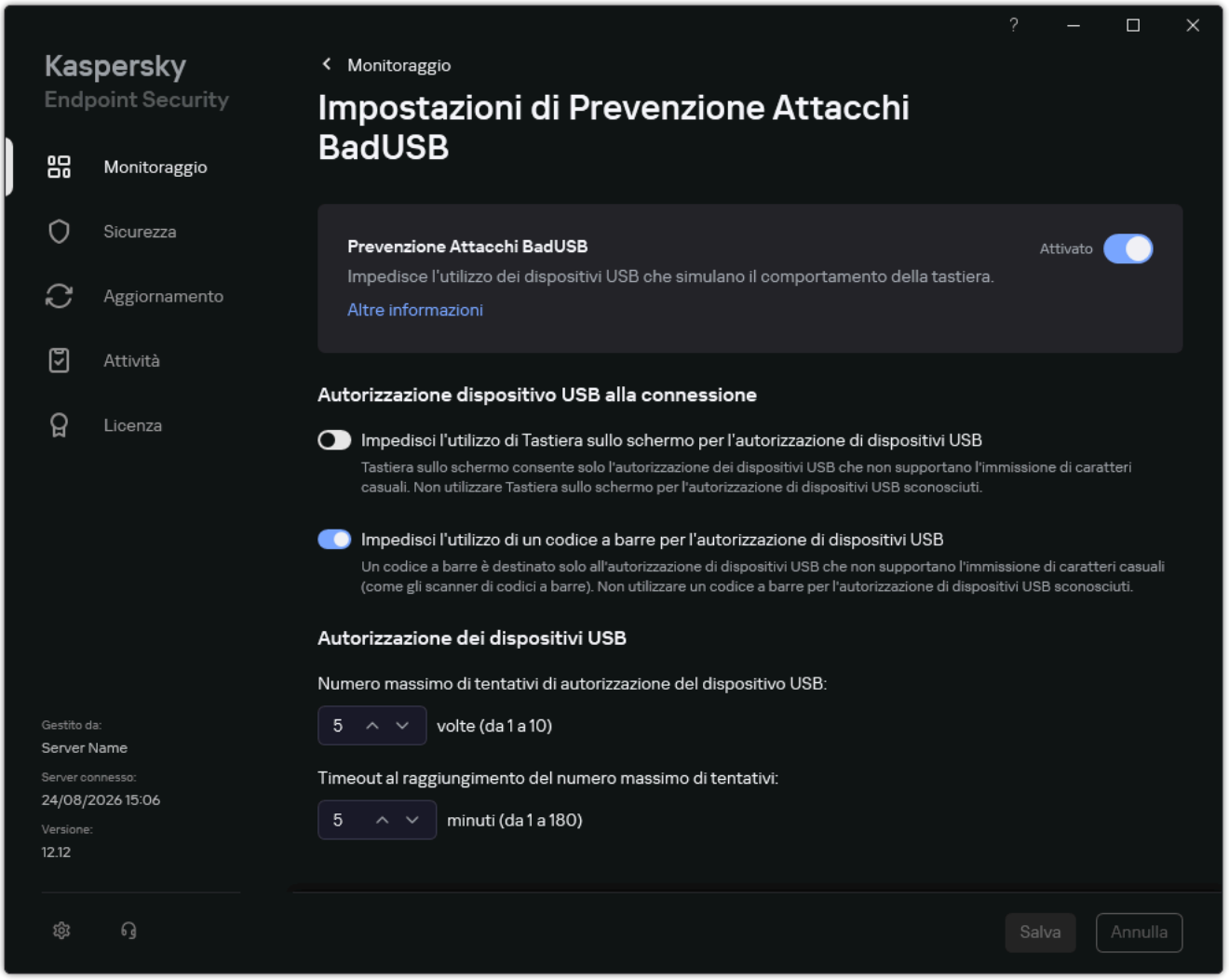
   - **Numero massimo di tentativi di autorizzazione del dispositivo USB**. Blocco automatico del dispositivo USB se il codice di autorizzazione viene immesso in modo errato per il numero di volte specificato. I valori validi sono compresi tra 1 e 10. Ad esempio, se si consentono cinque tentativi di immissione del codice di autorizzazione, l'applicazione blocca il dispositivo USB dopo il quinto tentativo non riuscito. Kaspersky Endpoint Security mostra la durata del blocco per il dispositivo USB. Trascorso questo tempo, sono di nuovo disponibili cinque tentativi di immissione del codice di autorizzazione.

   - **Timeout al raggiungimento del numero massimo di tentativi (min)**. Durata del blocco del dispositivo USB dopo il numero specificato di tentativi non riusciti di immissione del codice di autorizzazione. I valori validi sono compresi tra 1 e 180 (minuti).
7. Salvare le modifiche.

Come abilitare o disabilitare il componente Prevenzione Attacchi BadUSB nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Prevenzione Attacchi BadUSB**.



Impostazioni del componente Prevenzione Attacchi BadUSB

3. Utilizzare l'interruttore **Prevenzione Attacchi BadUSB** per abilitare o disabilitare il componente.

4. Nel blocco **Autorizzazione dispositivo USB alla connessione**, modificare le impostazioni di sicurezza per l'immissione del codice di autorizzazione:

   - **Numero massimo di tentativi di autorizzazione del dispositivo USB**. Blocco automatico del dispositivo USB se il codice di autorizzazione viene immesso in modo errato per il numero di volte specificato. I valori validi sono compresi tra 1 e 10. Ad esempio, se si consentono cinque tentativi di immissione del codice di autorizzazione, l'applicazione blocca il dispositivo USB dopo il quinto tentativo non riuscito. Kaspersky Endpoint Security mostra la durata del blocco per il dispositivo USB. Trascorso questo tempo, sono di nuovo disponibili cinque tentativi di immissione del codice di autorizzazione.

   - **Timeout al raggiungimento del numero massimo di tentativi**. Durata del blocco del dispositivo USB dopo il numero specificato di tentativi non riusciti di immissione del codice di autorizzazione. I valori validi sono compresi tra 1 e 180 (minuti).

5. Salvare le modifiche.

Di conseguenza, se Prevenzione Attacchi BadUSB è abilitato, Kaspersky Endpoint Security richiede l'autorizzazione di un dispositivo USB connesso identificato come tastiera dal sistema operativo. L'utente non può utilizzare una tastiera non autorizzata finché non viene autorizzata.

Utilizzo di Tastiera sullo schermo per l'autorizzazione di dispositivi USB

La Tastiera sullo schermo deve essere utilizzata solo per l'autorizzazione dei dispositivi USB che non supportano l'immissione di caratteri casuali (ad esempio, gli scanner di codici a barre). Non è consigliabile utilizzare la Tastiera sullo schermo per l'autorizzazione di dispositivi USB sconosciuti.

Come consentire o vietare l'utilizzo di Tastiera sullo schermo per l'autorizzazione in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale → Prevenzione Attacchi BadUSB**.
4. Utilizzare la casella di controllo **Impedisci l'utilizzo di Tastiera sullo schermo per l'autorizzazione di dispositivi USB** per bloccare o consentire l'utilizzo di Tastiera sullo schermo per l'autorizzazione.
5. Salvare le modifiche.

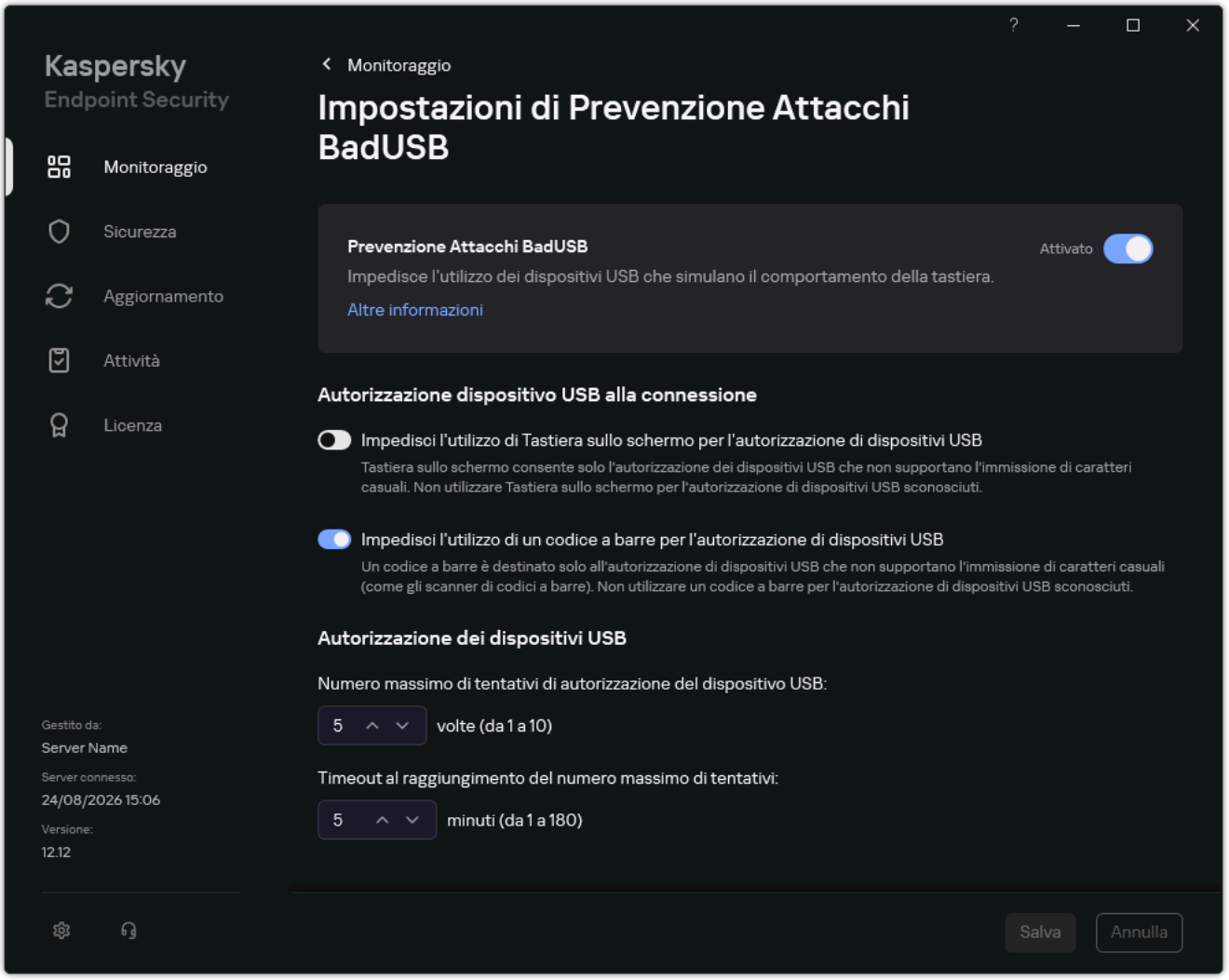
Come consentire o vietare l'utilizzo di Tastiera sullo schermo per l'autorizzazione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host → Prevenzione Attacchi BadUSB**.
5. Utilizzare l'interruttore **Vieta l'utilizzo di Tastiera sullo schermo per l'autorizzazione di dispositivi USB** per bloccare o consentire l'utilizzo di Tastiera sullo schermo per l'autorizzazione.
6. Salvare le modifiche.

Come consentire o vietare l'utilizzo di Tastiera sullo schermo per l'autorizzazione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Prevenzione Attacchi BadUSB**.



Impostazioni del componente Prevenzione Attacchi BadUSB

3. Utilizzare l'interruttore **Impedisci l'utilizzo di Tastiera sullo schermo per l'autorizzazione di dispositivi USB** per bloccare o consentire l'utilizzo di Tastiera sullo schermo per l'autorizzazione.

4. Salvare le modifiche.



Autorizzazione dei dispositivi USB

Autorizzazione del lettore di codici a barre

Quando si collega un lettore di codici a barre al computer, il componente Prevenzione Attacchi BadUSB identifica il dispositivo come dispositivo di input e richiede di eseguire l'autorizzazione. Per autorizzare il lettore di codici a barre, è necessario eseguire la scansione di un codice a barre visualizzato sullo schermo. L'applicazione genera un codice a barre nel formato Code39 supportato dalla maggior parte degli scanner di codici a barre e codici QR.

Kaspersky Endpoint Security supporta anche un altro metodo di autorizzazione dello scanner di codici a barre. Se si utilizzano dispositivi touchscreen, è possibile utilizzare una tastiera su schermo per digitare un codice. A tale scopo, è necessario consentire la tastiera su schermo. Questo metodo è particolarmente utile, ad esempio, nel caso di lettori di codici a barre fissi integrati nei registratori di cassa. Sono vietati altri metodi di autorizzazione dei lettori di codici a barre.

Per impostazione predefinita, l'applicazione non utilizza un codice a barre per l'autorizzazione dei dispositivi USB.

Come abilitare l'autorizzazione dei dispositivi USB tramite codice a barre in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella struttura della console, selezionare **Criteri**.

3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

4. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Prevenzione Attacchi BadUSB**.

5. Utilizzare la casella di controllo **Impedisci l'utilizzo di un codice a barre per l'autorizzazione di dispositivi USB** per bloccare o consentire l'utilizzo dei codici a barre per l'autorizzazione.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare l'autorizzazione dei dispositivi USB tramite codice a barre in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Protezione minacce host** → **Prevenzione Attacchi BadUSB**.

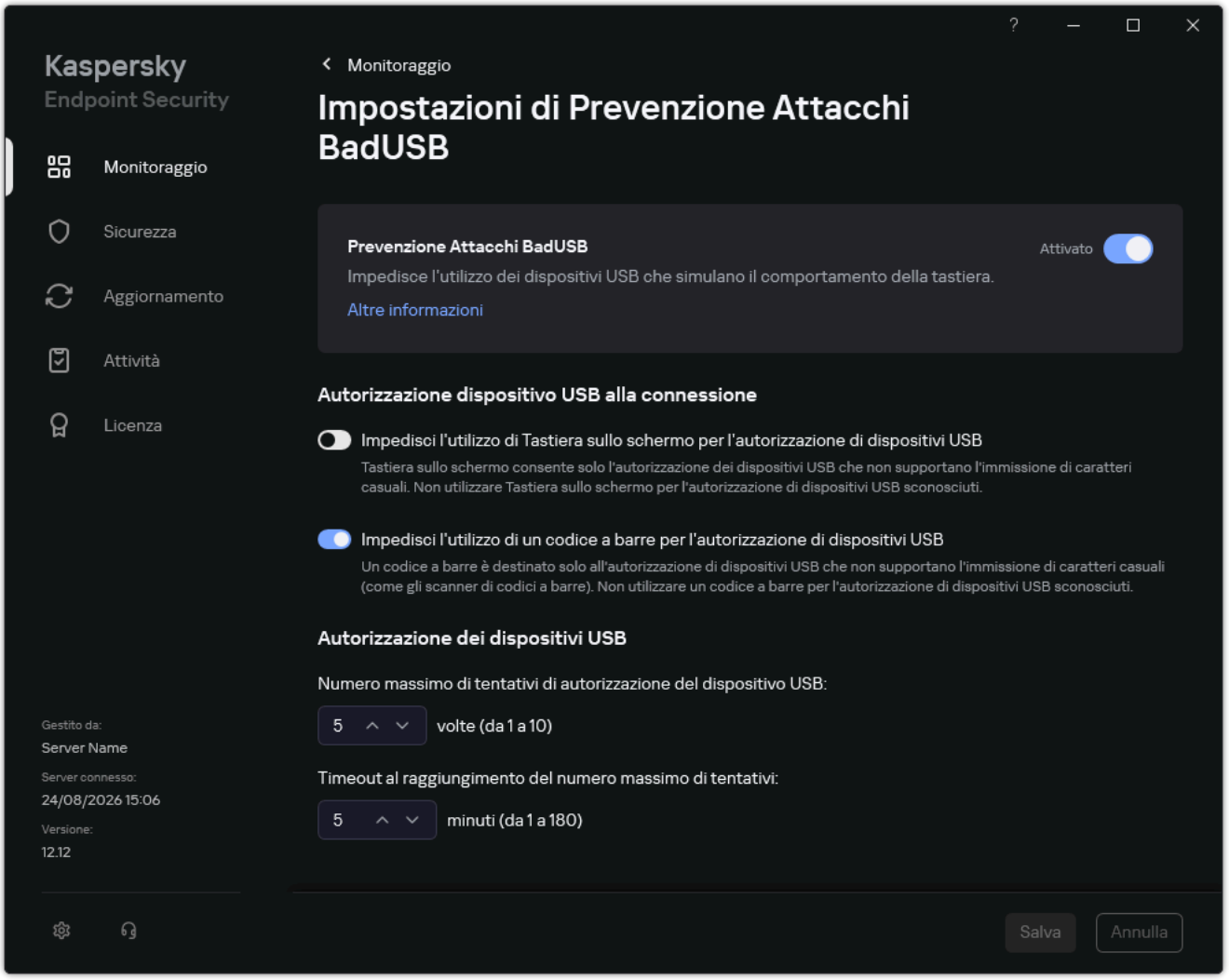
5. Utilizzare l'interruttore **Vieta l'utilizzo di un codice a barre l'autorizzazione di dispositivi USB** per bloccare o consentire l'utilizzo dei codici a barre per l'autorizzazione.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare l'autorizzazione dei dispositivi USB tramite codice a barre nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

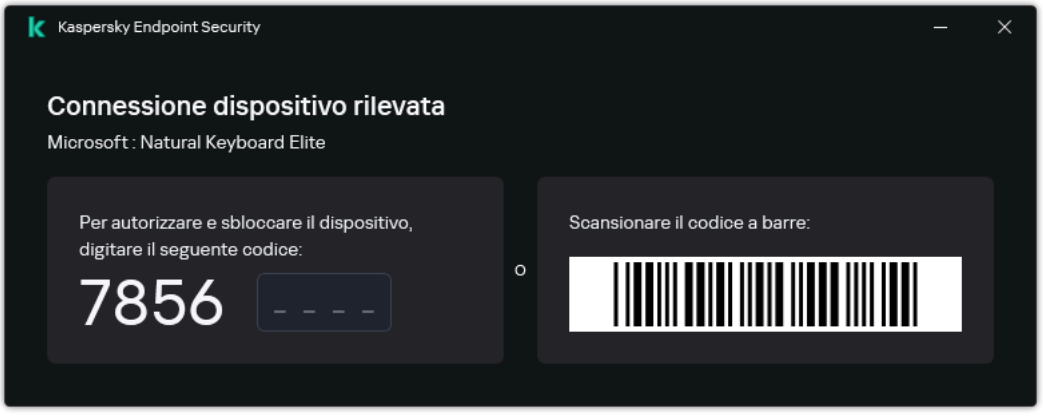
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Prevenzione Attacchi BadUSB**.



Impostazioni del componente Prevenzione Attacchi BadUSB

3. Utilizzare l'interruttore **Impedisci l'utilizzo di un codice a barre per l'autorizzazione di dispositivi USB** per bloccare o consentire l'utilizzo dei codici a barre per l'autorizzazione.

4. Salvare le modifiche.

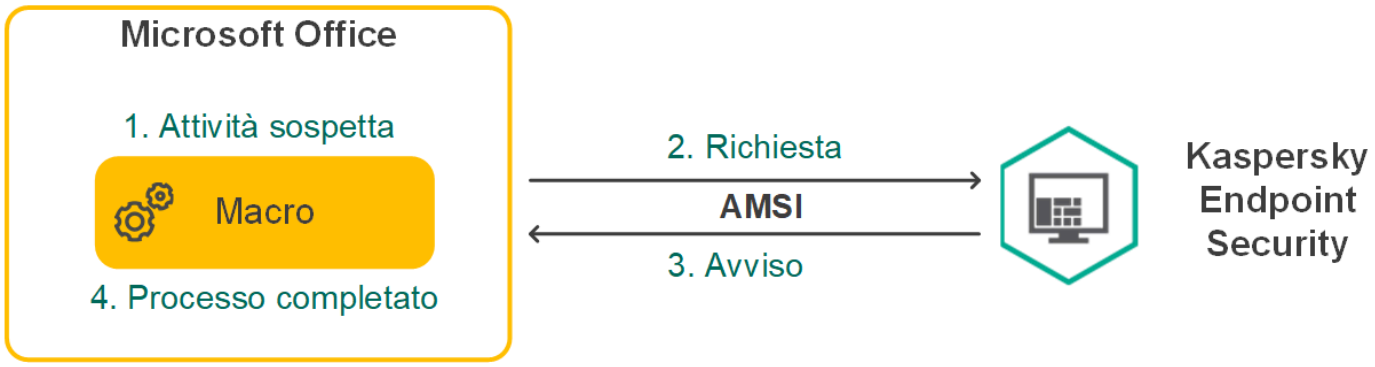


Autorizzazione del lettore di codici a barre

Protezione AMSI

Il componente Protezione AMSI è progettato per il supporto dell'interfaccia AMSI (Antimalware Scan Interface) di Microsoft. *AMSI (Antimalware Scan Interface)* consente ad applicazioni di terzi con il supporto AMSI di inviare oggetti (ad esempio script di PowerShell) a Kaspersky Endpoint Security per un'ulteriore analisi e quindi di ricevere i risultati della scansione di questi oggetti. Tra le applicazioni di terzi possono essere incluse, ad esempio, le applicazioni Microsoft Office (vedere la figura di seguito). Per informazioni dettagliate su AMSI, consultare la documentazione di Microsoft.

Protezione AMSI è solo in grado di rilevare una minaccia e di informare un'applicazione di terzi della minaccia rilevata. Dopo la ricezione di una notifica di minaccia, un'applicazione di terzi non consente azioni dannose (ad esempio arresti).



Esempio di funzionamento del Provider di protezione AMSI

Il componente Protezione AMSI può rifiutare una richiesta da un'applicazione di terzi, ad esempio se questa applicazione supera il numero massimo di richieste all'interno di un intervallo di tempo specificato. Kaspersky Endpoint Security invia le informazioni su una richiesta rifiutata da un'applicazione di terzi ad Administration Server. Il componente Protezione AMSI non nega le richieste provenienti dalle applicazioni di terzi per cui è abilitata l'integrazione continua con il componente Protezione AMSI.

Protezione AMSI è disponibile per i seguenti sistemi operativi per workstation e server:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessione;
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessione;
- Windows Server 2016 Essentials / Standard / Datacenter (inclusa la modalità Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (inclusa la modalità Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (inclusa la modalità Server Core);
- Windows Server 2025 Standard / Datacenter.

Abilitazione e disabilitazione di Protezione AMSI

Per impostazione predefinita, Protezione AMSI è abilitato e funziona nella modalità consigliata da Kaspersky (vedere la tabella di seguito).

Come abilitare o disabilitare Protezione AMSI in Administration Console (MMC)

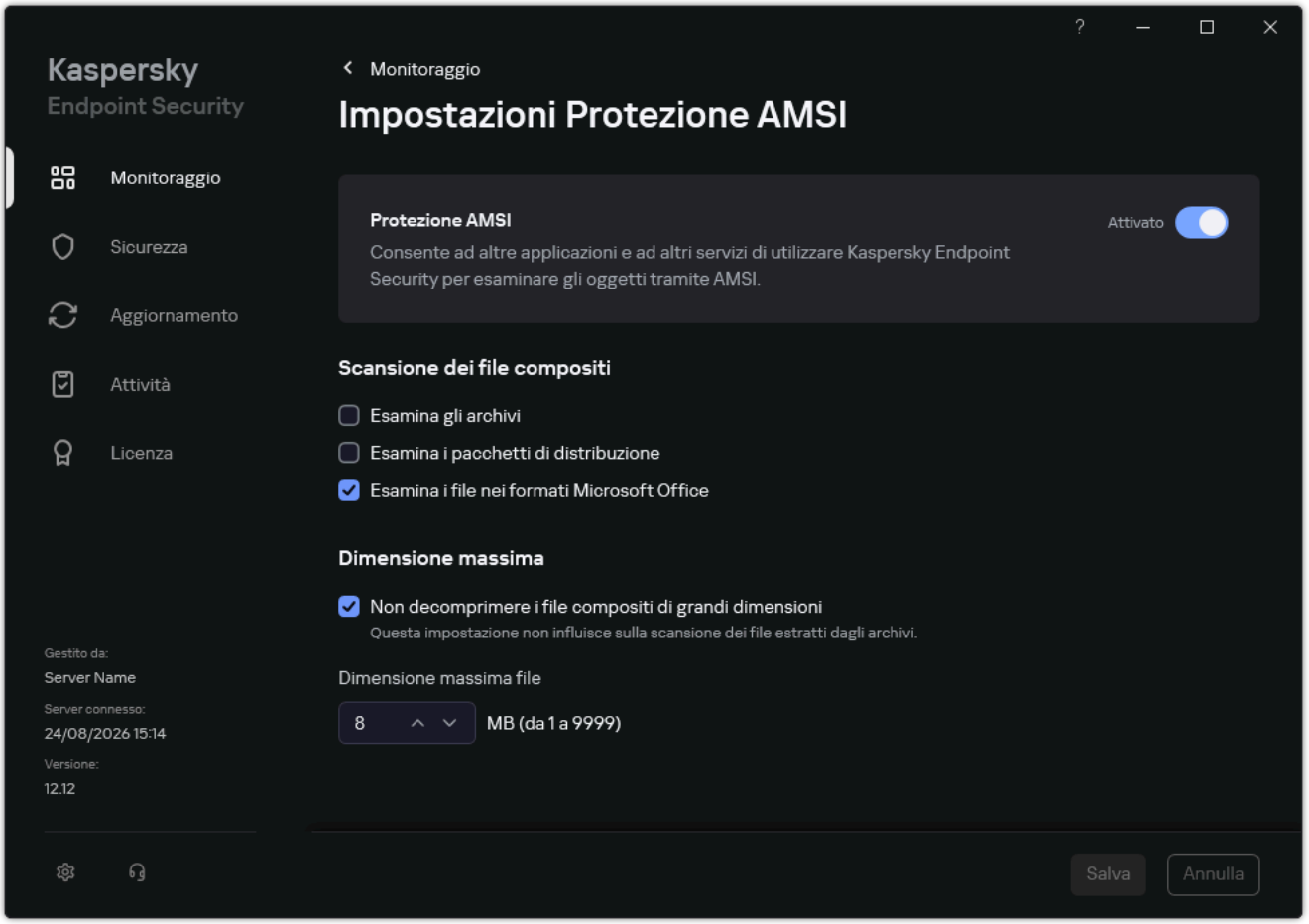
1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Scanner AMSI**.
4. Utilizzare la casella di controllo **Scanner AMSI** per abilitare o disabilitare il componente.
5. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare Protezione AMSI in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Protezione AMSI**.
5. Utilizzare l'interruttore **Protezione AMSI ABILITATA** per abilitare o disabilitare il componente.
6. Salvare le modifiche. Per applicare il criterio nei computer, chiudere i lucchetti .

Come abilitare o disabilitare Protezione AMSI nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione AMSI**.



Impostazioni di protezione AMSI

3. Utilizzare l'interruttore **Protezione AMSI** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Impostazioni di Protezione AMSI consigliate dagli esperti Kaspersky

Parametro	Valore	Descrizione
Esamina gli archivi	**Disattivato**	Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio).
Esamina i pacchetti di distribuzione	**Disattivato**	Scansione dei pacchetti di distribuzione delle applicazioni di terze parti.
Esamina i file nei formati Microsoft Office	**Attivato**	Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE. L'applicazione analizza i file in formato Office di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Non decomprimere i file compositi di grandi dimensioni	**Dimensione massima file 8 MB**	Se la casella di controllo è selezionata, l'applicazione non esegue la scansione dei file compositi se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, l'applicazione esamina i file compositi di qualsiasi dimensione. L'applicazione esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.

Ottimizzazione della scansione dei file tramite Protezione AMSI

È possibile ottimizzare la scansione dei file riducendo il tempo di scansione e aumentando la velocità di esecuzione di Kaspersky Endpoint Security. È possibile selezionare i file compositi di cui è necessaria la scansione: archivi, pacchetti di distribuzione o file in formato Office. È inoltre possibile limitare le dimensioni dei file compositi da acquisire. Il componente Protezione AMSI non decomprimerà i file compositi di dimensioni superiori al valore specificato.

Una tecnica comune per nascondere virus e altro malware è inserirli in file compositi, come gli archivi. Per rilevare i virus e il malware nascosti in questo modo, è necessario decomprimere il file composito, cosa che può rallentare la scansione. È possibile limitare i tipi di file compositi da esaminare, velocizzando la scansione.

Come ottimizzare la scansione dei file da parte di Protezione AMSI in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Scanner AMSI**.
4. Nel blocco **Scansione dei file compositi**, specificare i tipi di file compositi di cui eseguire la scansione: archivi, pacchetto di distribuzione o file nei formati di Office.
5. Nel blocco **Dimensione massima**, eseguire una delle seguenti operazioni:
   - Per impedire al componente Protezione AMSI di decomprimere i file compositi di grandi dimensioni, selezionare la casella di controllo **Non decomprimere i file compositi di grandi dimensioni**, quindi specificare il valore richiesto. Il componente Protezione AMSI non decomprimerà i file compositi di dimensioni superiori al valore specificato.
   - Per consentire al componente Protezione AMSI di decomprimere i file compositi di grandi dimensioni, deselezionare la casella di controllo **Non decomprimere i file compositi di grandi dimensioni**.

   Il componente Protezione AMSI esamina i file di grandi dimensioni estratti dagli archivi, indipendentemente dal fatto che la casella di controllo **Non decomprimere i file compositi di grandi dimensioni** sia selezionata o meno.
6. Salvare le modifiche. Per applicare il criterio nei computer, chiudere i lucchetti .

Come ottimizzare la scansione dei file da parte di Protezione AMSI in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Protezione AMSI**.

5. Nel blocco **Scansione dei file compositi**, specificare i tipi di file compositi di cui eseguire la scansione: archivi, pacchetto di distribuzione o file nei formati di Office.

6. Nel blocco **Ottimizzazione della scansione**, eseguire una delle seguenti operazioni:

   - Per impedire al componente Protezione AMSI di decomprimere i file compositi di grandi dimensioni, selezionare la casella di controllo **Limiti di dimensione abilitati**, quindi specificare il valore richiesto. Il componente Protezione AMSI non decomprimerà i file compositi di dimensioni superiori al valore specificato.

   - Per consentire al componente Protezione AMSI di decomprimere i file compositi di grandi dimensioni, deselezionare la casella di controllo **Limiti di dimensione abilitati**.

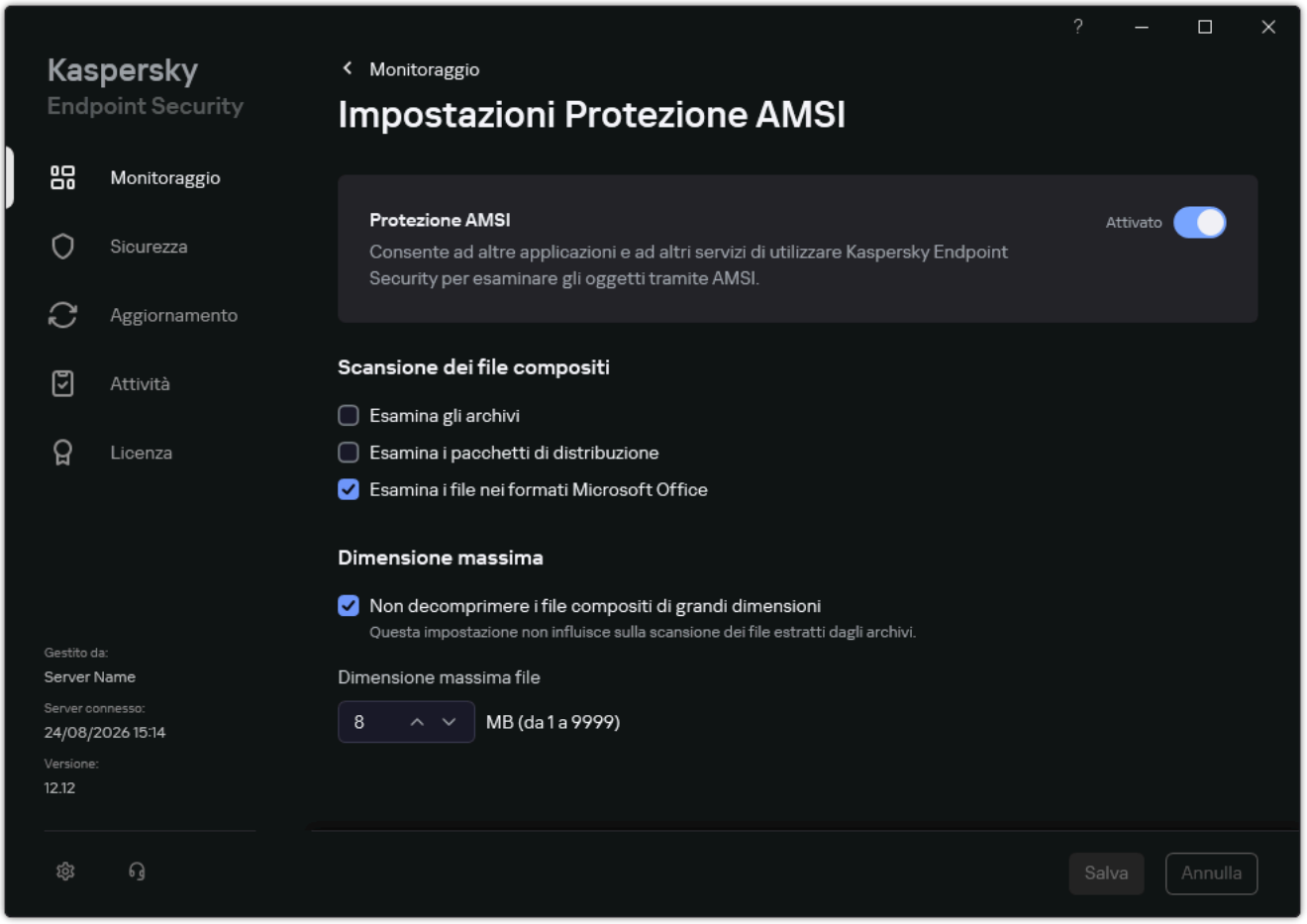
   Il componente Protezione AMSI esamina i file di grandi dimensioni estratti dagli archivi, indipendentemente dal fatto che la casella di controllo **Limiti di dimensione abilitati** sia selezionata o meno.

7. Salvare le modifiche. Per applicare il criterio nei computer, chiudere i lucchetti.

Come ottimizzare la scansione dei file da parte di Protezione AMSI nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione AMSI**.



Impostazioni di protezione AMSI

3. Nel blocco **Scansione dei file compositi**, specificare i tipi di file compositi di cui eseguire la scansione: archivi, pacchetto di distribuzione o file nei formati di Office.

4. Nel blocco **Dimensione massima**, eseguire una delle seguenti operazioni:

   - Per impedire al componente Protezione AMSI di decomprimere i file compositi di grandi dimensioni, selezionare la casella di controllo **Non decomprimere i file compositi di grandi dimensioni**, quindi specificare il valore richiesto. Il componente Protezione AMSI non decomprimerà i file compositi di dimensioni superiori al valore specificato.

   - Per consentire al componente Protezione AMSI di decomprimere i file compositi di grandi dimensioni, deselezionare la casella di controllo **Non decomprimere i file compositi di grandi dimensioni**.

   Il componente Protezione AMSI esamina i file di grandi dimensioni estratti dagli archivi, indipendentemente dal fatto che la casella di controllo **Non decomprimere i file compositi di grandi dimensioni** sia selezionata o meno.

5. Salvare le modifiche.

Protezione minacce Web

Il componente Protezione minacce Web impedisce il download di file dannosi da Internet e blocca inoltre la connessione a siti Web dannosi e di phishing. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica.

Kaspersky Endpoint Security esamina il traffico HTTP, HTTPS e FTP. Kaspersky Endpoint Security esamina URL e indirizzi IP.

Per utilizzare Protezione minacce Web, è necessario completare la configurazione iniziale dell'applicazione:

- Per il monitoraggio del traffico HTTPS, abilitare la scansione delle connessioni criptate (abilitata per impostazione predefinita).

- Selezionare le porte che Kaspersky Endpoint Security deve monitorare (per impostazione predefinita, l'applicazione monitora tutte le porte).

- Selezionare le applicazioni il cui traffico si desidera venga monitorato da Kaspersky Endpoint Security. La maggior parte dei browser è già presente nell'elenco delle applicazioni consigliate da Kaspersky. Se il browser non è presente nell'elenco, aggiungerlo manualmente.

- Si consiglia di inoculare lo script per l'interazione con le pagine Web nel traffico Web (per impostazione predefinita, l'inserimento dello script è disabilitato). Questo script consente la registrazione degli eventi di Protezione minacce Web per il registro eventi dell'applicazione, il registro eventi del sistema operativo e i rapporti.

Quando un utente tenta di aprire un sito Web dannoso o di phishing, Kaspersky Endpoint Security bloccherà l'accesso e mostrerà un avviso.

Abilitazione e disabilitazione di Protezione minacce web

Il componente Protezione minacce web è abilitato per impostazione predefinita e viene eseguito nella modalità consigliata dagli esperti Kaspersky. Per Protezione minacce Web, l'applicazione può applicare diversi gruppi di impostazioni. I gruppi di impostazioni archiviate nell'applicazione sono denominati *livelli di protezione*: **Alto**, **Consigliato**, **Basso**. Le impostazioni del livello di sicurezza del traffico Web **Consigliato** sono considerate le impostazioni ottimali consigliate dagli esperti di Kaspersky (vedere la tabella di seguito). È possibile selezionare uno dei livelli predefiniti di protezione per il traffico Web ricevuto e trasmesso tramite i protocolli HTTP e FTP oppure configurare un livello personalizzato di protezione del traffico Web. Se sono state modificate le impostazioni del livello di sicurezza del traffico Web, è possibile ripristinare in qualsiasi momento le impostazioni consigliate.

È possibile selezionare o configurare il livello di sicurezza solo in Administration Console (MMC) o nell'interfaccia locale dell'applicazione. Non è possibile selezionare o configurare il livello di sicurezza in Web Console o Cloud Console.

Come abilitare o disabilitare il componente Protezione minacce Web in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale → Protezione minacce Web**.
4. Utilizzare la casella di controllo **Protezione minacce Web** per abilitare o disabilitare il componente.
5. Se il componente è stato abilitato, eseguire una delle seguenti operazioni nel blocco **Livello di sicurezza**:
   - Se si desidera applicare uno dei livelli di protezione preimpostati, selezionarlo con il dispositivo di scorrimento:
     - **Alto**. Il livello di sicurezza in cui il componente Protezione minacce Web esegue la massima scansione del traffico Web ricevuto dal computer tramite i HTTP e FTP. Protezione minacce Web esegue la scansione dettagliata di tutti gli oggetti del traffico Web, utilizzando l'intero set di database dell'applicazione, ed esegue l'analisi euristica più approfondita possibile.
     - **Consigliato**. Questo livello di sicurezza assicura l'equilibrio ottimale tra le prestazioni dell'applicazione e la sicurezza del traffico Web. Il componente Protezione minacce Web esegue l'analisi euristica al livello di scansione Media. Questo livello di sicurezza del traffico Web è consigliato dagli specialisti di Kaspersky. I valori delle impostazioni per il livello di sicurezza consigliato sono specificati nella tabella seguente.
     - **Basso**. Le impostazioni di questo livello di sicurezza assicurano la massima velocità di scansione del traffico Web. Il componente Protezione minacce Web esegue l'analisi euristica al livello di scansione superficiale.
   - Se si desidera configurare un livello di sicurezza personalizzato, fare clic sul pulsante **Impostazioni** e definire le proprie impostazioni del componente (vedere la tabella seguente).

     È possibile ripristinare i valori dei livelli di sicurezza preimpostati facendo clic sul pulsante **Predefinito**.

6. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi del traffico Web:

   - **Blocca**. Se questa opzione è selezionata e viene rilevato un oggetto infetto nel traffico Web, il componente Protezione minacce Web blocca l'accesso all'oggetto e visualizza un messaggio nel browser.

   - **Informa**. Se questa opzione è selezionata e un oggetto infetto viene rilevato nel traffico Web, Kaspersky Endpoint Security consente il download di questo oggetto nel computer ma aggiunge informazioni sull'oggetto infetto all'elenco delle minacce attive.

7. Salvare le modifiche.

Come abilitare o disabilitare il componente Protezione minacce Web in Web Console

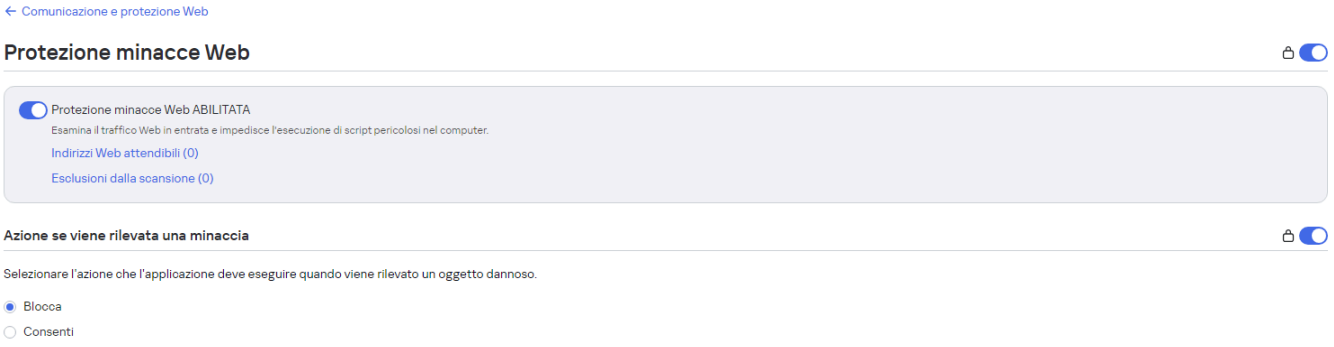
1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Comunicazione e protezione Web** → **Protezione minacce Web**.



Impostazioni di Protezione minacce Web

5. Utilizzare l'interruttore **Protezione minacce Web ABILITATA** per abilitare o disabilitare il componente.

6. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi del traffico Web:

   - **Blocca**. Se questa opzione è selezionata e viene rilevato un oggetto infetto nel traffico Web, il componente Protezione minacce Web blocca l'accesso all'oggetto e visualizza un messaggio nel browser.

   - **Consenti, informa o richiedi azione (dipende dal sistema operativo)**. Se questa opzione è selezionata e un oggetto infetto viene rilevato nel traffico Web, Kaspersky Endpoint Security consente il download di questo oggetto nel computer ma aggiunge informazioni sull'oggetto infetto all'elenco delle minacce attive.

7. Se necessario, creare un elenco di indirizzi Web attendibili.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare il componente Protezione minacce Web

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.

3. Utilizzare l'interruttore **Protezione minacce Web** per abilitare o disabilitare il componente.

4. Se il componente è stato abilitato, eseguire una delle seguenti operazioni nel blocco **Livello di sicurezza**:

   - Se si desidera applicare uno dei livelli di protezione preimpostati, selezionarlo con il dispositivo di scorrimento:

     - **Alto**. Il livello di sicurezza in cui il componente Protezione minacce Web esegue la massima scansione del traffico Web ricevuto dal computer tramite i HTTP e FTP. Protezione minacce Web esegue la scansione dettagliata di tutti gli oggetti del traffico Web, utilizzando l'intero set di database dell'applicazione, ed esegue l'analisi euristica più approfondita possibile.

     - **Consigliato**. Questo livello di sicurezza assicura l'equilibrio ottimale tra le prestazioni dell'applicazione e la sicurezza del traffico Web. Il componente Protezione minacce Web esegue l'analisi euristica al livello di scansione Media. Questo livello di sicurezza del traffico Web è consigliato dagli specialisti di Kaspersky. I valori delle impostazioni per il livello di sicurezza consigliato sono specificati nella tabella seguente.

     - **Basso**. Le impostazioni di questo livello di sicurezza assicurano la massima velocità di scansione del traffico Web. Il componente Protezione minacce Web esegue l'analisi euristica al livello di scansione superficiale.

   - Se si desidera configurare un livello di sicurezza personalizzato, fare clic sul pulsante **Impostazioni avanzate** e definire le proprie impostazioni del componente (vedere la tabella seguente).

     È possibile ripristinare i valori dei livelli di sicurezza preimpostati facendo clic sul pulsante **Ripristina il livello di sicurezza consigliato**.

5. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi del traffico Web:

   - **Blocca**. Se questa opzione è selezionata e viene rilevato un oggetto infetto nel traffico Web, il componente Protezione minacce Web blocca l'accesso all'oggetto e visualizza un messaggio nel browser.

   - **Informa**. Se questa opzione è selezionata e un oggetto infetto viene rilevato nel traffico Web, Kaspersky Endpoint Security consente il download di questo oggetto nel computer ma aggiunge informazioni sull'oggetto infetto all'elenco delle minacce attive.

6. Salvare le modifiche.

Impostazioni di Protezione minacce Web consigliate dagli esperti Kaspersky (livello di sicurezza consigliato)

Parametro	Valore	Descrizione
Verifica l'indirizzo Web a fronte del database degli indirizzi Web dannosi	**Attivato**	La scansione dei collegamenti per determinare se sono inclusi nel database degli indirizzi Web dannosi consente di tenere traccia dei siti Web che sono stati aggiunti alla lista vietati. Il database degli indirizzi Web dannosi è gestito da Kaspersky è incluso nel pacchetto di installazione dell'applicazione e viene aggiornato durante gli aggiornamenti del database di Kaspersky Endpoint Security.
Verifica l'indirizzo Web a fronte del database degli indirizzi Web di phishing	**Attivato**	Il database degli indirizzi Web di phishing include gli indirizzi Web dei siti Web attualmente noti utilizzati per generare attacchi di phishing. Kaspersky integra questo database dei collegamenti di phishing con gli indirizzi ottenuti dall'organizzazione internazionale nota come Anti-Phishing Working Group. Il database degli indirizzi di phishing è incluso nel pacchetto di installazione dell'applicazione e viene integrato dagli aggiornamenti del database di Kaspersky Endpoint Security.
Usa l'analisi euristica (Protezione minacce Web)	**Media**	Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto. Quando il traffico Web viene esaminato alla ricerca di virus e altre applicazioni che costituiscono una minaccia, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.

Parametro	Valore	Descrizione
Usa l'analisi euristica (Anti-Phishing)	**Attivato**	Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto.
Azione se viene rilevata una minaccia	**Blocca**	Se questa opzione è selezionata e viene rilevato un oggetto infetto nel traffico Web, il componente Protezione minacce Web blocca l'accesso all'oggetto e visualizza un messaggio nel browser.

Configurazione dei metodi di rilevamento degli indirizzi Web dannosi

Protezione minacce Web rileva gli indirizzi Web dannosi utilizzando il database anti-virus, il servizio cloud di Kaspersky Security Network e l'analisi euristica.

È possibile selezionare i metodi di rilevamento degli indirizzi Web dannosi solo in Administration Console (MMC) o nell'interfaccia locale dell'applicazione. Non è possibile selezionare i metodi di rilevamento di indirizzi Web dannosi in Web Console o Cloud Console. L'opzione predefinita controlla gli indirizzi Web rispetto al database di indirizzi dannosi con l'analisi euristica (scansione media).

Scansione tramite il database di indirizzi dannosi

La scansione dei collegamenti per determinare se sono inclusi nel database degli indirizzi Web dannosi consente di tenere traccia dei siti Web che sono stati aggiunti alla lista vietati. Il database degli indirizzi Web dannosi è gestito da Kaspersky è incluso nel pacchetto di installazione dell'applicazione e viene aggiornato durante gli aggiornamenti del database di Kaspersky Endpoint Security.

Kaspersky Endpoint Security esamina tutti i collegamenti per determinare se sono elencati nei database degli indirizzi Web dannosi. Le impostazioni di scansione della connessione sicura dell'applicazione non influiscono sulla funzionalità di scansione dei collegamenti. In altre parole, se la scansione delle connessioni criptate è disabilitata, Kaspersky Endpoint Security controlla i collegamenti a fronte dei database degli indirizzi Web dannosi anche se il traffico di rete viene trasmesso tramite una connessione criptata.

Come abilitare o disabilitare il controllo degli indirizzi Web rispetto al database di indirizzi Web dannosi utilizzando Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.
4. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nel blocco **Metodi di scansione**, selezionare o deselezionare **Verifica l'indirizzo Web a fronte del database degli indirizzi Web dannosi** per abilitare o disabilitare il controllo degli indirizzi rispetto al database di indirizzi Web dannosi.

6. Salvare le modifiche.

Come abilitare o disabilitare il controllo degli indirizzi rispetto al database di indirizzi dannosi nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.

3. Fare clic su **Impostazioni avanzate**.

4. Nel blocco **Metodi di scansione**, selezionare o deselezionare **Verifica l'indirizzo Web a fronte del database degli indirizzi Web dannosi** per abilitare o disabilitare il controllo degli indirizzi rispetto al database di indirizzi Web dannosi.

5. Salvare le modifiche.

Analisi euristica

Durante l'analisi euristica, Kaspersky Endpoint Security analizza l'attività delle applicazioni nel sistema operativo. L'analisi euristica consente di rilevare le minacce per cui al momento non sono presenti record nei database di Kaspersky Endpoint Security.

Quando il traffico Web viene esaminato alla ricerca di virus e altre applicazioni che costituiscono una minaccia, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.

Come abilitare o disabilitare l'uso dell'analisi euristica in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.

4. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nella sezione **Metodi di scansione**, selezionare la casella di controllo **Usa l'analisi euristica** se si desidera che l'applicazione utilizzi l'analisi euristica durante la scansione del traffico Web alla ricerca di virus e malware.

6. Utilizzare il dispositivo di scorrimento per impostare il livello di analisi euristica: **superficiale**, **media** o **approfondita**.

   Quando il traffico Web viene esaminato alla ricerca di virus e altre applicazioni che costituiscono una minaccia, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.

7. Salvare le modifiche.

Come abilitare o disabilitare l'uso dell'analisi euristica nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.

3. Fare clic su **Impostazioni avanzate**.

4. Nella sezione **Metodi di scansione** selezionare la casella di controllo **Usa l'analisi euristica** se si desidera che l'applicazione utilizzi l'analisi euristica durante la scansione del traffico Web alla ricerca di virus e malware.

   Quando il traffico Web viene esaminato alla ricerca di virus e altre applicazioni che costituiscono una minaccia, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.

5. Salvare le modifiche.

Anti-Phishing

Protezione minacce Web controlla i collegamenti per verificare se appartengono a indirizzi Web di phishing. In questo modo, è possibile prevenire gli *attacchi di phishing*. Un attacco di phishing può ad esempio presentarsi sotto forma di un messaggio e-mail presumibilmente ricevuto dalla propria banca con un collegamento al sito Web ufficiale della banca. Facendo clic sul collegamento, si viene indirizzati a una copia identica del sito Web della banca, che visualizza addirittura l'indirizzo effettivo nel browser, anche se in realtà si tratta di un sito falso. Da questo momento, tutte le operazioni eseguite nel sito vengono registrate e possono essere utilizzate per prelevare denaro dal conto dell'utente.

Poiché i collegamenti ai siti Web di phishing possono essere ricevuti non solo tramite messaggio e-mail ma anche da altre origini, come le applicazioni di chat, il componente Protezione minacce web monitora i tentativi di accesso a un sito Web di phishing a livello di scansione del traffico Web e blocca l'accesso a tali siti Web. Gli elenchi delle URL di phishing sono inclusi nel kit di distribuzione di Kaspersky Endpoint Security.

È possibile configurare Anti-Phishing solo in Administration Console (MMC) o nell'interfaccia locale dell'applicazione. Non è possibile configurare Anti-Phishing in Web Console o Cloud Console. Per impostazione predefinita, Anti-Phishing con analisi euristica è abilitato.

Come abilitare o disabilitare Anti-Phishing in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale → Protezione minacce Web**.
4. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nel blocco **Impostazioni di Anti-Phishing**, selezionare o deselezionare la casella di controllo **Verifica l'indirizzo Web a fronte del database degli indirizzi Web di phishing** per abilitare e disabilitare Anti-Phishing.

   Il database degli indirizzi Web di phishing include gli indirizzi Web dei siti Web attualmente noti utilizzati per generare attacchi di phishing. Kaspersky integra questo database dei collegamenti di phishing con gli indirizzi ottenuti dall'organizzazione internazionale nota come Anti-Phishing Working Group. Il database degli indirizzi di phishing è incluso nel pacchetto di installazione dell'applicazione e viene integrato dagli aggiornamenti del database di Kaspersky Endpoint Security.
6. Selezionare la casella di controllo **Usa l'analisi euristica** se si desidera che l'applicazione utilizzi l'analisi euristica durante la scansione delle pagine Web alla ricerca dei collegamenti di phishing.

   Durante l'analisi euristica, Kaspersky Endpoint Security analizza l'attività delle applicazioni nel sistema operativo. L'analisi euristica consente di rilevare le minacce per cui al momento non sono presenti record nei database di Kaspersky Endpoint Security.

   Per esaminare i collegamenti, oltre al database anti-virus e all'analisi euristica, è possibile utilizzare i database di reputazione Kaspersky Security Network.
7. Salvare le modifiche.

Come abilitare o disabilitare Anti-Phishing nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce Web**.
3. Fare clic su **Impostazioni avanzate**.
4. Se si desidera che il componente Protezione minacce Web controlli i collegamenti a fronte dei database degli indirizzi Web di phishing, selezionare la casella di controllo **Verifica l'indirizzo Web a fronte del database degli indirizzi Web di phishing** nella sezione **Anti-Phishing**. Il database degli indirizzi Web di phishing include gli indirizzi Web dei siti Web attualmente noti utilizzati per generare attacchi di phishing. Kaspersky integra questo database dei collegamenti di phishing con gli indirizzi ottenuti dall'organizzazione internazionale nota come Anti-Phishing Working Group. Il database degli indirizzi di phishing è incluso nel pacchetto di installazione dell'applicazione e viene integrato dagli aggiornamenti del database di Kaspersky Endpoint Security.
5. Selezionare la casella di controllo **Usa l'analisi euristica** se si desidera che l'applicazione utilizzi l'analisi euristica durante la scansione delle pagine Web alla ricerca dei collegamenti di phishing.

   Durante l'analisi euristica, Kaspersky Endpoint Security analizza l'attività delle applicazioni nel sistema operativo. L'analisi euristica consente di rilevare le minacce per cui al momento non sono presenti record nei database di Kaspersky Endpoint Security.

   Per esaminare i collegamenti, oltre al database anti-virus e all'analisi euristica, è possibile utilizzare i database di reputazione Kaspersky Security Network.
6. Salvare le modifiche.

Creazione dell'elenco di indirizzi Web attendibili

Oltre ai siti Web dannosi e di phishing, Protezione minacce Web può bloccare altri siti Web. Ad esempio, Protezione minacce Web blocca il traffico HTTP che non soddisfa gli standard RFC. È possibile creare un elenco di URL di cui si ritengono attendibili i contenuti. Il componente Protezione minacce web non analizza le informazioni degli indirizzi Web attendibili per verificare la presenza di virus o altre minacce. Questa opzione può ad esempio risultare utile nei casi in cui il componente Protezione minacce web interferisce con il download di un file da un sito Web conosciuto.

Un URL può essere l'indirizzo di una specifica pagina Web o l'indirizzo di un sito Web.

Come aggiungere un indirizzi Web attendibile in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.
5. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
6. Nella finestra visualizzata, selezionare la scheda **Indirizzi Web attendibili**.
7. Selezionare la casella di controllo **Non esaminare il traffico Web per gli indirizzi Web attendibili**.

   Se questa opzione di controllo è selezionata, il componente Protezione minacce Web non esegue la scansione del contenuto delle pagine Web o dei siti Web i cui indirizzi sono inclusi nell'elenco degli indirizzi Web attendibili. È possibile aggiungere sia l'indirizzo specifico che una maschera di indirizzi di una pagina Web o un sito Web all'elenco degli indirizzi Web attendibili.
8. Creare un elenco di URL o di pagine Web di cui si ritengono attendibili i contenuti.

   Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:

   È inoltre possibile importare un elenco di indirizzi Web attendibili da un file XML.
9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come aggiungere un indirizzo Web attendibile in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare alla sezione **Area attendibile**.
5. Nella finestra visualizzata, fare clic sul collegamento **Indirizzi Web**.

   Verrà visualizzata una finestra contenente un elenco di indirizzi Web attendibili.

6. Creare un elenco di URL o di pagine Web di cui si ritengono attendibili i contenuti.

   Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:

   È inoltre possibile importare un elenco di indirizzi Web attendibili da un file JSON.

7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come aggiungere un indirizzo Web attendibile nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.
3. Fare clic su **Impostazioni avanzate**.
4. Selezionare la casella di controllo **Non esaminare il traffico Web da URL attendibili**.

   Se questa opzione di controllo è selezionata, il componente Protezione minacce Web non esegue la scansione del contenuto delle pagine Web o dei siti Web i cui indirizzi sono inclusi nell'elenco degli indirizzi Web attendibili. È possibile aggiungere sia l'indirizzo specifico che una maschera di indirizzi di una pagina Web o un sito Web all'elenco degli indirizzi Web attendibili.

5. Creare un elenco di URL o di pagine Web di cui si ritengono attendibili i contenuti.

   Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:

   È inoltre possibile importare un elenco di indirizzi Web attendibili da un file XML.

6. Salvare le modifiche.

Di conseguenza, Protezione minacce Web non esamina il traffico di indirizzi Web attendibili. L'utente può sempre aprire un sito Web attendibile e scaricare un file da tale sito Web. Se non si riesce ad accedere al sito Web, controllare le impostazioni dei componenti Scansione delle connessioni criptate, Controllo Web e Monitoraggio porte di rete. Se Kaspersky Endpoint Security rileva un file scaricato da un sito Web attendibile come dannoso, è possibile aggiungere tale file alle esclusioni.

È inoltre possibile creare un elenco generale di esclusioni per le connessioni criptate. In questo caso, Kaspersky Endpoint Security non esamina il traffico HTTPS degli indirizzi Web attendibili quando i componenti Protezione minacce Web, Protezione minacce di posta e Controllo Web sono in esecuzione.

Esportazione e importazione dell'elenco degli indirizzi Web attendibili

È possibile esportare l'elenco degli indirizzi Web attendibili in un file XML. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di indirizzi Web dello stesso tipo. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco degli indirizzi Web attendibili o per eseguire la migrazione dell'elenco in un server diverso.

Come esportare e importare un elenco di indirizzi Web attendibili in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.

4. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, selezionare la scheda **Indirizzi Web attendibili**.

6. Per esportare l'elenco degli indirizzi Web attendibili:

   a. Selezionare gli indirizzi Web attendibili che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.

   Se non è stato selezionato alcun indirizzo Web attendibile, Kaspersky Endpoint Security esporterà tutti gli indirizzi Web.

   b. Fare clic sul collegamento **Esporta**.

   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco degli indirizzi Web attendibili e selezionare la cartella in cui si desidera salvare il file.

   d. Salvare il file.

   Kaspersky Endpoint Security esporta l'intero elenco degli indirizzi Web attendibili nel file XML.

7. Per importare l'elenco degli indirizzi attendibili:

   a. Fare clic sul collegamento **Importa**.

   Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco degli indirizzi attendibili.

   b. Aprire il file.

   Se il computer dispone già di un elenco di indirizzi attendibili, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

8. Salvare le modifiche.

Come esportare e importare un elenco di indirizzi Web attendibili in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Comunicazione e protezione Web** → **Protezione minacce Web**.

5. Per esportare l'elenco delle esclusioni nella sezione **Elenco di regole**:

   a. Selezionare gli indirizzi Web attendibili che si desidera esportare.

   b. Fare clic sul pulsante → **Esporta**.

   Kaspersky Endpoint Security esporta l'elenco degli indirizzi Web attendibili in un file JSON nella cartella dei download predefinita.

6. Per importare l'elenco di esclusioni nella sezione **Elenco di regole**:

   a. Fare clic sul pulsante → **Importa**.

   Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco degli indirizzi attendibili.

b. Aprire il file.

Se il computer dispone già di un elenco di indirizzi attendibili, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

7. Salvare le modifiche.

Protezione minacce di posta

Il componente Protezione minacce di posta esamina gli allegati dei messaggi e-mail in entrata e in uscita alla ricerca di virus e altre minacce. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica.

Protezione minacce di posta può eseguire la scansione sia dei messaggi in entrata che di quelli in uscita. L'applicazione supporta POP3, SMTP, IMAP e NNTP nei seguenti client di posta:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Per eseguire la scansione del traffico nei client di posta Thunderbird, MyOffice Mail e R7-Office Organizer, è necessario aggiungere il certificato Kaspersky all'archivio certificati e selezionare il proprio archivio certificati.

Protezione minacce di posta non supporta altri protocolli e client di posta.

Protezione minacce di posta potrebbe non essere sempre in grado di ottenere l'accesso a *livello di protocollo* ai messaggi (ad esempio, quando si utilizza la soluzione Microsoft Exchange). Per questo motivo, Protezione minacce di posta include un'estensione per Microsoft Office Outlook. L'estensione consente la scansione dei messaggi al *livello del client di posta*. L'estensione Protezione minacce di posta supporta le versioni a 32 bit e a 64 bit di Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365. Nei computer basati su Arm l'estensione Protezione minacce di posta supporta le versioni a 32 bit e a 64 bit di Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 per Arm64.

Il componente Protezione minacce di posta non esegue la scansione dei messaggi se il client di posta è aperto in un browser.

Quando viene rilevato un file dannoso in un allegato, Kaspersky Endpoint Security aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*.

Abilitazione e disabilitazione di Protezione minacce di posta

Il componente Protezione minacce di posta è abilitato per impostazione predefinita e viene eseguito nella modalità consigliata dagli esperti Kaspersky. Per Protezione minacce di posta, l'applicazione può applicare diversi gruppi di impostazioni. I gruppi di impostazioni archiviate nell'applicazione sono denominati *livelli di protezione*: **Alto**, **Consigliato**, **Basso**. Le impostazioni del livello di sicurezza di posta **Consigliato** sono considerate le impostazioni ottimali consigliate dagli esperti di Kaspersky (vedere la tabella di seguito). È possibile selezionare uno dei livelli predefiniti di protezione dei messaggi e-mail o configurare un livello personalizzato di protezione della posta elettronica. Se sono state modificate le impostazioni del livello di sicurezza dei messaggi e-mail, è possibile ripristinare in qualsiasi momento le impostazioni consigliate.

Se si utilizza il client di posta Mozilla Thunderbird, il componente Protezione minacce di posta non esamina i messaggi trasmessi tramite il protocollo IMAP alla ricerca di virus e altre minacce se vengono utilizzati filtri per spostare i messaggi dalla cartella Posta in arrivo.

Come abilitare o disabilitare il componente Protezione minacce di posta in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale → Protezione minacce di posta**.
4. Utilizzare la casella di controllo **Protezione minacce di posta** per abilitare o disabilitare il componente.
5. Se il componente è stato abilitato, eseguire una delle seguenti operazioni nel blocco **Livello di sicurezza**:
   - Se si desidera applicare uno dei livelli di protezione preimpostati, selezionarlo con il dispositivo di scorrimento:
     - **Alto**. Quando questo livello di sicurezza dei messaggi e-mail è selezionato, il componente Protezione minacce di posta esamina i messaggi e-mail in modo più approfondito. Il componente Protezione minacce di posta esamina i messaggi e-mail in entrata e in uscita ed esegue l'analisi euristica in modo approfondito. Il livello di sicurezza di posta Alto è consigliato per gli ambienti ad alto rischio. Un esempio di ambiente di questo tipo è rappresentato da una connessione a un servizio di posta elettronica gratuito da una rete domestica priva di protezione centralizzata della posta elettronica.
     - **Consigliato**. Il livello di sicurezza e-mail che assicura un equilibrio ottimale tra le prestazioni dell'applicazione e la sicurezza della posta elettronica. Il componente Protezione minacce di posta esamina i messaggi e-mail in entrata e in uscita ed esegue l'analisi euristica di livello medio. Questo livello di sicurezza del traffico e-mail è consigliato dagli specialisti di Kaspersky. I valori delle impostazioni per il livello di sicurezza consigliato sono specificati nella tabella seguente.
     - **Basso**. Quando si seleziona questo livello di sicurezza, il componente Protezione minacce di posta esamina solo i messaggi e-mail in entrata, esegue l'analisi euristica in modo superficiale e non esamina gli archivi allegati ai messaggi e-mail. A questo livello di sicurezza e-mail, Protezione minacce di posta esamina i messaggi e-mail con la massima velocità e con il minimo utilizzo di risorse del sistema operativo. Il livello di sicurezza Basso è consigliato quando si lavora in un ambiente protetto in modo affidabile. Un esempio di ambiente di questo tipo è rappresentato da una rete LAN aziendale con protezione centralizzata della posta elettronica.

- Se si desidera configurare un livello di sicurezza personalizzato, fare clic sul pulsante **Impostazioni** e definire le proprie impostazioni del componente (vedere la tabella seguente).

  È possibile ripristinare i valori dei livelli di sicurezza preimpostati facendo clic sul pulsante **Predefinito**.

6. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi:

   - **Disinfetta (se non è possibile, elimina)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata o in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione elimina l'oggetto infetto. L'applicazione aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*.

   - **Disinfetta (se non è possibile, blocca)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Quando un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. Se l'oggetto non può essere disinfettato, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.

   - **Blocca**. Se un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Se un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.

7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare il componente Protezione minacce di posta in Web Console

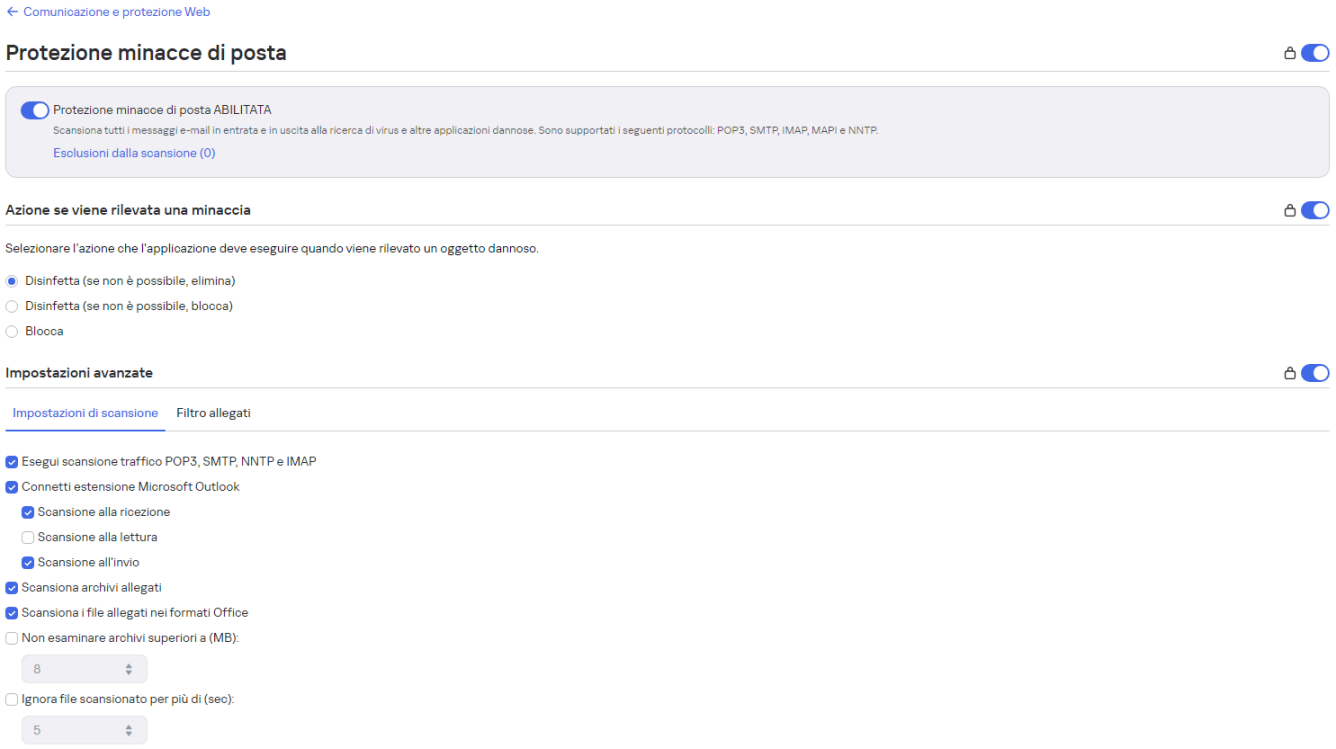
1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Comunicazione e protezione Web → Protezione minacce di posta**.



Impostazioni di Protezione minacce di posta

5. Utilizzare l'interruttore **Protezione minacce di posta ABILITATA** per abilitare o disabilitare il componente.

6. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi:

   - **Disinfetta (se non è possibile, elimina)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata o in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione elimina l'oggetto infetto. L'applicazione aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*.

   - **Disinfetta (se non è possibile, blocca)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Quando un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. Se l'oggetto non può essere disinfettato, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.

   - **Blocca**. Se un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Se un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.

7. Se necessario, modificare le impostazioni avanzate di Protezione minacce di posta.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare il componente Protezione minacce di posta nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce di posta**.
3. Utilizzare l'interruttore **Protezione minacce di posta** per abilitare o disabilitare il componente.
4. Se il componente è stato abilitato, eseguire una delle seguenti operazioni nel blocco **Livello di sicurezza**:
   - Se si desidera applicare uno dei livelli di protezione preimpostati, selezionarlo con il dispositivo di scorrimento:
     - **Alto**. Quando questo livello di sicurezza dei messaggi e-mail è selezionato, il componente Protezione minacce di posta esamina i messaggi e-mail in modo più approfondito. Il componente Protezione minacce di posta esamina i messaggi e-mail in entrata e in uscita ed esegue l'analisi euristica in modo approfondito. Il livello di sicurezza di posta Alto è consigliato per gli ambienti ad alto rischio. Un esempio di ambiente di questo tipo è rappresentato da una connessione a un servizio di posta elettronica gratuito da una rete domestica priva di protezione centralizzata della posta elettronica.
     - **Consigliato**. Il livello di sicurezza e-mail che assicura un equilibrio ottimale tra le prestazioni dell'applicazione e la sicurezza della posta elettronica. Il componente Protezione minacce di posta esamina i messaggi e-mail in entrata e in uscita ed esegue l'analisi euristica di livello medio. Questo livello di sicurezza del traffico e-mail è consigliato dagli specialisti di Kaspersky. I valori delle impostazioni per il livello di sicurezza consigliato sono specificati nella tabella seguente.
     - **Basso**. Quando si seleziona questo livello di sicurezza, il componente Protezione minacce di posta esamina solo i messaggi e-mail in entrata, esegue l'analisi euristica in modo superficiale e non esamina gli archivi allegati ai messaggi e-mail. A questo livello di sicurezza e-mail, Protezione minacce di posta esamina i messaggi e-mail con la massima velocità e con il minimo utilizzo di risorse del sistema operativo. Il livello di sicurezza Basso è consigliato quando si lavora in un ambiente protetto in modo affidabile. Un esempio di ambiente di questo tipo è rappresentato da una rete LAN aziendale con protezione centralizzata della posta elettronica.
   - Se si desidera configurare un livello di sicurezza personalizzato, fare clic sul pulsante **Impostazioni avanzate** e definire le proprie impostazioni del componente (vedere la tabella seguente).

     È possibile ripristinare i valori dei livelli di sicurezza preimpostati facendo clic sul pulsante **Ripristina il livello di sicurezza consigliato**.

5. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi:

   - **Disinfetta (se non è possibile, elimina)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata o in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione elimina l'oggetto infetto. L'applicazione aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*.

   - **Disinfetta (se non è possibile, blocca)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Quando un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. Se l'oggetto non può essere disinfettato, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.

   - **Blocca**. Se un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Se un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.

6. Salvare le modifiche.

Impostazioni di Protezione minacce di posta consigliate dagli esperti di Kaspersky (livello di sicurezza consigliato)

Parametro	Valore	Descrizione
Ambito della protezione	**Messaggi in entrata e in uscita**	L'*ambito della protezione* include gli oggetti che il componente controlla durante l'esecuzione: Messaggi in entrata e in uscita o Solo messaggi in entrata. Per proteggere i computer, è sufficiente esaminare i messaggi in entrata. È possibile attivare la scansione dei messaggi in uscita per impedire l'invio dei file infetti negli archivi. È inoltre possibile attivare la scansione dei messaggi in uscita se si desidera impedire l'invio di file di determinati formati, ad esempio file audio e video.
Connetti estensione Microsoft Outlook	**Attivato**	Se la casella di controllo è selezionata, la scansione dei messaggi e-mail trasmessi tramite i protocolli POP3, SMTP, NNTP, IMAP è abilitata per l'estensione integrata in Microsoft Outlook. Se viene eseguita la scansione dei messaggi tramite l'estensione per Microsoft Outlook, è consigliabile utilizzare Cached Exchange Mode. Per informazioni più dettagliate sulla Modalità cache e per raccomandazioni sul relativo utilizzo, fare riferimento alla Microsoft Knowledge Base.
Esamina gli archivi allegati	**Attivato**	Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio).
Esamina i file allegati nei formati Microsoft Office	**Attivato**	Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE. L'applicazione analizza i file in formato Office di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Filtro allegati	**Rinomina allegati dei tipi selezionati**	Se questa opzione è selezionata, il componente Protezione minacce di posta sostituirà l'ultimo carattere dell'estensione rilevato nei file allegati dei tipi specificati con il carattere di sottolineatura (ad esempio allegato.doc_). Per aprire il file l'utente deve quindi rinominare il file.
Analisi euristica	**Media**	Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto. Durante la scansione dei file alla ricerca di codice dannoso, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.
Azione se viene rilevata una minaccia	**Disinfetta (se non è possibile, elimina)**	Quando un oggetto infetto viene rilevato in un messaggio in entrata o in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione elimina l'oggetto infetto. L'applicazione aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*.

Modifica dell'azione da eseguire sui messaggi e-mail infetti

Per impostazione predefinita, il componente Protezione minacce di posta tenta automaticamente di disinfettare tutti i messaggi e-mail infetti rilevati. Se la disinfezione non riesce, il componente Protezione minacce di posta elimina i messaggi e-mail infetti.

Per modificare l'azione da eseguire sui messaggi e-mail infetti:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Protezione minacce di posta**.
3. Nel blocco **Azione se viene rilevata una minaccia**, selezionare l'azione che deve essere eseguita da Kaspersky Endpoint Security quando viene rilevato un messaggio infetto:
   - **Disinfetta (se non è possibile, elimina)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata o in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione elimina l'oggetto infetto. L'applicazione aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*.
   - **Disinfetta (se non è possibile, blocca)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Quando un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. Se l'oggetto non può essere disinfettato, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.
   - **Blocca**. Se un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Se un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.
4. Salvare le modifiche.

Creazione dell'ambito di protezione del componente Protezione minacce di posta

L'*ambito di protezione* si riferisce agli oggetti che vengono esaminati dal componente quando è attivo. Gli ambiti di protezione dei vari componenti dispongono di differenti proprietà. Le proprietà dell'ambito di protezione del componente Protezione minacce di posta includono le impostazioni per l'integrazione del componente Protezione minacce di posta nei client di posta e il tipo di messaggi e protocolli e-mail per cui il traffico viene esaminato dal componente Protezione minacce di posta. Per impostazione predefinita, Kaspersky Endpoint Security esegue la scansione sia dei messaggi e-mail in entrata e in uscita che del traffico dei protocolli POP3, SMTP, NNTP e IMAP ed è integrato nei client di posta Microsoft Office Outlook.

Per creare l'ambito di protezione del componente Protezione minacce di posta:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce di posta**.
3. Fare clic su **Impostazioni avanzate**.
4. Nella sezione **Ambito della protezione** selezionare i messaggi da esaminare:
   - **Messaggi in entrata e in uscita**.
   - **Solo messaggi in entrata**.

   Per proteggere i computer, è sufficiente esaminare i messaggi in entrata. È possibile attivare la scansione dei messaggi in uscita per impedire l'invio dei file infetti negli archivi. È inoltre possibile attivare la scansione dei messaggi in uscita se si desidera impedire l'invio di file di determinati formati, ad esempio file audio e video.

   Se si sceglie di esaminare solo i messaggi in entrata, è consigliabile eseguire una volta una scansione di tutti i messaggi in uscita perché è possibile che nel computer siano presenti worm e-mail che si propagano tramite e-mail. Questa misura precauzionale contribuisce a evitare problemi causati da invii non controllati di grandi quantità di messaggi infetti provenienti dal proprio computer.
5. Nel blocco **Connettività**, eseguire una delle seguenti operazioni:
   - Se si desidera che il componente Protezione minacce di posta esamini i messaggi trasferiti tramite i protocolli POP3, SMTP, NNTP e IMAP prima che vengano ricevuti nel computer dell'utente, selezionare la casella di controllo **Esegui scansione traffico POP3, SMTP, NNTP e IMAP**.

     Se non si desidera che il componente Protezione minacce di posta esamini i messaggi trasferiti tramite i protocolli POP3, SMTP, NNTP e IMAP prima che vengano scaricati nel computer dell'utente, deselezionare la casella di controllo **Esegui scansione traffico POP3, SMTP, NNTP e IMAP**. In questo caso, i messaggi vengono esaminati dall'estensione di Protezione minacce di posta incorporata nel client di posta Microsoft Office Outlook dopo la ricezione nel computer dell'utente se la casella di controllo **Connetti estensione Microsoft Outlook** è selezionata.

     Se si utilizza un client di posta diverso da Microsoft Office Outlook, il componente Protezione minacce di posta non esegue la scansione dei messaggi trasmessi tramite i protocolli POP3, SMTP, NNTP e IMAP se la casella di controllo **Esegui scansione traffico POP3, SMTP, NNTP e IMAP** è deselezionata.
   - Se si desidera consentire l'accesso alle impostazioni del componente Protezione minacce di posta da Microsoft Office Outlook e abilitare la scansione dei messaggi trasferiti tramite i protocolli POP3, SMTP, NNTP, IMAP e MAPI una volta ricevuti dal computer tramite l'estensione incorporata in Microsoft Office Outlook, selezionare la casella di controllo **Connetti estensione Microsoft Outlook**.

     Se si desidera bloccare l'accesso alle impostazioni del componente Protezione minacce di posta da Microsoft Office Outlook e disabilitare la scansione dei messaggi trasferiti tramite i protocolli POP3, SMTP, NNTP, IMAP e MAPI una volta ricevuti dal computer tramite l'estensione incorporata in Microsoft Office Outlook, deselezionare la casella di controllo **Connetti estensione Microsoft Outlook**.

L'estensione Protezione minacce di posta è incorporata nel client di posta Microsoft Office Outlook durante l'installazione di Kaspersky Endpoint Security.

6. Salvare le modifiche.

Scansione dei file compositi allegati ai messaggi e-mail

È possibile abilitare o disabilitare la scansione degli allegati dei messaggi, limitare la dimensione massima degli allegati dei messaggio da esaminare e limitare la durata massima della scansione degli allegati dei messaggi.

Per configurare la scansione dei file compositi allegati ai messaggi e-mail:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce di posta**.
3. Fare clic su **Impostazioni avanzate**.
4. Nel blocco **Scansione dei file compositi**, configurare le impostazioni di scansione:
   - **Esamina i file allegati nei formati Microsoft Office**. Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE. L'applicazione analizza i file in formato Office di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
   - **Esamina gli archivi allegati**. Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio).

     Se durante la scansione l'applicazione rileva una password per un archivio nel testo del messaggio, tale password verrà utilizzata per analizzare il contenuto dell'archivio alla ricerca di applicazioni dannose. In questo caso, la password non viene salvata. Un archivio viene decompresso durante la scansione. Se si verifica un errore dell'applicazione durante il processo di decompressione, è possibile eliminare manualmente i file decompressi che vengono salvati nel percorso seguente: %systemroot%\temp. I file hanno il prefisso PR.

   - **Non esaminare archivi superiori a N MB (da 1 a 9999)**. Se la casella di controllo è selezionata, il componente Protezione minacce di posta esclude dalla scansione gli archivi allegati ai messaggi e-mail se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, il componente Protezione minacce di posta esamina gli archivi allegati ai messaggi e-mail di qualsiasi dimensione.
   - **Limita il tempo per il controllo degli archivi a N sec (da 1 a 9999)**. Se la casella di controllo è selezionata, il tempo allocato per la scansione degli archivi allegati ai messaggi e-mail è limitato al periodo specificato.
5. Salvare le modifiche.

Filtraggio degli allegati dei messaggi e-mail

Il filtro allegati non viene applicato ai messaggi e-mail in uscita.

Le applicazioni dannose possono essere distribuite sotto forma di allegati dei messaggi e-mail. È possibile configurare il filtro in base al tipo di allegati del messaggio, in modo che i file dei tipi specificati vengano automaticamente rinominati o eliminati. Rinominando un allegato di un determinato tipo, Kaspersky Endpoint Security può proteggere il computer dall'esecuzione automatica di un'applicazione dannosa.

Per configurare il filtro degli allegati:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce di posta**.
3. Fare clic su **Impostazioni avanzate**.
4. Nel blocco **Filtro allegati**, eseguire una delle seguenti operazioni:
   - **Disabilita il filtro**. Se questa opzione è selezionata, il componente Protezione minacce di posta non filtra i file allegati ai messaggi e-mail.
   - **Rinomina allegati dei tipi selezionati**. Se questa opzione è selezionata, il componente Protezione minacce di posta sostituirà l'ultimo carattere dell'estensione rilevato nei file allegati dei tipi specificati con il carattere di sottolineatura (ad esempio allegato.doc_). Per aprire il file l'utente deve quindi rinominare il file.
   - **Elimina allegati dei tipi selezionati**. Se questa opzione è selezionata, il componente Protezione minacce di posta elimina i file allegati dei tipi specificati dai messaggi e-mail.
5. Se è stata selezionata l'opzione **Rinomina allegati dei tipi selezionati** o l'opzione **Elimina allegati dei tipi selezionati** durante il passaggio precedente, selezionare le caselle di controllo accanto ai tipi di file desiderati.
6. Salvare le modifiche.

Esportazione e importazione delle estensioni per il filtro degli allegati

È possibile esportare l'elenco delle estensioni del filtro degli allegati in un file XML. È possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco delle estensioni o per eseguire la migrazione dell'elenco in un server diverso.

Come esportare e importare un elenco di estensioni del filtro degli allegati in Administration Console (MMC)

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Comunicazione e protezione Web** → **Protezione minacce di posta**.
5. Per esportare l'elenco delle estensioni nella sezione **Filtro allegati**:
   a. Selezionare le estensioni che si desidera esportare.
   b. Fare clic sul collegamento **Esporta**.
   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle estensioni e selezionare la cartella in cui si desidera salvare il file.
   d. Salvare il file.

      Kaspersky Endpoint Security esporta l'intero elenco di estensioni nel file XML.
6. Per importare l'elenco di estensioni nella sezione **Filtro allegati**:
   a. Fare clic sul collegamento **Importa**.
   b. Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle estensioni.
   c. Aprire il file.

      Se il computer dispone già di un elenco di estensioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.
7. Salvare le modifiche.

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce di posta**.
4. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
5. Viene visualizzata una finestra, che consente di selezionare la scheda **Filtro allegati**.
6. Per esportare l'elenco delle estensioni:
   a. Selezionare le estensioni che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.
   b. Fare clic sul collegamento **Esporta**.
   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle estensioni e selezionare la cartella in cui si desidera salvare il file.

d. Salvare il file.

Kaspersky Endpoint Security esporta l'intero elenco di estensioni nel file XML.

7. Per importare l'elenco delle estensioni:

a. Fare clic sul collegamento **Importa**.

b. Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle estensioni.

c. Aprire il file.

Se il computer dispone già di un elenco di estensioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

8. Salvare le modifiche.

Scansione dei messaggi e-mail in Microsoft Office Outlook

Durante l'installazione di Kaspersky Endpoint Security, l'estensione di Protezione minacce di posta è incorporata in Microsoft Office Outlook (di seguito denominato anche Outlook). L'estensione consente la scansione dei messaggi a livello di un client di posta anziché a livello di protocollo. Oltre ai messaggi, l'estensione consente di eseguire la scansione degli oggetti ricevuti tramite l'interfaccia MAPI dagli archivi di Microsoft Exchange (ad esempio, gli oggetti nel Calendario). Questa scansione avviene nel client di posta.

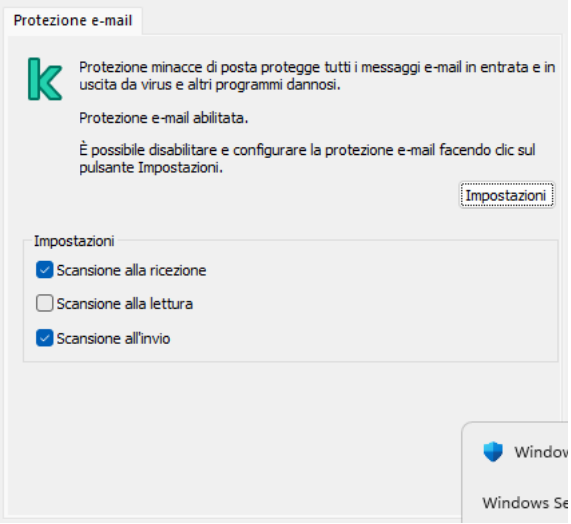
È possibile aprire le impostazioni del componente Protezione minacce di posta direttamente da Outlook e specificare quando eseguire la scansione dei messaggi e-mail alla ricerca di virus e altre minacce.

L'estensione Protezione minacce di posta supporta le versioni a 32 bit e a 64 bit di Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365.

Nei computer basati su Arm l'estensione Protezione minacce di posta supporta le versioni a 32 bit e a 64 bit di Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 per Arm64.

In Outlook i messaggi in entrata vengono prima esaminati dal componente Protezione minacce di posta (se la casella di controllo Esegui scansione traffico POP3, SMTP, NNTP e IMAP è selezionata nell'interfaccia di Kaspersky Endpoint Security) e quindi dall'estensione Protezione minacce di posta per Outlook. Se il componente Protezione minacce di posta rileva un oggetto dannoso in un messaggio, l'evento viene segnalato all'utente.

Le impostazioni del componente Protezione minacce di posta possono essere configurate direttamente in Outlook se l'estensione Microsoft Outlook è connessa nell'interfaccia di Kaspersky Endpoint Security (vedere la figura riportata di seguito).



Impostazioni del componente Protezione minacce di posta in Outlook

I messaggi in uscita vengono prima esaminati dall'estensione di Protezione minacce di posta per Outlook e quindi dal componente Protezione minacce di posta.

Durante la scansione delle e-mail con l'estensione Protezione minacce di posta per Outlook, è consigliabile utilizzare la modalità cache di Exchange Server (Use Cached Exchange Mode). Per informazioni più dettagliate sulla Modalità cache e per raccomandazioni sul relativo utilizzo, fare riferimento alla Microsoft Knowledge Base.

Come configurare la modalità operativa dell'estensione di Protezione minacce di posta per Outlook in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce di posta**.
5. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
6. Nella finestra visualizzata, nel blocco **Connettività**, selezionare la casella di controllo **Connetti estensione Microsoft Outlook**.
7. Fare clic su **Impostazioni**.

8. Nella finestra **Protezione e-mail**, procedere come segue:

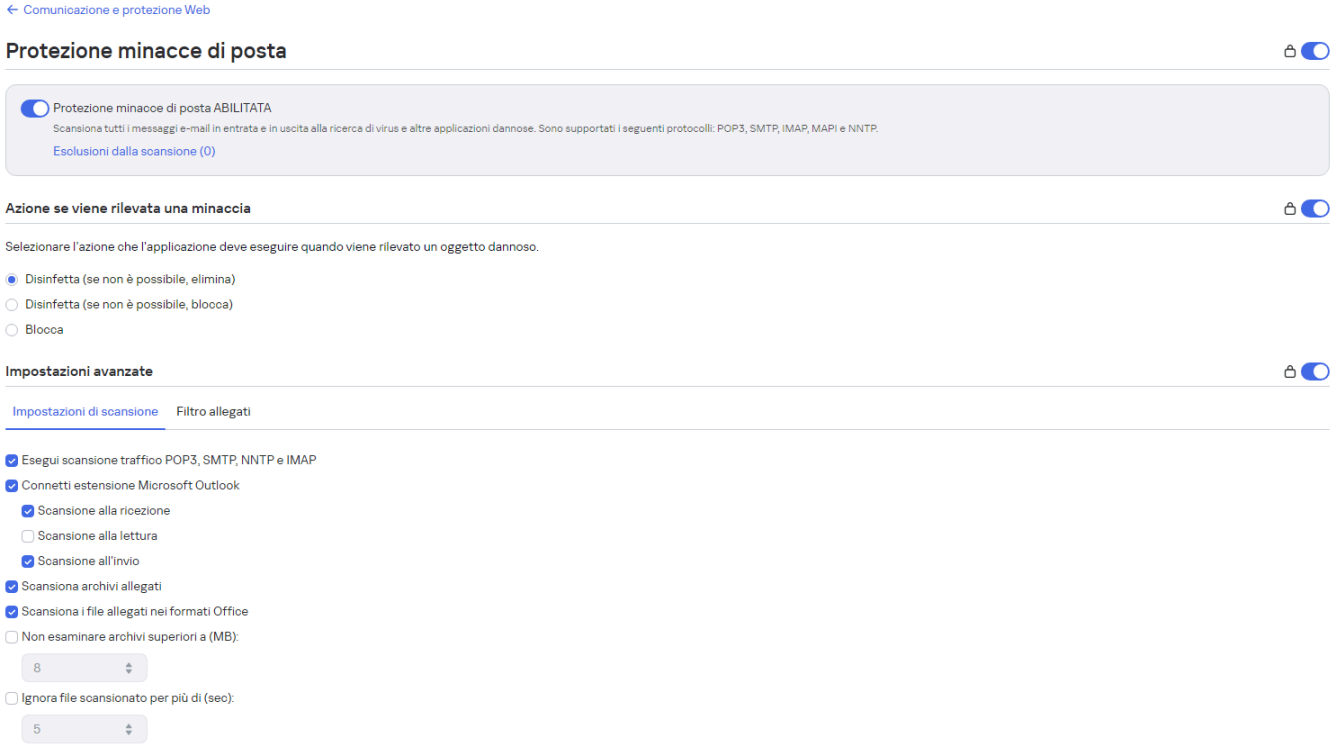
   - Selezionare la casella di controllo **Scansione alla ricezione** se si desidera che l'estensione di Protezione minacce di posta per Outlook esamini i messaggi in entrata non appena vengono ricevuti dalla cassetta postale.
   - Selezionare la casella di controllo **Scansione alla lettura** se si desidera che l'estensione di Protezione minacce di posta per Outlook esamini i messaggi in entrata quando l'utente li apre.
   - Selezionare la casella di controllo **Scansione all'invio** se si desidera che l'estensione di Protezione minacce di posta per Outlook esamini i messaggi in uscita quando vengono inviati.

9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare la modalità operativa dell'estensione di Protezione minacce di posta per Outlook in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Comunicazione e protezione Web** → **Protezione minacce di posta**.



Impostazioni di Protezione minacce di posta

5. In **Impostazioni avanzate**, selezionare la scheda **Impostazioni di scansione**.
6. Selezionare la casella di controllo **Connetti estensione Microsoft Outlook**.

7. Configurare la modalità dell'estensione:

   - Selezionare la casella di controllo **Scansione alla ricezione** se si desidera che l'estensione di Protezione minacce di posta per Outlook esamini i messaggi in entrata non appena vengono ricevuti dalla cassetta postale.
   - Selezionare la casella di controllo **Scansione alla lettura** se si desidera che l'estensione di Protezione minacce di posta per Outlook esamini i messaggi in entrata quando l'utente li apre.
   - Selezionare la casella di controllo **Scansione all'invio** se si desidera che l'estensione di Protezione minacce di posta per Outlook esamini i messaggi in uscita quando vengono inviati.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Scansione delle e-mail in Thunderbird, MyOffice, R7-Office

Il componente Protezione minacce di posta esamina gli allegati dei messaggi e-mail in entrata e in uscita alla ricerca di virus e altre minacce. Per i client di posta Mozilla Thunderbird, MyOffice Mail e R7-Office Organizer, l'applicazione può accedere ai messaggi solo al *livello di protocollo* (POP3, SMTP, IMAP, NNTP).

Per eseguire la scansione del traffico nei client di posta Thunderbird, MyOffice Mail e R7-Office Organizer, è necessario aggiungere il certificato Kaspersky all'archivio certificati e selezionare il proprio archivio certificati.

Il componente Protezione minacce di posta non esegue la scansione dei messaggi se il client di posta è aperto in un browser.

Protezione minacce di posta in tempo reale

Protezione minacce di posta può eseguire la scansione sia dei messaggi in entrata che di quelli in uscita. Per impostazione predefinita, il componente Protezione minacce di posta tenta automaticamente di disinfettare tutti i messaggi e-mail infetti rilevati. Se la disinfezione non riesce, il componente Protezione minacce di posta elimina i messaggi e-mail infetti. Quando viene rilevato un file dannoso in un allegato, Kaspersky Endpoint Security aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*.

Se si utilizza il client di posta Mozilla Thunderbird, il componente Protezione minacce di posta non esamina i messaggi trasmessi tramite il protocollo IMAP alla ricerca di virus e altre minacce se vengono utilizzati filtri per spostare i messaggi dalla cartella Posta in arrivo.

Scansione malware nei database di posta

Protezione minacce di posta previene l'infezione del computer a livello di protocollo, ma se il computer era stato infettato prima dell'installazione di Kaspersky Endpoint Security, l'applicazione potrebbe rilevare la minaccia nei database di posta utilizzando l'attività *Scansione malware*. L'applicazione non disinfetta o elimina i file infetti nei database di posta, indipendentemente dalle impostazioni dell'attività. Ciò è dovuto al fatto che Kaspersky Endpoint Security non suddivide i messaggi di Thunderbird, MyOffice e P7-Office nelle relative parti (intestazione, corpo e allegati) allo stesso modo dei messaggi di Microsoft Office Outlook. L'applicazione aggiunge solo le informazioni sugli oggetti rilevati all'elenco delle minacce attive.

Per eliminare le minacce attive:

1. Trovare ed eliminare manualmente il messaggio con l'oggetto rilevato nell'interfaccia del client di posta.

   L'applicazione mostra le informazioni sull'oggetto rilevato nell'elenco delle minacce attive.

   Esempio di scheda oggetto rilevato:

   HEUR:Trojan.PDF.Phish.gen
   Oggetto: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Eseguire l'operazione di compattazione del database.

   Quando un messaggio viene eliminato nell'interfaccia utente, il client di posta aggiunge solo un contrassegno di eliminazione. Il client di posta elimina effettivamente il messaggio dopo la compattazione del database. Per i dettagli sulla compattazione dei database, vedere la Guida del client di posta (ad esempio Mozilla Thunderbird).

3. Eseguire di nuovo l'attività *Scansione malware* e verificare che la minaccia non sia più presente.

Se l'eliminazione dei messaggi con file infetti non è al momento disponibile per qualsiasi motivo, è possibile gestire tali minacce nell'interfaccia utente di Kaspersky Endpoint Security. Per i file dei client di posta elettronica, sono disponibili due opzioni per l'elaborazione di una minaccia: **Ignora** e **Aggiungi alle esclusioni**. Per impedire all'applicazione di aggiungere questi oggetti all'elenco delle minacce attive durante una nuova scansione, aggiungerli all'elenco delle esclusioni dalla scansione.

Protezione minacce di rete

Il componente *Protezione minacce di rete* (chiamato anche Intrusion Detection System, IDS) monitora il traffico di rete in entrata per verifiche le caratteristiche delle attività degli attacchi di rete. Quando l'applicazione rileva un tentativo di attacco di rete nel computer dell'utente, blocca la connessione di rete con il computer che ha originato l'attacco. Nei database dell'applicazione è inclusa una descrizione degli attacchi di rete attualmente conosciuti, nonché dei metodi utilizzati per contrastarli. L'elenco degli attacchi di rete che il componente Protezione minacce di Rete è in grado di rilevare viene aggiornato durante gli aggiornamenti dei database e dei moduli dell'applicazione.

Abilitazione e disabilitazione di Protezione minacce di Rete

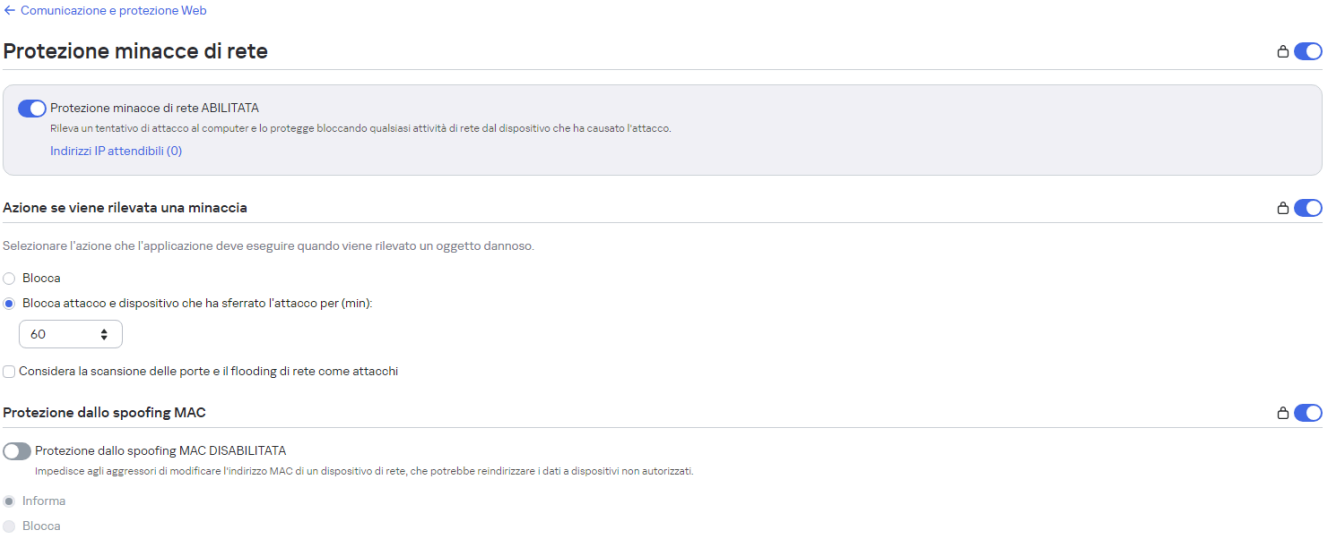
Per impostazione predefinita, Protezione minacce di Rete è abilitato e viene eseguito in modalità normale. Kaspersky Endpoint Security monitora il traffico di rete in entrata per verificare le caratteristiche delle attività degli attacchi di rete e blocca gli attacchi.

Come abilitare o disabilitare Protezione minacce di rete in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce di rete**.
4. Utilizzare la casella di controllo **Protezione minacce di rete** per abilitare o disabilitare il componente.
5. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare Protezione minacce di Rete in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Comunicazione e protezione Web** → **Protezione minacce di rete**.

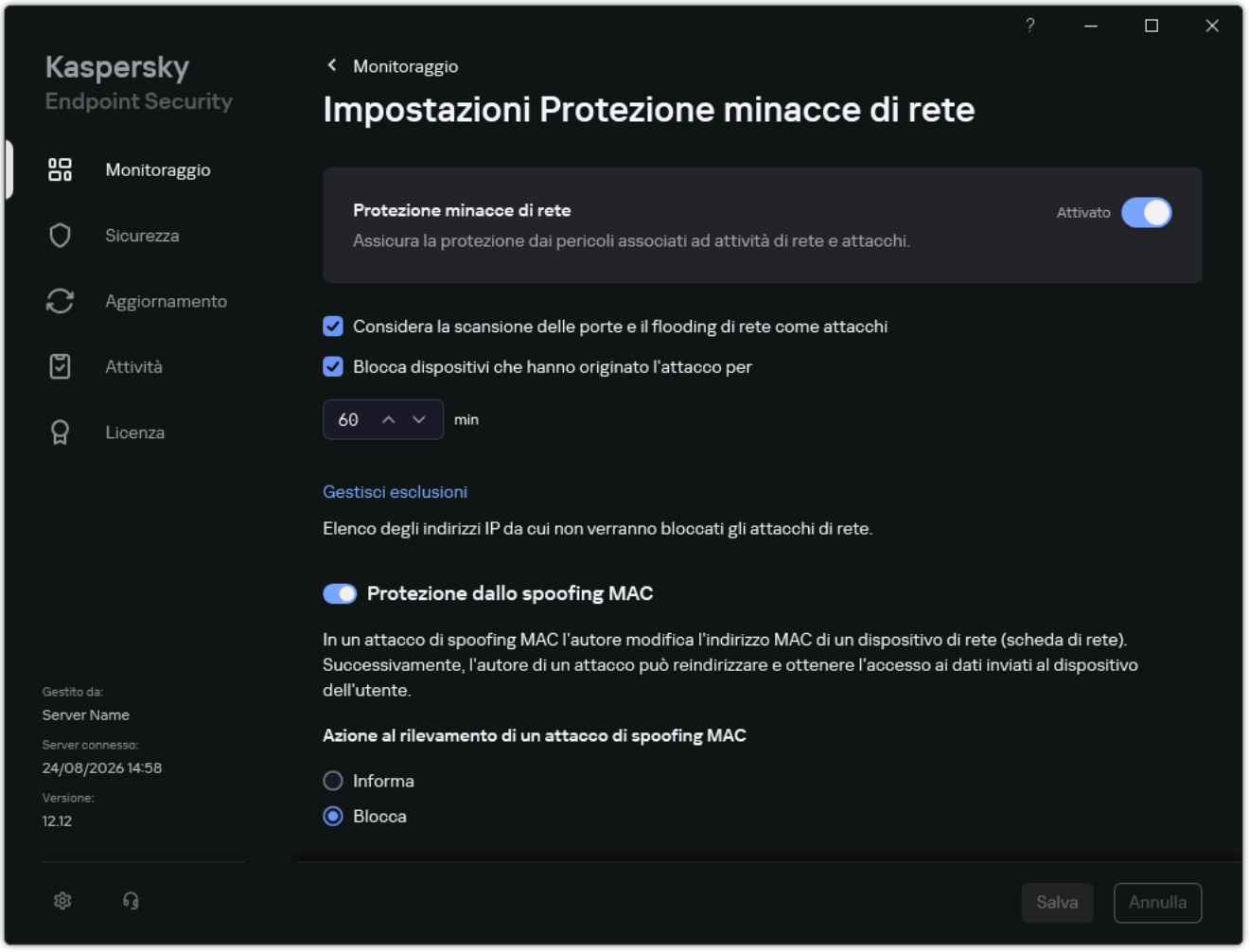


Impostazioni di Protezione minacce di Rete

5. Utilizzare l'interruttore **Protezione minacce di rete ABILITATA** per abilitare o disabilitare il componente.
6. Salvare le modifiche.

Come abilitare o disabilitare Protezione minacce di rete nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce di rete**.



Impostazioni di Protezione minacce di Rete

3. Utilizzare l'interruttore **Protezione minacce di rete** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Blocco di un computer che ha originato l'attacco

Se il componente Protezione minacce di rete è abilitato, Kaspersky Endpoint Security blocca automaticamente le minacce di rete. Inoltre, l'applicazione può bloccare il computer che ha originato l'attacco e limitare l'invio di pacchetti di rete per un determinato periodo di tempo. Per impostazione predefinita, Kaspersky Endpoint Security blocca il computer per un'ora.

Come bloccare un computer che ha originato l'attacco in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale → Protezione minacce di rete**.

4. In **Impostazioni Protezione minacce di rete**, selezionare la casella di controllo **Blocca dispositivi che hanno originato l'attacco per N min**.

   Se l'opzione è abilitata, il componente Protezione minacce di rete aggiunge il computer che ha originato l'attacco all'elenco di computer bloccati. In altre parole, il componente Protezione minacce di rete blocca la connessione di rete con il computer che ha originato l'attacco dopo il primo tentativo di un attacco di rete per il periodo di tempo specificato. Questo blocco protegge automaticamente il computer dell'utente da ulteriori possibili attacchi di rete dallo stesso indirizzo. Il tempo minimo che un computer che ha originato l'attacco deve trascorrere nell'elenco dei blocchi è di un minuto. Il tempo massimo è 999 minuti.

5. Impostare una durata di blocco diversa per un computer che ha originato l'attacco nel campo a destra della casella di controllo **Blocca dispositivi che hanno originato l'attacco per N min**.

6. Salvare le modifiche.

Come bloccare un computer che ha originato l'attacco in Web Console

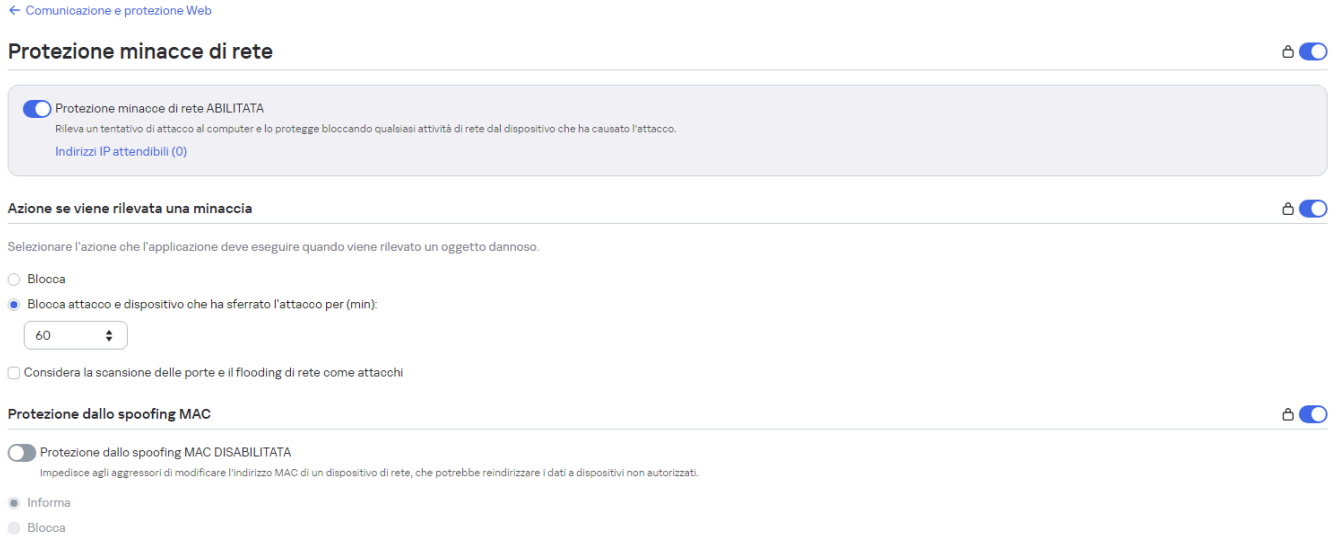
1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Comunicazione e protezione Web** → **Protezione minacce di rete**.



Impostazioni di Protezione minacce di Rete

5. Nella sezione **Azione se viene rilevata una minaccia** selezionare la casella di controllo **Blocca attacco e dispositivo che ha sferrato l'attacco per (min)**.

   Se l'opzione è abilitata, il componente Protezione minacce di rete aggiunge il computer che ha originato l'attacco all'elenco di computer bloccati. In altre parole, il componente Protezione minacce di rete blocca la connessione di rete con il computer che ha originato l'attacco dopo il primo tentativo di un attacco di rete per il periodo di tempo specificato. Questo blocco protegge automaticamente il computer dell'utente da ulteriori possibili attacchi di rete dallo stesso indirizzo. Il tempo minimo che un computer che ha originato l'attacco deve trascorrere nell'elenco dei blocchi è di un minuto. Il tempo massimo è 999 minuti.

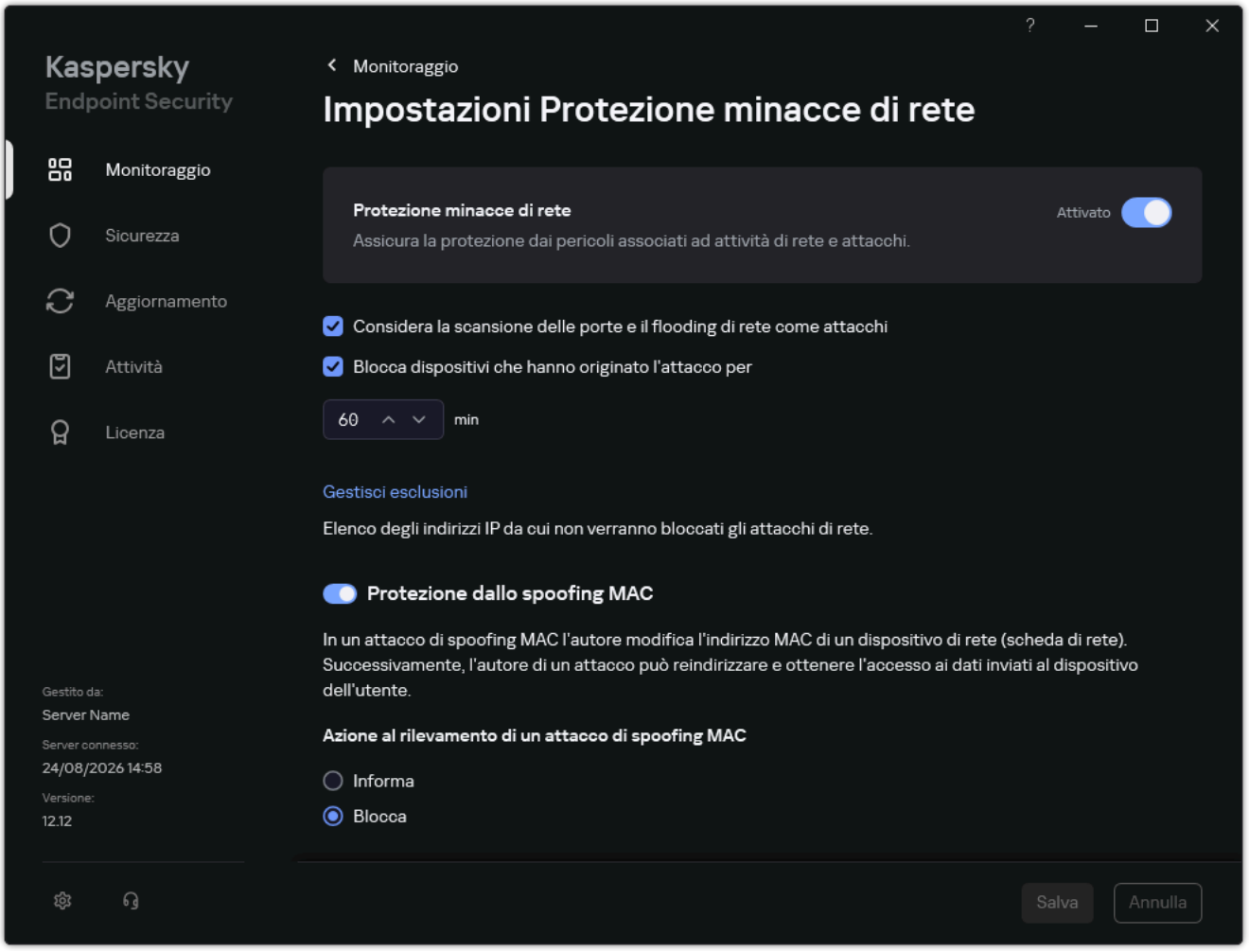
6. Modificare la durata del blocco del computer che ha originato l'attacco.

7. Salvare le modifiche.

Come bloccare un computer che ha originato l'attacco nell'interfaccia utente dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce di rete**.



Impostazioni di Protezione minacce di Rete

3. Attivare l'interruttore **Blocca dispositivi che hanno originato l'attacco per N min**.

   Se l'opzione è abilitata, il componente Protezione minacce di rete aggiunge il computer che ha originato l'attacco all'elenco di computer bloccati. In altre parole, il componente Protezione minacce di rete blocca la connessione di rete con il computer che ha originato l'attacco dopo il primo tentativo di un attacco di rete per il periodo di tempo specificato. Questo blocco protegge automaticamente il computer dell'utente da ulteriori possibili attacchi di rete dallo stesso indirizzo. Il tempo minimo che un computer che ha originato l'attacco deve trascorrere nell'elenco dei blocchi è di un minuto. Il tempo massimo è 999 minuti.

4. Impostare una durata di blocco diversa per un computer che ha originato l'attacco nel campo sotto l'interruttore **Blocca dispositivi che hanno originato l'attacco per N min**.

5. Salvare le modifiche.

Di conseguenza, quando Kaspersky Endpoint Security rileva un tentativo di attacco di rete contro il computer dell'utente, blocca tutte le connessioni con il computer che ha originato l'attacco. Kaspersky Endpoint Security crea l'evento *Attacco di rete rilevato*. L'evento contiene informazioni sul computer che ha originato l'attacco: indirizzi IP e MAC.

È possibile visualizzare l'indirizzo MAC del computer autore dell'attacco nell'interfaccia utente dell'applicazione o nella console di Kaspersky Security Center versione 15.1 o successiva.



Notifica sul rilevamento di attacchi di rete

Kaspersky Endpoint Security sblocca il computer allo scadere del tempo specificato. La console di Kaspersky Security Center non fornisce strumenti per il monitoraggio dei computer bloccati diversi dagli eventi *Attacco di rete rilevato* nel rapporto. È possibile visualizzare solo un elenco di computer bloccanti nell'interfaccia dell'applicazione. Questa funzionalità è fornita dallo strumento *Monitor di rete*. È inoltre possibile utilizzare lo strumento Monitor di rete per sbloccare un computer.

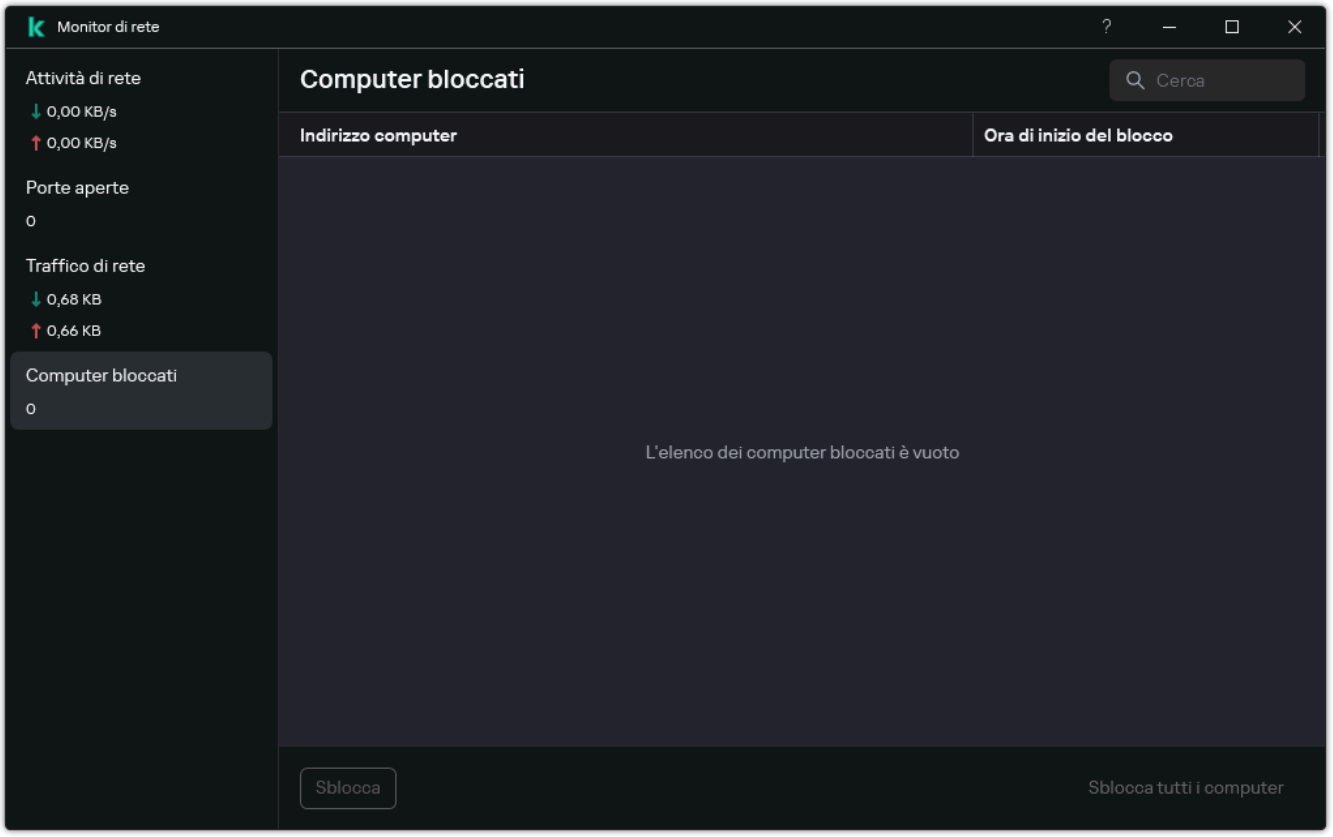
Per sbloccare un computer:

1. Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **Monitor di rete**.
2. Passare alla scheda **Computer bloccati**.

   Viene visualizzato un elenco di computer bloccati (vedere la figura riportata di seguito).

   Kaspersky Endpoint Security cancella l'elenco dei blocchi al riavvio dell'applicazione e quando le impostazioni di Protezione minacce di rete vengono modificate.

3. Selezionare il computer che si desidera sbloccare e fare clic su **Sblocca**.



Elenco dei computer bloccati

Configurazione degli indirizzi delle esclusioni dal blocco

Kaspersky Endpoint Security è in grado di riconoscere un attacco di rete e bloccare una connessione di rete non protetta che sta trasmettendo un numero elevato di pacchetti (ad esempio da telecamere di sorveglianza). Per il funzionamento con dispositivi attendibili è possibile aggiungere gli indirizzi IP di questi dispositivi all'elenco delle esclusioni. È inoltre possibile selezionare il protocollo e la porta utilizzati per la comunicazione e consentire attività di rete specifiche.

Come configurare gli indirizzi delle esclusioni dal blocco in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Protezione minacce essenziale** → **Protezione minacce di rete**.
5. Nel blocco **Impostazioni Protezione minacce di rete**, fare clic sul pulsante **Esclusioni**.
6. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.
7. Immettere l'Indirizzo IP del computer da cui non devono essere bloccati gli attacchi di rete.

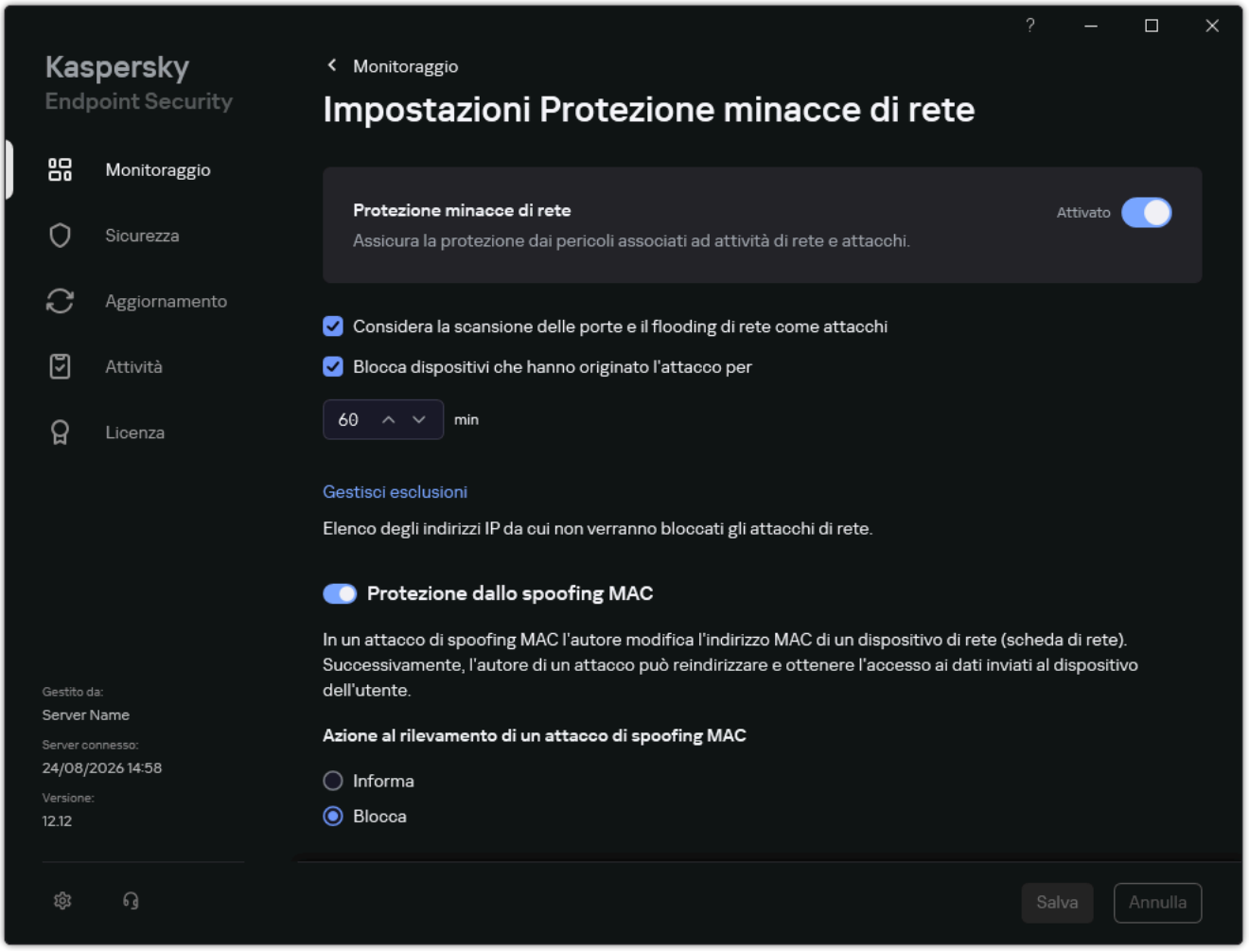
   Se necessario, selezionare il protocollo e le porte attraverso le quali vengono trasmessi i dati.
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare gli indirizzi esclusi dal blocco in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare alla sezione **Area attendibile**.
5. Nella finestra visualizzata, fare clic sul collegamento **Indirizzi IP**.
   Verrà visualizzata una finestra contenente un elenco di indirizzi IP attendibili.
6. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.
7. Immettere l'Indirizzo IP del computer da cui non devono essere bloccati gli attacchi di rete.
   Se necessario, specificare la subnet.
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare gli indirizzi delle esclusioni dal blocco nell'interfaccia utente dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce di rete**.



Impostazioni di Protezione minacce di Rete

3. Fare clic sul collegamento **Gestisci esclusioni**.
4. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.
5. Immettere l'Indirizzo IP del computer da cui non devono essere bloccati gli attacchi di rete.

   Se necessario, selezionare il protocollo e le porte attraverso le quali vengono trasmessi i dati.
6. Salvare le modifiche.

Esportazione e importazione dell'elenco delle esclusioni dal blocco

È possibile esportare l'elenco delle esclusioni in un file XML. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di indirizzi dello stesso tipo. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco delle esclusioni o per eseguire la migrazione dell'elenco in un server diverso.

Come esportare e importare un elenco di esclusioni in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale → Protezione minacce di rete**.
4. Nel blocco **Impostazioni Protezione minacce di rete**, fare clic sul pulsante **Esclusioni**.
5. Per esportare l'elenco delle regole:
   a. Selezionare le esclusioni che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.
      Se non è stata selezionata alcuna esclusione, Kaspersky Endpoint Security esporterà tutte le esclusioni.
   b. Fare clic sul pulsante → **Esporta**.
   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle esclusioni e selezionare la cartella in cui si desidera salvare il file.
   d. Salvare il file.
      Kaspersky Endpoint Security esporta l'intero elenco di esclusioni nel file XML.
6. Per importare l'elenco delle esclusioni:
   a. Fare clic sul pulsante → **Importa**.
   b. Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle esclusioni.
   c. Aprire il file.
      Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.
7. Salvare le modifiche.

Come esportare e importare un elenco di esclusioni in Kaspersky Security Center Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Comunicazione e protezione Web → Protezione minacce di rete**.
5. Nella parte superiore della finestra, fare clic sul collegamento **Indirizzi IP attendibili**.
   Verrà visualizzato l'elenco delle esclusioni.

6. Per esportare l'elenco delle regole:

   a. Selezionare le esclusioni che si desidera esportare.

   b. Fare clic sul pulsante → **Esporta**.

      Kaspersky Endpoint Security esporta l'elenco delle esclusioni in un file JSON nella cartella dei download predefinita.

7. Per importare l'elenco delle esclusioni:

   a. Fare clic sul pulsante → **Importa**.

      Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco delle esclusioni.

   b. Aprire il file.

      Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

8. Salvare le modifiche.

Configurazione di Protezione minacce di rete in base al tipo

Kaspersky Endpoint Security consente di gestire la protezione dai seguenti tipi di attacchi di rete:

- Il *flooding di rete* è un attacco alle risorse di rete di un'organizzazione (come i server Web). Questo attacco consiste nell'invio di un gran numero di richieste per sovraccaricare la larghezza di banda delle risorse di rete. Quando ciò accade, gli utenti non sono in grado di accedere alle risorse di rete dell'organizzazione.

- Un attacco di *scansione delle porte* consiste nella scansione di porte UDP, TCP e servizi di rete nel computer. Questo attacco consente all'autore dell'attacco di identificare il grado di vulnerabilità del computer prima di eseguire tipi più pericolosi di attacchi di rete. La scansione delle porte consente inoltre all'autore dell'attacco di identificare il sistema operativo nel computer e selezionare gli attacchi di rete appropriati per tale sistema operativo.

- Un *attacco di spoofing MAC* consiste nella modifica dell'indirizzo MAC di un dispositivo di rete (scheda di rete). L'autore di un attacco può quindi reindirizzare i dati inviati a un dispositivo a un altro dispositivo e ottenere l'accesso a questi dati. Kaspersky Endpoint Security consente di bloccare gli attacchi di spoofing MAC e di ricevere notifiche sugli attacchi.

È possibile disabilitare il rilevamento di questi tipi di attacchi nel caso in cui alcune delle applicazioni consentite eseguano operazioni tipiche di queste tipologie di attacchi. Ciò contribuirà a evitare falsi allarmi.

Per impostazione predefinita, Kaspersky Endpoint Security non monitora gli attacchi di flooding di rete, scansione delle porte e spoofing MAC.

Non è possibile configurare esclusioni separate per questi tipi di attacchi. Ciò significa che, anche se i singoli indirizzi IP vengono aggiunti alla zona attendibile, Kaspersky Endpoint Security blocca il computer che esegue l'attacco se rileva un attacco di questo tipo. È possibile abilitare o disabilitare il rilevamento di tali attacchi.

Non è consigliabile abilitare la protezione dallo spoofing MAC nelle macchine virtuali nell'infrastruttura Microsoft Hyper-V. A causa delle specifiche della piattaforma Microsoft Hyper-V, Kaspersky Industrial CyberSecurity for Nodes potrebbe bloccare l'hypervisor a causa di risultati falsi positivi.

Come configurare Protezione minacce di rete in base al tipo in Administration Console (MMC)

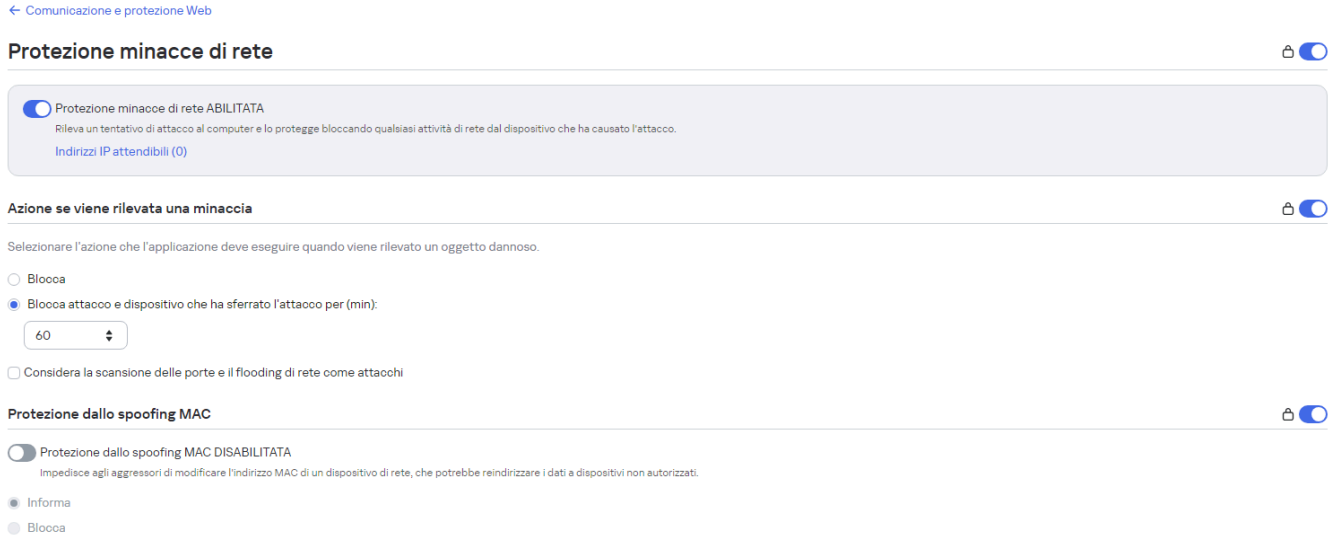
1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce essenziale → Protezione minacce di rete**.
4. Utilizzare la casella di controllo **Considera la scansione delle porte e il flooding di rete come attacchi** per abilitare o disabilitare il rilevamento di questi attacchi.

   Se questa funzionalità è abilitata, Kaspersky Endpoint Security monitora il traffico di rete per la scansione delle porte e il sovraccarico della rete. Se viene rilevato tale comportamento, l'applicazione avvisa l'utente e invia l'evento corrispondente a Kaspersky Security Center. L'applicazione fornisce informazioni sul computer che sta effettuando le richieste. Queste informazioni sono necessarie per una risposta tempestiva. Tuttavia, Kaspersky Endpoint Security non blocca il computer che sta effettuando le richieste, poiché tale traffico potrebbe essere un evento normale nella rete aziendale.
5. Nella sezione **Modalità di protezione dallo spoofing MAC** selezionare una delle seguenti opzioni:
   - **Non monitorare spoofing MAC**.
   - **Informa**.
   - **Blocca**.
6. Salvare le modifiche.

Come configurare Protezione minacce di Rete in base al tipo in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Comunicazione e protezione Web → Protezione minacce di rete**.



Impostazioni di Protezione minacce di Rete

5. Utilizzare la casella di controllo **Considera la scansione delle porte e il flooding di rete come attacchi** per abilitare o disabilitare il rilevamento di questi attacchi.

   Se questa funzionalità è abilitata, Kaspersky Endpoint Security monitora il traffico di rete per la scansione delle porte e il sovraccarico della rete. Se viene rilevato tale comportamento, l'applicazione avvisa l'utente e invia l'evento corrispondente a Kaspersky Security Center. L'applicazione fornisce informazioni sul computer che sta effettuando le richieste. Queste informazioni sono necessarie per una risposta tempestiva. Tuttavia, Kaspersky Endpoint Security non blocca il computer che sta effettuando le richieste, poiché tale traffico potrebbe essere un evento normale nella rete aziendale.

6. In **Protezione dallo spoofing MAC** configurare il rilevamento degli attacchi di spoofing MAC:

   a. Utilizzare l'interruttore **Protezione dallo spoofing MAC ABILITATA** per abilitare o disabilitare il rilevamento di questi attacchi.

   b. Selezionare l'azione da eseguire quando viene rilevato un attacco di spoofing MAC:

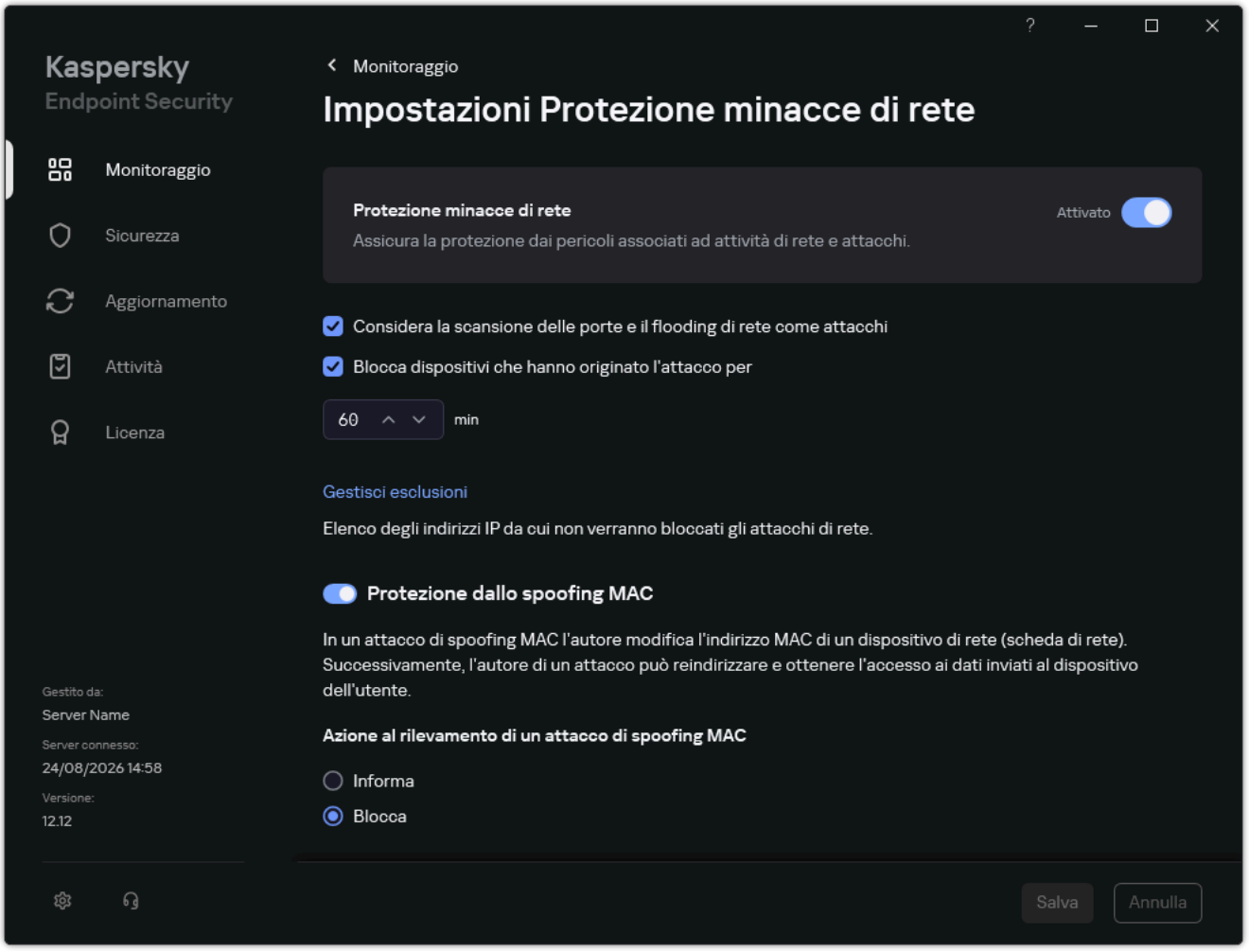
      - **Informa**.
      - **Blocca**.

7. Salvare le modifiche.

Come configurare Protezione minacce di rete in base al tipo nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Protezione minacce di rete**.



Impostazioni di Protezione minacce di Rete

3. Utilizzare l'interruttore **Considera la scansione delle porte e il flooding di rete come attacchi** per abilitare o disabilitare il rilevamento di questi attacchi.

   Se questa funzionalità è abilitata, Kaspersky Endpoint Security monitora il traffico di rete per la scansione delle porte e il sovraccarico della rete. Se viene rilevato tale comportamento, l'applicazione avvisa l'utente e invia l'evento corrispondente a Kaspersky Security Center. L'applicazione fornisce informazioni sul computer che sta effettuando le richieste. Queste informazioni sono necessarie per una risposta tempestiva. Tuttavia, Kaspersky Endpoint Security non blocca il computer che sta effettuando le richieste, poiché tale traffico potrebbe essere un evento normale nella rete aziendale.

4. Utilizzare l'interruttore **Protezione dallo spoofing MAC** per abilitare o disabilitare il rilevamento di questi attacchi.

5. Nella sezione **Azione al rilevamento di un attacco di spoofing MAC** selezionare una delle seguenti opzioni:

   - **Informa**.
   - **Blocca**.

6. Salvare le modifiche.

Firewall

Il componente Firewall blocca le connessioni non autorizzate al computer in Internet o sulla rete locale. Firewall controlla anche l'attività di rete delle applicazioni nel computer. Questo consente di proteggere la LAN aziendale dal furto di identità e da altri attacchi. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e *regole di rete* predefinite.

Network Agent viene utilizzato per l'interazione con Kaspersky Security Center. Firewall crea automaticamente le regole di rete necessarie per il funzionamento dell'applicazione e di Network Agent. Successivamente Firewall apre diverse porte nel computer. Le porte aperte dipendono dal ruolo del computer (ad esempio il ruolo di punto di distribuzione). Per ulteriori informazioni sulle porte che verranno aperte nel computer, consultare la Guida di Kaspersky Security Center.

Regole di rete

È possibile configurare le regole di rete ai seguenti livelli:

- *Regole per i pacchetti di rete*. Le regole per i pacchetti di rete applicano restrizioni ai pacchetti di rete, indipendentemente dall'applicazione. Le regole di questo tipo limitano il traffico di rete in entrata e in uscita tramite specifiche porte del protocollo dati selezionato. Kaspersky Endpoint Security ha regole predefinite per i pacchetti di rete con autorizzazioni consigliate dagli esperti di Kaspersky.

- *Regole di rete dell'applicazione*. Le regole di rete dell'applicazione applicano restrizioni all'attività di rete per una specifica applicazione. Tengono conto non solo delle caratteristiche del pacchetto di rete, ma anche della specifica applicazione a cui il pacchetto di rete è indirizzato o da cui è stato generato.

L'accesso controllato delle applicazioni alle risorse del sistema operativo, ai processi e ai dati personali viene garantito dal componente Prevenzione Intrusioni Host utilizzando *i diritti delle applicazioni*.

Durante il primo avvio dell'applicazione, Firewall esegue le seguenti azioni:

1. Verifica la sicurezza dell'applicazione utilizzando i database anti-virus scaricati.

2. Verifica la sicurezza dell'applicazione in Kaspersky Security Network.

   È consigliabile partecipare a Kaspersky Security Network per un miglior funzionamento di Firewall.

3. Colloca l'applicazione in uno dei gruppi di attendibilità: *Attendibili*, *Restrizione bassa*, *Restrizione alta*, *Non attendibili*.

   Un gruppo di attendibilità definisce i diritti a cui Kaspersky Endpoint Security fa riferimento durante il controllo delle attività delle applicazioni. Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità in base al livello di pericolosità che l'applicazione può rappresentare per il computer.

   Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità per i componenti Firewall e Prevenzione Intrusioni Host. Non è possibile modificare il gruppo di attendibilità solo per Firewall o Prevenzione Intrusioni Host.

Se si rifiuta di partecipare a KSN o non è disponibile alcuna rete, Kaspersky Endpoint Security inserisce l'applicazione in un gruppo di attendibilità in base alle impostazioni del componente Prevenzione Intrusioni Host. Dopo la ricezione della reputazione dell'applicazione da KSN, il gruppo di attendibilità può essere modificato automaticamente.

4. Blocca l'attività di rete dell'applicazione in base al gruppo di attendibilità. Ad esempio, alle applicazioni nel gruppo di attendibilità *Restrizione alta* non è consentito l'utilizzo di nessuna connessione di rete.

Al successivo avvio dell'applicazione, Kaspersky Endpoint Security verifica l'integrità dell'applicazione. Se l'applicazione non è stata modificata, il componente utilizza le regole di rete correnti. Se l'applicazione è stata modificata, Kaspersky Endpoint Security la analizza come se si trattasse del primo avvio.

Priorità delle regole di rete

Ogni regola ha una priorità. Più alta è la posizione di una regola nell'elenco, maggiore è la priorità. Se l'attività di rete viene aggiunta a diverse regole, Firewall regola l'attività di rete in base alla regola con la priorità più elevata.

Le regole per i pacchetti di rete hanno una priorità superiore rispetto alle regole di rete per le applicazioni. Se per lo stesso tipo di attività di rete sono specificate sia regole per i pacchetti di rete che regole di rete per le applicazioni, l'attività viene gestita in base alle regole per i pacchetti di rete.

Le regole di rete per le applicazioni funzionano in un modo particolare. La regola di rete per le applicazioni include regole di accesso basate sullo stato della rete: *Rete pubblica*, *Rete locale*, *Rete attendibile*. Ad esempio, per impostazione predefinita per le applicazioni nel gruppo di attendibilità *Restrizione alta* non è autorizzata alcuna attività di rete nelle reti con qualsiasi stato. Se viene specificata una regola di rete per una singola applicazione (applicazione padre), i processi figlio delle altre applicazioni verranno eseguiti in base alla regola di rete dell'applicazione padre. Se non esiste una regola di rete per l'applicazione, i processi figlio verranno eseguiti in base alla regola di accesso alla rete del gruppo di attendibilità dell'applicazione.

Se ad esempio hai vietato qualsiasi attività di rete nelle reti con qualsiasi stato per tutte le applicazioni, ad eccezione del browser X e avvii l'installazione del browser Y (processo figlio) dal browser X (applicazione padre), il programma di installazione del browser Y accederà alla rete e scaricherà i file necessari. Dopo l'installazione, al browser Y verrà negata qualsiasi connessione di rete in base alle impostazioni del firewall. Per vietare l'attività di rete del programma di installazione del browser Y come processo figlio, è necessario aggiungere una regola di rete per il programma di installazione del browser Y.

Tipi di connessioni di rete

Firewall consente di controllare l'attività di rete in base al tipo di connessione di rete. Kaspersky Endpoint Security riceve il tipo di connessione di rete dal sistema operativo del computer. Il tipo di connessione di rete nel sistema operativo viene impostato dall'utente durante la configurazione della connessione. È possibile modificare il tipo di connessione di rete nelle impostazioni di Kaspersky Endpoint Security. Firewall monitorerà l'attività di rete in base al tipo di rete specificato nelle impostazioni di Kaspersky Endpoint Security e non nel sistema operativo.

Sono disponibili i seguenti tipi di connessioni di rete:

- **Rete pubblica**. La rete non è protetta da applicazioni anti-virus, firewall o filtri (ad esempio la rete Wi-Fi di un bar). Quando l'utente utilizza un computer connesso a una rete di questo tipo, Firewall blocca l'accesso ai file e alle stampanti del computer in uso. Anche gli utenti esterni non sono in grado di accedere ai dati tramite cartelle condivise e di accedere in remoto al desktop del computer in uso. Firewall filtra l'attività di rete di ogni applicazione in base alle regole di rete impostate per l'applicazione.

  Per impostazione predefinita, Firewall assegna a Internet il tipo *Rete pubblica*. Non è possibile modificare il tipo di Internet.

- **Rete locale**. Rete per utenti con accesso limitato a file e stampanti in questo computer (ad esempio una rete LAN aziendale o una rete domestica).

- **Rete attendibile**. Rete sicura in cui il computer non è esposto ad attacchi o a tentativi di accesso non autorizzato ai dati. Per le reti di questa categoria, Firewall consente qualsiasi attività di rete.

Compatibilità con Windows Defender Firewall

Il sistema operativo dispone di un firewall integrato, *Windows Defender Firewall*. L'applicazione si comporta in modo diverso a seconda del tipo di sistema operativo:

- **Postazione di lavoro**. L'utilizzo di Kaspersky Firewall insieme a Windows Defender Firewall può causare malfunzionamenti del sistema operativo. Pertanto, Kaspersky Endpoint Security dispone di un meccanismo che impedisce l'utilizzo simultaneo di entrambi i firewall. Quando si attiva Kaspersky Firewall, il sistema operativo disattiva automaticamente Windows Defender Firewall. Quando si disattiva Kaspersky Firewall, il sistema operativo riattiva automaticamente Windows Defender Firewall per mantenere protetto il computer.

- **Server**. Kaspersky Firewall e Windows Defender Firewall non sono compatibili tra loro. Il programma di installazione di Kaspersky Endpoint Security rimuove automaticamente Windows Defender Firewall durante l'installazione dell'applicazione.

Abilitazione o disabilitazione di Firewall

Per impostazione predefinita, Firewall è abilitato e funziona in modalità ottimale.

Come abilitare o disabilitare il firewall in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio selezionare **Protezione minacce essenziale → Firewall**.
4. Utilizzare la casella di controllo **Firewall** per abilitare o disabilitare il componente.
5. Salvare le modifiche.

Come abilitare o disabilitare Firewall in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Selezionare **Comunicazione e protezione Web** → **Firewall**.
5. Utilizzare l'interruttore **Firewall ABILITATO** per abilitare o disabilitare il componente.
6. Salvare le modifiche.

Come abilitare o disabilitare il firewall nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Firewall**.
3. Utilizzare l'interruttore **Firewall** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Di conseguenza, se il firewall è abilitato, Kaspersky Endpoint Security controlla le attività di rete e blocca le connessioni di rete non autorizzate al computer, nonché le attività di rete non autorizzate delle applicazioni nel computer. Le attività di rete sono controllate anche dal componente Protezione minacce di rete. Il componente Protezione minacce di Rete (chiamato anche Intrusion Detection System, IDS) monitora il traffico di rete in entrata alla ricerca di attività caratteristiche degli attacchi di rete.

Kaspersky Endpoint Security registra gli eventi di attacco alla rete nei propri rapporti indipendentemente dalle impostazioni del firewall. Anche se il firewall blocca la connessione di rete utilizzando le regole e quindi impedisce un attacco di rete, il componente Protezione minacce di rete registra gli eventi di attacco di rete. È necessario per generare informazioni statistiche sugli attacchi di rete nei computer dell'organizzazione.

Modifica del tipo di connessione di rete

Per impostazione predefinita, Firewall assegna a Internet il tipo *Rete pubblica*. Non è possibile modificare il tipo di Internet.

Per modificare il tipo della connessione di rete:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Firewall**.
3. Fare clic su **Reti disponibili**.
4. Selezionare la connessione di rete di cui si desidera modificare il tipo.

5. Nella colonna **Tipo di rete** selezionare il tipo di connessione di rete:

   - **Rete pubblica**. La rete non è protetta da applicazioni anti-virus, firewall o filtri (ad esempio la rete Wi-Fi di un bar). Quando l'utente utilizza un computer connesso a una rete di questo tipo, Firewall blocca l'accesso ai file e alle stampanti del computer in uso. Anche gli utenti esterni non sono in grado di accedere ai dati tramite cartelle condivise e di accedere in remoto al desktop del computer in uso. Firewall filtra l'attività di rete di ogni applicazione in base alle regole di rete impostate per l'applicazione.

   - **Rete locale**. Rete per utenti con accesso limitato a file e stampanti in questo computer (ad esempio una rete LAN aziendale o una rete domestica).

   - **Rete attendibile**. Rete sicura in cui il computer non è esposto ad attacchi o a tentativi di accesso non autorizzato ai dati. Per le reti di questa categoria, Firewall consente qualsiasi attività di rete.

6. Salvare le modifiche.

Gestione delle regole per i pacchetti di rete

Durante la gestione delle regole per i pacchetti di rete è possibile eseguire le seguenti azioni:

- Creare una nuova regola per i pacchetti di rete.

  È possibile creare una nuova regola per i pacchetti di rete creando un set di condizioni e azioni applicate ai pacchetti di rete e ai flussi di dati.

- Abilitare o disabilitare una regola per i pacchetti di rete.

  Tutte le regole per i pacchetti di rete create da Firewall per impostazione predefinita dispongono dello stato *Abilitato*. Quando una regola per i pacchetti di rete è abilitata, Firewall applica la regola.

  È possibile disabilitare qualsiasi regola per i pacchetti di rete selezionata nell'elenco delle regole per i pacchetti di rete. Quando una regola per i pacchetti di rete è disabilitata, Firewall non applica temporaneamente la regola.

  > Per impostazione predefinita, una nuova regola personalizzata per i pacchetti di rete viene aggiunta all'elenco delle regole per i pacchetti di rete con lo stato *Abilitato*.

- Modificare le impostazioni di una regola per i pacchetti di rete esistente.

  Dopo avere creato una nuova regola per i pacchetti di rete, è possibile modificarne le impostazioni in qualsiasi momento.

- Modificare l'azione eseguita da Firewall per una regola per i pacchetti di rete.

  Nell'elenco delle regole per i pacchetti di rete è possibile modificare l'azione eseguita da Firewall quando viene rilevata un'attività di rete che corrisponde a una specifica regola per i pacchetti di rete.

- Modificare la priorità di una regola per i pacchetti di rete.

  È possibile aumentare o ridurre la priorità di una regola per i pacchetti di rete selezionata nell'elenco.

- Rimuovere una regola per i pacchetti di rete.

  È possibile rimuovere una regola per i pacchetti di rete in modo da interrompere l'applicazione della regola da parte di Firewall quando viene rilevata attività di rete e per rimuovere la regola dall'elenco delle regole per i pacchetti di rete con stato *Disabilitato*.

Creazione di una regola per i pacchetti di rete

Firewall filtra tutte le attività di rete nel computer in base alle regole per i pacchetti di rete. Le regole per i pacchetti di rete contengono le condizioni (ad esempio, direzione, protocollo) che Firewall applica per controllare le connessioni di rete del computer. Le regole per i pacchetti di rete specificano inoltre l'azione che Firewall esegue con la connessione corrispondente alla regola (consentire o bloccare la connessione).

Suggerimenti per la creazione di regole per i pacchetti di rete

È possibile specificare un indirizzo IP o un intervallo di indirizzi IP per filtrare le attività di rete. È inoltre possibile specificare un nome DNS.

Se in una regola viene utilizzato un nome DNS, Kaspersky Endpoint Security risolve il nome DNS in un indirizzo IP e successivamente tratta la regola come se in essa fosse specificato tale indirizzo IP.

Kaspersky Endpoint Security può risolvere i nomi DNS nei seguenti casi:

- Avvio dell'applicazione
- Modifica delle impostazioni di Firewall

Quando l'applicazione risolve i nomi DNS dal computer in cui è installata, può essere inviato un numero elevato di query al server DNS. Per evitare questa situazione, è consigliabile utilizzare indirizzi IP anziché nomi DNS durante la creazione delle regole.

In alcuni casi, l'utilizzo dei nomi DNS nei nomi dei pacchetti di rete potrebbe non essere sicuro, poiché il proprietario del server DNS può modificare i parametri del record DNS. Un utente malintenzionato può inoltre falsificare i messaggi DNS ed eludere le regole di Firewall.

È possibile controllare le connessioni di rete in base ai nomi DNS utilizzando le regole di Controllo Web. Se è necessario specificare un nome DNS nelle regole di Firewall:

- Garantire la sicurezza della LAN aziendale.
- Garantire la sicurezza della memorizzazione nella cache e dei server DNS autorevoli.
- Abilitare la protezione del record DNS dalle modifiche.

Quando si creano regole per i pacchetti di rete, è necessario tenere presente che queste sono prioritarie rispetto alle regole di rete per le applicazioni.

Metodi di creazione delle regole per i pacchetti di rete

È possibile creare una regola per i pacchetti di rete nei seguenti modi:

- Utilizzare lo strumento Monitor di rete.

  Monitor di Rete è uno strumento progettato per la visualizzazione in tempo reale di informazioni sulle attività di rete nel computer di un utente. Questo strumento è comodo perché non è necessario configurare tutte le impostazioni delle regole. Alcune impostazioni di Firewall verranno inserite automaticamente dai dati di Monitor di rete. Monitor di rete è disponibile solo nell'interfaccia dell'applicazione.

- Configurare le impostazioni di Firewall.

  Questo consente di ottimizzare le impostazioni di Firewall. È possibile creare regole per qualsiasi attività di rete, anche se al momento non è presente alcuna attività di rete.

Come utilizzare lo strumento Monitor di rete per creare una regola per i pacchetti di rete nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **Monitor di rete**.
2. Passare alla scheda **Attività di rete**.

   La scheda **Attività di rete** mostra tutte le connessioni di rete attualmente attive con il computer. Vengono visualizzate le connessioni di rete sia in entrata che in uscita.
3. Nel menu di scelta rapida di una connessione di rete, selezionare **Crea regola per i pacchetti di rete**.

   Verranno visualizzate le proprietà delle regole di rete.
4. Impostare lo stato **Attivo** per la regola per i pacchetti.
5. Immettere manualmente il nome del servizio di rete nel campo **Nome**.
6. Configurare le impostazioni delle regole di rete (vedere la tabella seguente).

   È possibile selezionare un modello di regole predefinito facendo clic sul collegamento **Modello regola di rete**. I modelli di regole descrivono le connessioni di rete utilizzate più di frequente.

   Tutte le impostazioni delle regole di rete verranno compilate automaticamente.
7. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.
8. Fare clic su **Salva**.

   La nuova regola di rete verrà aggiunta all'elenco.
9. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.
10. Salvare le modifiche.

Come utilizzare le impostazioni di Firewall per creare una regola per i pacchetti di rete nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Firewall**.

3. Fare clic su **Regole per i pacchetti**.

   Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.

4. Utilizzando l'elenco a discesa **Aggiungi**, selezionare la posizione della regola nell'elenco: all'inizio dell'elenco, alla fine dell'elenco o accanto alla regola selezionata.

   La posizione della regola nell'elenco determina la priorità della regola. La regola all'inizio dell'elenco ha la priorità più alta.

5. Impostare lo stato **Attivo** per la regola per i pacchetti.

6. Immettere manualmente il nome del servizio di rete nel campo **Nome**.

7. Configurare le impostazioni delle regole di rete (vedere la tabella seguente).

   È possibile selezionare un modello di regole predefinito facendo clic sul collegamento **Modello regola di rete**. I modelli di regole descrivono le connessioni di rete utilizzate più di frequente.

   Tutte le impostazioni delle regole di rete verranno compilate automaticamente.

8. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.

9. Fare clic su **Salva**.

   La nuova regola di rete verrà aggiunta all'elenco.

10. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.

11. Salvare le modifiche.

Come creare una regola per i pacchetti di rete in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio selezionare **Protezione minacce essenziale → Firewall**.

4. Nel blocco **Impostazioni di Firewall**, fare clic sul pulsante **Impostazioni**.

   Verrà visualizzato l'elenco delle regole dei pacchetti di rete e l'elenco delle regole di rete dell'applicazione.

5. Passare alla scheda **Regole per i pacchetti di rete**.

   Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.

6. Utilizzando l'elenco a discesa **Aggiungi**, selezionare la posizione della regola nell'elenco: all'inizio dell'elenco, alla fine dell'elenco o accanto alla regola selezionata.

   La posizione della regola nell'elenco determina la priorità della regola. La regola all'inizio dell'elenco ha la priorità più alta.

7. Immettere manualmente il nome del servizio di rete nel campo **Nome**.

8. Configurare le impostazioni delle regole di rete (vedere la tabella seguente).

   È possibile selezionare un modello di regole predefinito facendo clic sul pulsante . I modelli di regole descrivono le connessioni di rete utilizzate più di frequente.

   Tutte le impostazioni delle regole di rete verranno compilate automaticamente.

9. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.

10. Salvare la nuova regola di rete.

11. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.

12. Salvare le modifiche.

Firewall controllerà i pacchetti di rete in base alla regola. È possibile disabilitare una regola per i pacchetti dall'esecuzione di Firewall senza eliminarla dall'elenco. A tale scopo, deselezionare la casella di controllo accanto all'oggetto.

Come creare una regola per i pacchetti di rete in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Selezionare **Comunicazione e protezione Web** → **Firewall**.

5. Selezionare la scheda **Regole per i pacchetti di rete**.

   Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.

6. Fare clic su **Aggiungi**.

   Si apre il modulo per una nuova regola di rete.

7. Immettere manualmente il nome del servizio di rete nel campo **Nome regola**.

8. Configurare le impostazioni delle regole di rete (vedere la tabella seguente).

   È possibile selezionare un modello di regole predefinito facendo clic sul collegamento **Seleziona modello di regola**. I modelli di regole descrivono le connessioni di rete utilizzate più di frequente.

   Tutte le impostazioni delle regole di rete verranno compilate automaticamente.

9. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.

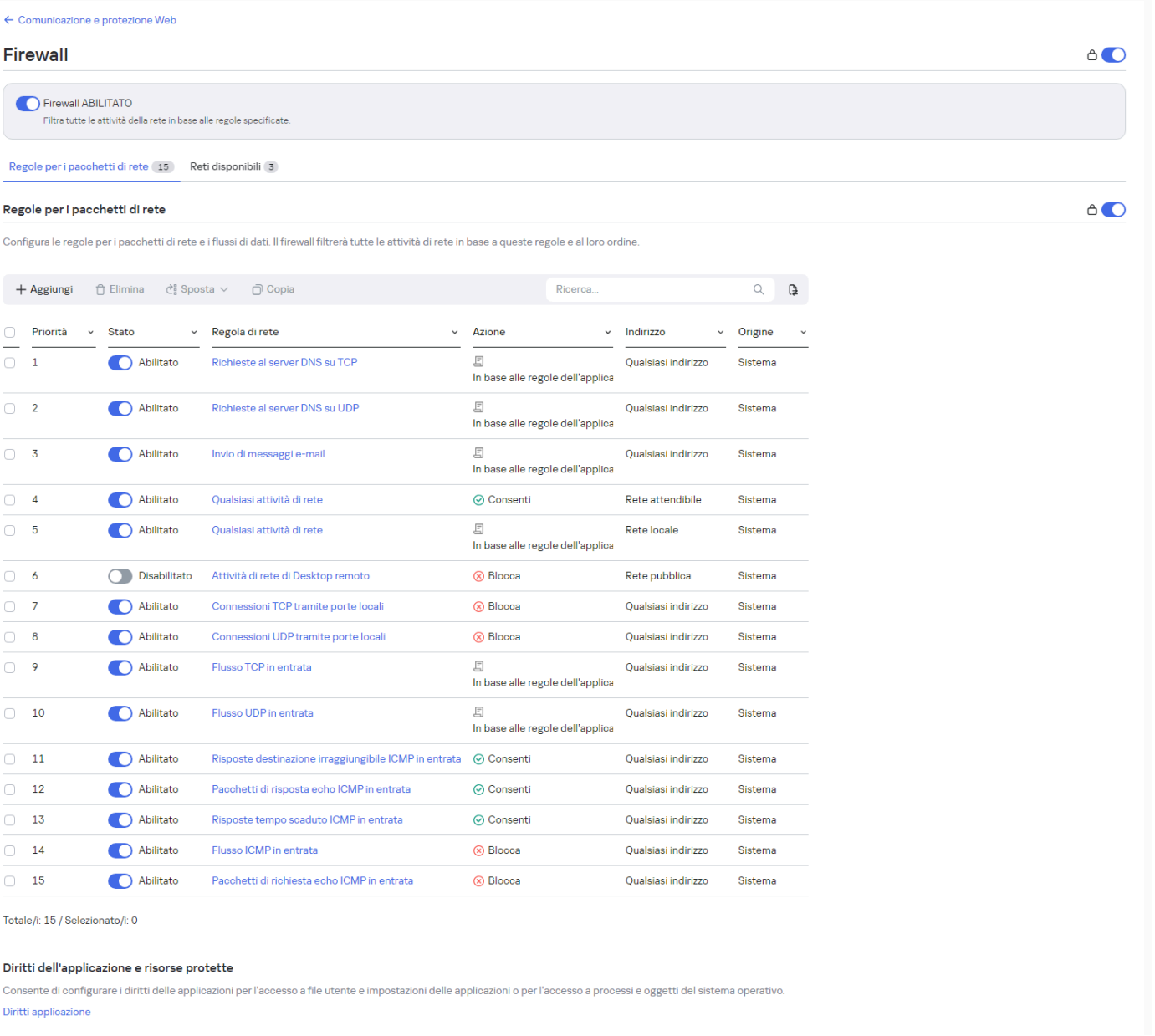
10. Salvare la regola di rete.

    La nuova regola di rete verrà aggiunta all'elenco.

11. Utilizzare i pulsanti **Sposta** per impostare la priorità della regola di rete.

12. Salvare le modifiche.

Firewall controllerà i pacchetti di rete in base alla regola. È possibile disabilitare una regola per i pacchetti dall'esecuzione di Firewall senza eliminarla dall'elenco. Utilizzare l'interruttore nella colonna **Stato** per abilitare o disabilitare la regola per i pacchetti.



Regole per i pacchetti di Firewall

Impostazioni delle regole per i pacchetti di rete

Parametro	Descrizione
Azione	**Consenti**. **Blocca**. **In base alle regole dell'applicazione**. Se questa opzione è selezionata, Firewall applica le regole di rete dell'applicazione alla connessione di rete.
Protocollo	Controlla le attività di rete tramite il protocollo selezionato: TCP, UDP, ICMP, ICMPv6, IGMP e GRE. Se come protocollo è selezionato ICMP o ICMPv6, è possibile definire il codice e il tipo di pacchetto ICMP. Se come tipo di protocollo è selezionato TCP o UDP, è possibile specificare i numeri di porta del computer locale e remoto tra cui monitorare la connessione. Intervallo di valori possibili per i numeri di porta: 0-65535. In ogni campo è possibile immettere più valori separati da `,` oppure specificare un intervallo di valori utilizzando `-`. Ad esempio: • `100,101` • `100-130` • `100,110-130`

Parametro	Descrizione
Direzione	**In entrata (pacchetto)**. Firewall applica la regola di rete a tutti i pacchetti di rete in entrata. **In entrata**. Firewall applica la regola di rete a tutti i pacchetti di rete inviati tramite una connessione avviata da un computer remoto. **In entrata/In uscita**. Firewall applica la regola di rete a tutti i pacchetti di rete in entrata e in uscita. **In uscita (pacchetto)**. Firewall applica la regola di rete a tutti i pacchetti di rete in uscita. **In uscita**. Firewall applica la regola di rete a tutti i pacchetti di rete inviati tramite una connessione avviata dal computer dell'utente.
Schede di rete	Schede di rete che possono inviare e/o ricevere pacchetti di rete. Specificando le impostazioni delle schede di rete è possibile differenziare i pacchetti di rete inviati da quelli ricevuti dalle schede di rete con indirizzi IP identici.
Time to live (TTL)	Limitazione del controllo dei pacchetti di rete in base alla loro durata (Time to Live, TTL).
Indirizzi remoti	Indirizzi di rete dei computer remoti che possono inviare e/o ricevere i pacchetti di rete. Firewall applica la regola di rete all'intervallo specificato di indirizzi di rete remoti. È possibile includere tutti gli indirizzi IP in una regola di rete, creare un elenco separato di indirizzi IP, specificare un intervallo di indirizzi IP o selezionare una subnet (Reti attendibili, Reti locali, Reti pubbliche). È inoltre possibile specificare un nome DNS di un computer anziché il suo indirizzo IP. È necessario utilizzare i nomi DNS solo per computer LAN o servizi interni. L'interazione con i servizi cloud (come Microsoft Azure) e altre risorse Internet deve essere gestita dal componente Controllo Web. Se nella regola per i pacchetti di rete è stato aggiunto un nome DNS per il quale non è stato possibile determinare l'indirizzo IP, Kaspersky Endpoint Security mostrerà un avviso. Nell'elenco delle regole per i pacchetti di rete in Web Console, viene aggiunta una colonna con una descrizione dell'errore. In Administration Console (MMC), la descrizione dell'errore non è disponibile. Tali regole dei pacchetti sono evidenziate con colori.
Indirizzi locali	Indirizzi di rete dei computer che possono inviare e ricevere i pacchetti di rete. Firewall applica una regola di rete all'intervallo specificato di indirizzi di rete locali. È possibile includere tutti gli indirizzi IP in una regola di rete, creare un elenco separato di indirizzi IP o specificare un intervallo di indirizzi IP. L'applicazione memorizza gli indirizzi locali solo se viene specificato un elenco di indirizzi remoti. In altre parole, il valore **Indirizzi dall'elenco** è stato selezionato per **Indirizzi remoti** ed è stato aggiunto almeno un indirizzo. A volte l'indirizzo locale non può essere ottenuto per le applicazioni. In tal caso, questo parametro viene ignorato.

Abilitazione o disabilitazione di una regola per i pacchetti di rete

Per abilitare o disabilitare una regola per i pacchetti di rete:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Firewall**.
3. Fare clic su **Regole per i pacchetti**.
   Verrà visualizzato un elenco di regole per i pacchetti di rete predefinite configurate da Firewall.
4. Selezionare la regola per i pacchetti di rete desiderata nell'elenco.
5. Utilizzare l'interruttore nella colonna **Stato** per abilitare o disabilitare la regola.
6. Salvare le modifiche.

Modifica dell'azione eseguita da Firewall per una regola per i pacchetti di rete

Per modificare l'azione di Firewall applicata a una regola per i pacchetti di rete:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Firewall**.
3. Fare clic su **Regole per i pacchetti**.

   Verrà visualizzato un elenco di regole per i pacchetti di rete predefinite configurate da Firewall.
4. Selezionarla nell'elenco delle regole per i pacchetti di rete, quindi fare clic sul pulsante **Modifica**.
5. Nell'elenco a discesa **Azione** selezionare l'azione che deve essere eseguita dal componente Firewall se viene rilevato questo tipo di attività di rete:
   - **Consenti**.
   - **Blocca**.
   - **In base alle regole dell'applicazione**. Se questa opzione è selezionata, Firewall applica le regole di rete dell'applicazione alla connessione di rete.
6. Salvare le modifiche.

Modifica della priorità di una regola per i pacchetti di rete

La priorità di una regola per i pacchetti di rete è determinata dalla relativa posizione nell'elenco delle regole per i pacchetti di rete. La prima regola per i pacchetti di rete nell'elenco delle regole per i pacchetti di rete ha la priorità più alta.

Ogni regola per i pacchetti di rete creata manualmente viene aggiunta in fondo all'elenco delle regole per i pacchetti di rete e ha la priorità più bassa.

Firewall elabora le regole nell'ordine in cui compaiono nell'elenco delle regole per i pacchetti di rete, dalla prima all'ultima. In base a ciascuna regola per i pacchetti di rete elaborata per una particolare connessione di rete, Firewall consente o blocca l'accesso di rete all'indirizzo e alla porta specificati nelle impostazioni della connessione di rete.

Per modificare la priorità delle regole per i pacchetti di rete:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Firewall**.
3. Fare clic su **Regole per i pacchetti**.

   Verrà visualizzato un elenco di regole per i pacchetti di rete predefinite configurate da Firewall.
4. Nell'elenco selezionare la regola per i pacchetti di rete di cui si desidera modificare la priorità.

5. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.

6. Salvare le modifiche.

Esportazione e importazione di regole per i pacchetti di rete

È possibile esportare l'elenco delle regole per i pacchetti di rete in un file XML. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di regole dello stesso tipo. È possibile utilizzare la funzione di esportazione/importazione per eseguire il backup delle regole per i pacchetti di rete o per eseguire la migrazione dell'elenco in un server diverso.

Come esportare e importare un elenco di regole per i pacchetti di rete in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio selezionare **Protezione minacce essenziale → Firewall**.

4. Nel blocco **Impostazioni di Firewall**, fare clic sul pulsante **Impostazioni**.

   Verrà visualizzato l'elenco delle regole dei pacchetti di rete e l'elenco delle regole di rete dell'applicazione.

5. Passare alla scheda **Regole per i pacchetti di rete**.

6. Per esportare l'elenco delle regole per i pacchetti di rete:

   a. Selezionare le regole che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.

      Se non è stata selezionata alcuna regola, Kaspersky Endpoint Security esporterà tutte le regole.

   b. Fare clic sul collegamento **Esporta**.

   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle regole e selezionare la cartella in cui si desidera salvare il file.

   d. Salvare il file.

      Kaspersky Endpoint Security esporta l'intero elenco di regole nel file XML.

7. Per importare un elenco di regole per i pacchetti di rete:

   a. Fare clic sul collegamento **Importa**.

      Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle regole.

   b. Aprire il file.

      Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

8. Salvare le modifiche.

Come esportare e importare un elenco di regole per i pacchetti di rete in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Selezionare **Comunicazione e protezione Web** → **Firewall**.
5. Per esportare l'elenco delle regole, nella sezione **Regole per i pacchetti di rete**:

   a. Selezionare le regole che si desidera esportare.

   b. Fare clic sul pulsante → **Esporta**.

   Kaspersky Endpoint Security esporta l'elenco delle regole in un file JSON nella cartella dei download predefinita.
6. Per importare l'elenco delle regole, nella sezione **Regole per i pacchetti di rete**:

   a. Fare clic sul pulsante → **Importa**.

   Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco delle regole.

   b. Aprire il file.

   Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.
7. Salvare le modifiche.

Definizione delle regole per i pacchetti di rete in XML

Il firewall consente di esportare le regole per i pacchetti di rete in formato XML. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di regole dello stesso tipo.

Il file XML contiene due nodi principali: `Rules` e `Resources`. Il nodo `Rules` elenca le regole per i pacchetti di rete. Questo nodo contiene le regole configurate per impostazione predefinita (*regole predefinite*), nonché le regole aggiunte dall'utente (*regole personalizzate*).

Impostazioni dei commenti dei pacchetti di rete

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Parametro	Descrizione	Valore
`<key name="0000">`	Priorità della regola. Più basso è il valore, maggiore sarà la priorità.	Numero intero Il valore di priorità deve essere composto da 4 cifre. I nodi nel file XML devono essere ordinati per valore di priorità, a partire da `0000`.
`RuleId`	ID della regola.	**Regole predefinite** `100`: **Richieste al server DNS su TCP**. `101`: **Richieste al server DNS su UDP**. `102`: **Invio di messaggi e-mail**. `110`: **Qualsiasi attività di rete** (Reti attendibili). `125`: **Qualsiasi attività di rete** (Reti locali). `130`: **Attività di rete di Desktop remoto**. `131`: **Connessioni TCP tramite porte locali**. `132`: **Connessioni UDP tramite porte locali**. `133`: **Flusso TCP in entrata**. `134`: **Flusso UDP in entrata**. `137`: **Risposte destinazione irraggiungibile ICMP in entrata**. `138`: **Pacchetti di risposta echo ICMP in entrata**. `140`: **Risposte tempo scaduto ICMP in entrata**. `142`: **Flusso ICMP in entrata**. `266`: **Pacchetti di richiesta echo ICMPv6 in entrata**.
`RuleState`	Stato della regola.	`0`: la regola predefinita è disabilitata `1`: la regola predefinita è abilitata `2`: la regola personalizzata è disabilitata `3`: la regola personalizzata è abilitata
`RuleTypeId`	ID del tipo di regola.	`4`: regola per i pacchetti di rete.
`AppIdEx`	ID dell'applicazione a cui appartiene la regola per i pacchetti di rete.	Se la regola non appartiene ad alcuna applicazione, il valore è `0`.
`ResIdEx`	ID principale della risorsa con le impostazioni della regola. È possibile utilizzare questo identificatore per individuare un blocco con le impostazioni delle regole nel nodo `Resources`.	Numero intero
`ResIdEx2`	ID del tipo di rete.	`0`: **Qualsiasi indirizzo**. `50`: **Reti attendibili**. `51`: **Reti locali**. `52`: **Reti pubbliche**. `<Network Identifier>`: **Indirizzi dall'elenco** (gli indirizzi sono definiti manualmente).
`AccessFlag`	Valore del parametro **Azione**.	`0`: **Consenti**. `2`: **In base alle regole dell'applicazione**. `3`: **Blocca**. `4`: **Consenti** e **Registra eventi**. `6`: **In base alle regole dell'applicazione** e **Registra eventi**. `7`: **Blocca** e **Registra eventi**.
`</key>`		

Il nodo `Resources` contiene le impostazioni delle regole per i pacchetti di rete. Le impostazioni delle regole per i pacchetti di rete sono elencate nel blocco `<key name="0004">`.

Commenti delle regola per i pacchetti di rete personalizzati

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Impostazioni delle regole per i pacchetti di rete personalizzate

Parametro	Descrizione	Valore
`<key name="Data">`	ID del blocco di parametri.	Numero intero
`RemotePorts`	Valore del parametro **Porte remote**.	Elenco dell'intervallo di porte remote.
`LocalPorts`	Valore del parametro **Porte locali**.	Elenco dell'intervallo di porte locali.

Parametro	Descrizione	Valore
`AdapterBindings`	Valore del parametro **Schede di rete**.	`IpAddresses`: valore del parametro **Indirizzi IP**. `MacAddresses`: valore del parametro **Indirizzi MAC**. `AdapterName`: nome della schede di rete. `InterfaceType`: valore del parametro **Tipo di interfaccia**: • `0`: **Altro**. • `1`: **LoopBack**. • `2`: **Rete via cavo (Ethernet)**. • `3`: **Rete wireless (Wi-Fi)**. • `4`: **Tunnel**. • `5`: **Connessione PPP**. • `6`: **Connessione PPPoE**. • `7`: **Connessione VPN**. • `8`: **Connessione modem**.
`unique`	ID interno della struttura.	Numero intero Si consiglia di lasciare questo parametro immutato.
`Proto`	Valore del parametro **Protocollo**.	`0`: disabilitato. `1`: **ICMP**. `2`: **IGMP**. `6`: **TCP**. `17`: **UDP**. `47`: **GRE**. `58`: **ICMPv6**.
`Direction`	Valore del parametro **Direzione**.	`1`: **In entrata (pacchetto)**. `2`: **In uscita (pacchetto)**. `3`: **In entrata/In uscita**. `4`: **In entrata**. `5`: **In uscita**.

Parametro	Descrizione	Valore
`IcmpType`	Valore del parametro **Tipo ICMP**.	**Protocollo ICMP** `0`: **Risposta Echo** (ICMP) o disabilitato. `3`: **Destinazione irraggiungibile** (ICMP). `4`: **Richiesta di rallentamento dell'origine**. `5`: **Reindirizzamento**. `6`: **Indirizzo host alternativo**. `8`: **Richiesta Echo**. `9`: **Annuncio router**. `10`: **Richiesta router**. `11`: **Tempo scaduto**. `12`: **Problema con il parametro**. `13`: **Timestamp**. `14`: **Risposta timestamp**. `15`: **Richiesta informazioni**. `16`: **Risposta informazioni**. `17`: **Richiesta maschera indirizzo**. `18`: **Risposta maschera indirizzo**. `30`: **Traceroute**. `31`: **Errore di conversione datagramma**. `32`: **Reindirizzamento host mobile**. `33`: **Where-Are-You IPv6**. `34`: **I-Am-Here IPv6**. `35`: **Richiesta registrazione mobile**. `36`: **Risposta registrazione mobile**. `37`: **Richiesta nome dominio**. `38`: **Risposta nome dominio**. `40`: **Photuris**. **Protocollo ICMPv6** `1`: **Destinazione irraggiungibile**. `2`: **Pacchetto di dimensioni troppo grandi**. `3`: **Tempo scaduto**. `4`: **Problema con il parametro**. `128`: **Richiesta Echo**. `129`: **Risposta Echo**. `130`: **Query listener multicast**. `131`: **Report listener multicast**. `132`: **Listener multicast completato**. `133`: **Richiesta router**. `134`: **Annuncio router**. `135`: **Richiesta router adiacente**. `136`: **Annuncio router adiacente**. `137`: **Messaggio reindirizzamento**. `138`: **Rinumerazione router**. `139`: **Query informazioni nodo ICMP**. `141`: **Messaggio richiesta individuazione inversa router adiacenti**. `142`: **Messaggio annuncio individuazione inversa router adiacenti**. `143`: **Report listener multicast versione 2**.

Parametro	Descrizione	Valore
		`144`: **Messaggio richiesta individuazione indirizzo agente principale**. `145`: **Messaggio risposta individuazione indirizzo agente principale**. `146`: **Richiesta prefisso mobile**. `147`: **Annuncio prefisso mobile**. `148`: **Messaggio richiesta percorso certificazione**. `149`: **Messaggio annuncio percorso certificazione**. `151`: **Annuncio router multicast**. `152`: **Richiesta router multicast**. `153`: **Terminazione router multicast**.
`IcmpCode`	Valore del parametro **Codice ICMP**.	`0`: **Codice 0** o disabilitato. `1`: **Codice 1**. `2`: **Codice 2**.
`Flags`	Puntatore dell'attributo della struttura.	Numero intero Si consiglia di lasciare questo parametro immutato.
`TTL`	Valore del parametro **Time to live (TTL)**.	Valore in secondi. Se disabilitato, il valore è `0`.
`</key>`		
`Id`	ID principale della risorsa (vedere il nodo `Rules`).	Numero intero
`ParentID`	ID del gruppo principale.	Numero intero Si consiglia di lasciare questo parametro immutato.
`Flags`	Stato della regola.	`6`: la regola è disabilitata. `38`: la regola è abilitata.
`Name`	Nome della regola per i pacchetti di rete.	Stringa

Gestione delle regole di rete delle applicazioni

Per impostazione predefinita, Kaspersky Endpoint Security raggruppa tutte le applicazioni installate nel computer in base al nome del produttore del software di cui vengono monitorati i file o le attività di rete. I gruppi di applicazioni vengono a propria volta suddivisi in gruppi di attendibilità. Tutte le applicazioni e i gruppi di applicazioni ereditano le proprietà dal relativo gruppo padre: regole di controllo dell'applicazione, regole di rete dell'applicazione e priorità di esecuzione.

Analogamente al componente Prevenzione Intrusioni Host, per impostazione predefinita il componente Firewall applica le regole di rete per un gruppo di applicazioni durante il filtro dell'attività di rete di tutte le applicazioni all'interno del gruppo. Le regole di rete dei gruppi di applicazioni definiscono i diritti delle applicazioni all'interno del gruppo per l'accesso a differenti connessioni di rete.

Per impostazione predefinita, Firewall crea un set di regole di rete per ogni gruppo di applicazioni rilevato da Kaspersky Endpoint Security nel computer. È possibile modificare l'azione di Firewall applicata alle regole di rete per i gruppi di applicazioni create per impostazione predefinita. Non è possibile modificare, rimuovere, disabilitare o cambiare la priorità delle regole di rete per i gruppi di applicazioni create per impostazione predefinita.

È inoltre possibile creare una regola di rete per una singola applicazione. Una regola di questo tipo avrà una priorità più alta della regola di rete del gruppo a cui appartiene l'applicazione.

Creazione di una regola di rete dell'applicazione

Per impostazione predefinita, l'attività delle applicazioni è controllata da regole di rete definite per il gruppo di attendibilità a cui Kaspersky Endpoint Security ha assegnato l'applicazione al primo avvio. Se necessario, è possibile creare regole di rete per un intero gruppo di attendibilità, per una singola applicazione o per un gruppo di applicazioni all'interno di un gruppo di attendibilità.

Le regole di rete definite manualmente hanno una priorità più elevata rispetto alle regole di rete determinate per un gruppo di attendibilità. In altre parole, se le regole dell'applicazione definite manualmente differiscono dalle regole dell'applicazione determinate per un gruppo di attendibilità, Firewall controlla l'attività delle applicazioni in base alle regole definite manualmente per le applicazioni.

Per impostazione predefinita, Firewall crea le seguenti regole di rete per ciascuna applicazione:

- Qualsiasi attività di rete in Reti attendibili.
- Qualsiasi attività di rete in Reti locali.
- Qualsiasi attività di rete in Reti pubbliche.

Kaspersky Endpoint Security controlla l'attività di rete delle applicazioni in base a regole di rete predefinite come segue:

- Attendibile e Restrizione bassa: tutta l'attività di rete è consentita.
- Restrizione alta e Non attendibile: tutte le attività di rete sono bloccate.

Le regole predefinite delle applicazioni non possono essere modificate o eliminate.

È possibile creare una regola di rete per le applicazioni nei seguenti modi:

- Utilizzare lo strumento Monitor di rete.

  Monitor di Rete è uno strumento progettato per la visualizzazione in tempo reale di informazioni sulle attività di rete nel computer di un utente. Questo strumento è comodo perché non è necessario configurare tutte le impostazioni delle regole. Alcune impostazioni di Firewall verranno inserite automaticamente dai dati di Monitor di rete. Monitor di rete è disponibile solo nell'interfaccia dell'applicazione.

- Configurare le impostazioni di Firewall.

  Questo consente di ottimizzare le impostazioni di Firewall. È possibile creare regole per qualsiasi attività di rete, anche se al momento non è presente alcuna attività di rete.

Quando si creano regole di rete per le applicazioni, tenere presente che le regole per i pacchetti di rete hanno la priorità sulle regole di rete delle applicazioni.

Come utilizzare lo strumento Monitor di rete per creare una regola di rete per le applicazioni nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **Monitor di rete**.
2. Passare alla scheda **Attività di rete** o **Porte aperte**.

   La scheda **Attività di rete** mostra tutte le connessioni di rete attualmente attive con il computer. Vengono visualizzate le connessioni di rete sia in entrata che in uscita.

   La scheda **Porte aperte** elenca tutte le porte di rete aperte del computer.
3. Nel menu di scelta rapida di una connessione di rete, selezionare **Crea una regola di rete per le applicazioni**.

   Verrà visualizzata la finestra delle regole e delle proprietà dell'applicazione.
4. Selezionare la scheda **Regole di rete**.

   Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.
5. Fare clic su **Aggiungi**.

   Verranno visualizzate le proprietà delle regole di rete.
6. Immettere manualmente il nome del servizio di rete nel campo **Nome**.
7. Configurare le impostazioni delle regole di rete (vedere la tabella seguente).

   È possibile selezionare un modello di regole predefinito facendo clic sul collegamento **Modello regola di rete**. I modelli di regole descrivono le connessioni di rete utilizzate più di frequente.

   Tutte le impostazioni delle regole di rete verranno compilate automaticamente.
8. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.
9. Fare clic su **Salva**.

   La nuova regola di rete verrà aggiunta all'elenco.
10. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.
11. Salvare le modifiche.

Come utilizzare le impostazioni di Firewall per creare una regola di rete per le applicazioni nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Firewall**.

3. Fare clic su **Regole per le applicazioni**.

   Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.

4. Nell'elenco delle applicazioni selezionare l'applicazione o il gruppo di applicazioni per cui si desidera creare una regola di rete.

5. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida, quindi selezionare **Dettagli e regole**.

   Verrà visualizzata la finestra delle regole e delle proprietà dell'applicazione.

6. Selezionare la scheda **Regole di rete**.

7. Fare clic su **Aggiungi**.

   Verranno visualizzate le proprietà delle regole di rete.

8. Immettere manualmente il nome del servizio di rete nel campo **Nome**.

9. Configurare le impostazioni delle regole di rete (vedere la tabella seguente).

   È possibile selezionare un modello di regole predefinito facendo clic sul collegamento **Modello regola di rete**. I modelli di regole descrivono le connessioni di rete utilizzate più di frequente.

   Tutte le impostazioni delle regole di rete verranno compilate automaticamente.

10. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.

11. Fare clic su **Salva**.

    La nuova regola di rete verrà aggiunta all'elenco.

12. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.

13. Salvare le modifiche.

Come creare una regola di rete per le applicazioni in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Firewall**.

4. Nel blocco **Impostazioni di Firewall**, fare clic sul pulsante **Impostazioni**.

   Verrà visualizzato l'elenco delle regole dei pacchetti di rete e l'elenco delle regole di rete dell'applicazione.

5. Passare alla scheda **Regole di rete dell'applicazione**.

6. Fare clic su **Aggiungi**.

7. Nella finestra visualizzata, immettere i criteri per cercare l'applicazione per cui si desidera creare una regola di rete.

   È possibile immettere il nome dell'applicazione o il nome del fornitore. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

8. Fare clic su **Aggiorna**.

   Kaspersky Endpoint Security cercherà l'applicazione nell'elenco consolidato di applicazioni installate nei computer gestiti. Kaspersky Endpoint Security mostrerà un elenco di applicazioni che soddisfano i criteri di ricerca.

9. Selezionare l'applicazione desiderata.

10. Nell'elenco a discesa **Aggiungi l'applicazione selezionata al gruppo di attendibilità**, selezionare **Gruppi predefiniti** e fare clic su **OK**.

    L'applicazione verrà aggiunta al gruppo predefinito.

11. Selezionare l'applicazione opportuna, quindi selezionare **Diritti applicazione** dal menu di scelta rapida dell'applicazione.

    Verrà visualizzata la finestra delle regole e delle proprietà dell'applicazione.

12. Selezionare la scheda **Regole di rete**.

    Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.

13. Fare clic su **Aggiungi**.

    Verranno visualizzate le proprietà delle regole di rete.

14. Immettere manualmente il nome del servizio di rete nel campo **Nome**.

15. Configurare le impostazioni delle regole di rete (vedere la tabella seguente).

    È possibile selezionare un modello di regole predefinito facendo clic sul pulsante . I modelli di regole descrivono le connessioni di rete utilizzate più di frequente.

    Tutte le impostazioni delle regole di rete verranno compilate automaticamente.

16. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.

17. Salvare la nuova regola di rete.

18. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.

19. Salvare le modifiche.

Come creare una regola di rete per le applicazioni in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Selezionare **Comunicazione e protezione Web** → **Firewall**.

5. Nella sezione **Diritti dell'applicazione e risorse protette**, fare clic sul collegamento **Diritti applicazione**.

   Verranno visualizzati la finestra di configurazione dei diritti dell'applicazione e l'elenco delle risorse protette.

6. Passare alla scheda **Diritti applicazione**.

   Verrà visualizzato un elenco di gruppi di attendibilità sul lato sinistro della finestra e le relative proprietà sul lato destro.

7. Nel blocco **Applicazioni**, fare clic sul pulsante **Aggiungi**.

   Verrà avviata la procedura guidata per l'aggiunta di un'applicazione a un gruppo di attendibilità.

8. Selezionare il gruppo di attendibilità pertinente per l'applicazione.

9. Selezionare il tipo **Applicazione**. Procedere con il passaggio successivo.

   Se si desidera creare una regola di rete per più applicazioni, selezionare il tipo **Gruppo** e definire un nome per il gruppo di applicazioni.

10. Nell'elenco delle applicazioni visualizzato selezionare le applicazioni per cui si desidera creare una regola di rete.

    Utilizzare un filtro. È possibile immettere il nome dell'applicazione o il nome del fornitore. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

11. Terminare la procedura guidata.

    L'applicazione verrà aggiunta al gruppo di attendibilità.

12. Nella parte sinistra della finestra selezionare l'applicazione attinente.

13. Nella parte destra della finestra, selezionare **Regole di rete** nell'elenco a discesa.

    Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.

14. Fare clic su **Aggiungi**.

    Verranno visualizzate le proprietà delle regole delle applicazioni.

15. Immettere manualmente il nome del servizio di rete nel campo **Nome regola**.

16. Configurare le impostazioni delle regole di rete (vedere la tabella seguente).

    È possibile selezionare un modello di regole predefinito facendo clic sul collegamento **Seleziona modello di regola**. I modelli di regole descrivono le connessioni di rete utilizzate più di frequente.

    Tutte le impostazioni delle regole di rete verranno compilate automaticamente.

17. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.

18. Salvare la regola di rete.

    La nuova regola di rete verrà aggiunta all'elenco.

19. Utilizzare i pulsanti **Sposta** per impostare la priorità della regola di rete.

20. Salvare le modifiche.

Parametro	Descrizione
Azione	**Consenti**. **Blocca**.
Protocollo	Controlla le attività di rete tramite il protocollo selezionato: TCP, UDP, ICMP, ICMPv6, IGMP e GRE. Se come protocollo è selezionato ICMP o ICMPv6, è possibile definire il codice e il tipo di pacchetto ICMP. Se come tipo di protocollo è selezionato TCP o UDP, è possibile specificare i numeri di porta del computer locale e remoto tra cui monitorare la connessione. Intervallo di valori possibili per i numeri di porta: 0-65535. In ogni campo è possibile immettere più valori separati da `,` oppure specificare un intervallo di valori utilizzando `-`. Ad esempio: • `100,101` • `100-130` • `100,110-130`
Direzione	**In entrata**. **In entrata/In uscita**. **In uscita**.
Indirizzi remoti	Indirizzi di rete dei computer remoti che possono inviare e/o ricevere i pacchetti di rete. Firewall applica la regola di rete all'intervallo specificato di indirizzi di rete remoti. È possibile includere tutti gli indirizzi IP in una regola di rete, creare un elenco separato di indirizzi IP, specificare un intervallo di indirizzi IP o selezionare una subnet (Reti attendibili, Reti locali, Reti pubbliche). È inoltre possibile specificare un nome DNS di un computer anziché il suo indirizzo IP. È necessario utilizzare i nomi DNS solo per computer LAN o servizi interni. L'interazione con i servizi cloud (come Microsoft Azure) e altre risorse Internet deve essere gestita dal componente Controllo Web. Se nella regola per i pacchetti di rete è stato aggiunto un nome DNS per il quale non è stato possibile determinare l'indirizzo IP, Kaspersky Endpoint Security mostrerà un avviso. Nell'elenco delle regole per i pacchetti di rete in Web Console, viene aggiunta una colonna con una descrizione dell'errore. In Administration Console (MMC), la descrizione dell'errore non è disponibile. Tali regole dei pacchetti sono evidenziate con colori.
Indirizzi locali	Indirizzi di rete dei computer che possono inviare e ricevere i pacchetti di rete. Firewall applica una regola di rete all'intervallo specificato di indirizzi di rete locali. È possibile includere tutti gli indirizzi IP in una regola di rete, creare un elenco separato di indirizzi IP o specificare un intervallo di indirizzi IP. L'applicazione memorizza gli indirizzi locali solo se viene specificato un elenco di indirizzi remoti. In altre parole, il valore **Indirizzi dall'elenco** è stato selezionato per **Indirizzi remoti** ed è stato aggiunto almeno un indirizzo. A volte l'indirizzo locale non può essere ottenuto per le applicazioni. In tal caso, questo parametro viene ignorato.

Abilitazione e disabilitazione di una regola di rete per un'applicazione

Per abilitare o disabilitare una regola di rete per un'applicazione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Firewall**.
3. Fare clic su **Regole per le applicazioni**.

   Verrà visualizzato l'elenco delle regole delle applicazioni.
4. Nell'elenco delle applicazioni selezionare l'applicazione o il gruppo di applicazioni per cui si desidera creare o modificare una regola di rete.
5. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida, quindi selezionare **Dettagli e regole**.

   Verrà visualizzata la finestra delle regole e delle proprietà dell'applicazione.
6. Selezionare la scheda **Regole di rete**.

7. Nell'elenco delle regole di rete per un gruppo di applicazioni selezionare la regola di rete desiderata.

   Verrà visualizzata la finestra delle proprietà delle regola di rete.

8. Impostare lo stato **Attivo** o **Inattivo** della regola di rete.

   Non è possibile disabilitare una regola di rete per un gruppo di applicazioni creata da Firewall per impostazione predefinita.

9. Salvare le modifiche.

Modifica dell'azione eseguita da Firewall per una regola di rete per un'applicazione

È possibile modificare l'azione eseguita da Firewall applicata alle regole di rete per un'applicazione o un gruppo di applicazioni create per impostazione predefinita e modificare l'azione eseguita da Firewall per una singola regola di rete personalizzata per un'applicazione o un gruppo di applicazioni.

Per modificare l'azione di Firewall per tutte le regole di rete per un'applicazione o un gruppo di applicazioni:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Firewall**.

3. Fare clic su **Regole per le applicazioni**.

   Verrà visualizzato l'elenco delle regole delle applicazioni.

4. Se si desidera modificare l'azione di Firewall applicata a tutte le regole di rete create per impostazione predefinita, selezionare un'applicazione o un gruppo di applicazioni nell'elenco. Le regole di rete create manualmente restano invariate.

5. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida, selezionare **Regole di rete**, quindi selezionare l'azione che si desidera assegnare:

   - **Eredita**.
   - **Consenti**.
   - **Blocca**.

6. Salvare le modifiche.

Per modificare la risposta di Firewall per una regola di rete per un'applicazione o un gruppo di applicazioni:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Firewall**.

3. Fare clic su **Regole per le applicazioni**.

   Verrà visualizzato l'elenco delle regole delle applicazioni.

4. Nell'elenco selezionare l'applicazione o il gruppo di applicazioni per cui modificare l'azione per una regola di rete.

5. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida, quindi selezionare **Dettagli e regole**.

   Verrà visualizzata la finestra delle regole e delle proprietà dell'applicazione.

6. Selezionare la scheda **Regole di rete**.

7. Selezionare la regola di rete per cui modificare l'azione di Firewall.

8. Nella colonna **Autorizzazione** fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare l'azione da assegnare:

   - **Eredita**.
   - **Consenti**.
   - **Nega**.
   - **Registra eventi**.

9. Salvare le modifiche.

Modifica della priorità di una regola di rete per un'applicazione

La priorità di una regola di rete è determinata dalla relativa posizione nell'elenco delle regole di rete. Firewall elabora le regole nell'ordine in cui compaiono nell'elenco delle regole di rete, dalla prima all'ultima. In base a ciascuna regola di rete elaborata per una particolare connessione di rete, Firewall consente o blocca l'accesso di rete all'indirizzo e alla porta indicati nelle impostazioni della connessione di rete.

Le regole di rete create manualmente hanno una priorità più alta delle regole di rete predefinite.

Non è possibile cambiare la priorità delle regole di rete per i gruppi di applicazioni create per impostazione predefinita.

Per modificare la priorità di una regola di rete:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale → Firewall**.

3. Fare clic su **Regole per le applicazioni**.

   Verrà visualizzato l'elenco delle regole delle applicazioni.

4. Nell'elenco delle applicazioni selezionare l'applicazione o il gruppo di applicazioni per cui si desidera modificare la priorità di una regola di rete.

5. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida, quindi selezionare **Dettagli e regole**.

   Verrà visualizzata la finestra delle regole e delle proprietà dell'applicazione.

6. Selezionare la scheda **Regole di rete**.

7. Selezionare la regola di rete di cui si desidera modificare la priorità.

8. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.

9. Salvare le modifiche.

Monitor di Rete

Monitor di Rete è uno strumento progettato per la visualizzazione in tempo reale di informazioni sulle attività di rete nel computer di un utente.

Per avviare Monitor di Rete:

Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **Monitor di rete**.

Verrà visualizzata la finestra Monitor di Rete. In questa finestra le informazioni sull'attività di rete del computer vengono visualizzate in quattro schede:

- La scheda **Attività di rete** mostra tutte le connessioni di rete attualmente attive con il computer. Vengono visualizzate le connessioni di rete sia in entrata che in uscita. In questa scheda è inoltre possibile creare regole per i pacchetti di rete per il funzionamento del Firewall.
- La scheda **Porte aperte** elenca tutte le porte di rete aperte del computer. In questa scheda è inoltre possibile creare regole per i pacchetti di rete e regole per le applicazioni per il funzionamento di Firewall.
- La scheda **Traffico di rete** mostra il volume del traffico di rete in entrata e in uscita tra il computer dell'utente e altri computer nella rete a cui l'utente è attualmente connesso.
- La scheda **Computer bloccati** elenca gli indirizzi IP dei computer remoti la cui attività di rete è stata bloccata dal componente Protezione minacce di rete dopo il rilevamento di tentativi di attacchi di rete da parte di tali indirizzi IP.

Prevenzione Exploit

Il componente Prevenzione Exploit rileva il codice del programma che sfrutta le vulnerabilità del computer per sfruttare i privilegi di amministratore o eseguire attività dannose. Gli exploit possono ad esempio utilizzare un attacco di overflow del buffer. A tale scopo, l'exploit invia una grande quantità di dati a un'applicazione vulnerabile. Durante l'elaborazione di questi dati, l'applicazione vulnerabile esegue un codice dannoso. In seguito a questo attacco, l'exploit può avviare un'installazione non autorizzata di malware. In caso di tentativo di esecuzione di un file eseguibile da un'applicazione vulnerabile non eseguito dall'utente, Kaspersky Endpoint Security blocca l'esecuzione di questo file o invia una notifica all'utente.

Il componente Prevenzione Exploit consente inoltre di monitorare le porte di rete alla ricerca di processi delle applicazioni che possono minacciare la sicurezza del computer. L'applicazione ottiene informazioni su tali processi con i database anti-virus.

Abilitazione e disabilitazione di Prevenzione Exploit

Per impostazione predefinita, Prevenzione Exploit è abilitato e funziona in modalità ottimale. Kaspersky Endpoint Security monitora i file eseguibili eseguiti dalle applicazioni vulnerabili. Se Kaspersky Endpoint Security rileva che non è stato l'utente a eseguire un file eseguibile di un'applicazione vulnerabile, eseguirà l'azione selezionata, ad esempio bloccando l'operazione.

Come abilitare o disabilitare Prevenzione Exploit in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata** → **Prevenzione Exploit**.
4. Utilizzare la casella di controllo **Prevenzione Exploit** per abilitare o disabilitare il componente.
5. Selezionare l'azione attinente nella sezione **Al rilevamento di exploit**:
   - **Blocca**. Se questo elemento è selezionato, quando viene rilevato un exploit Kaspersky Endpoint Security blocca le operazioni di questo exploit e crea una voce del registro con informazioni sull'exploit.
   - **Informa**. Se questo elemento è selezionato, quando Kaspersky Endpoint Security rileva un exploit registra una voce contenente le informazioni sull'exploit e aggiunge informazioni sull'exploit all'elenco delle minacce attive.
6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare Prevenzione Exploit in Web Console e Cloud Console

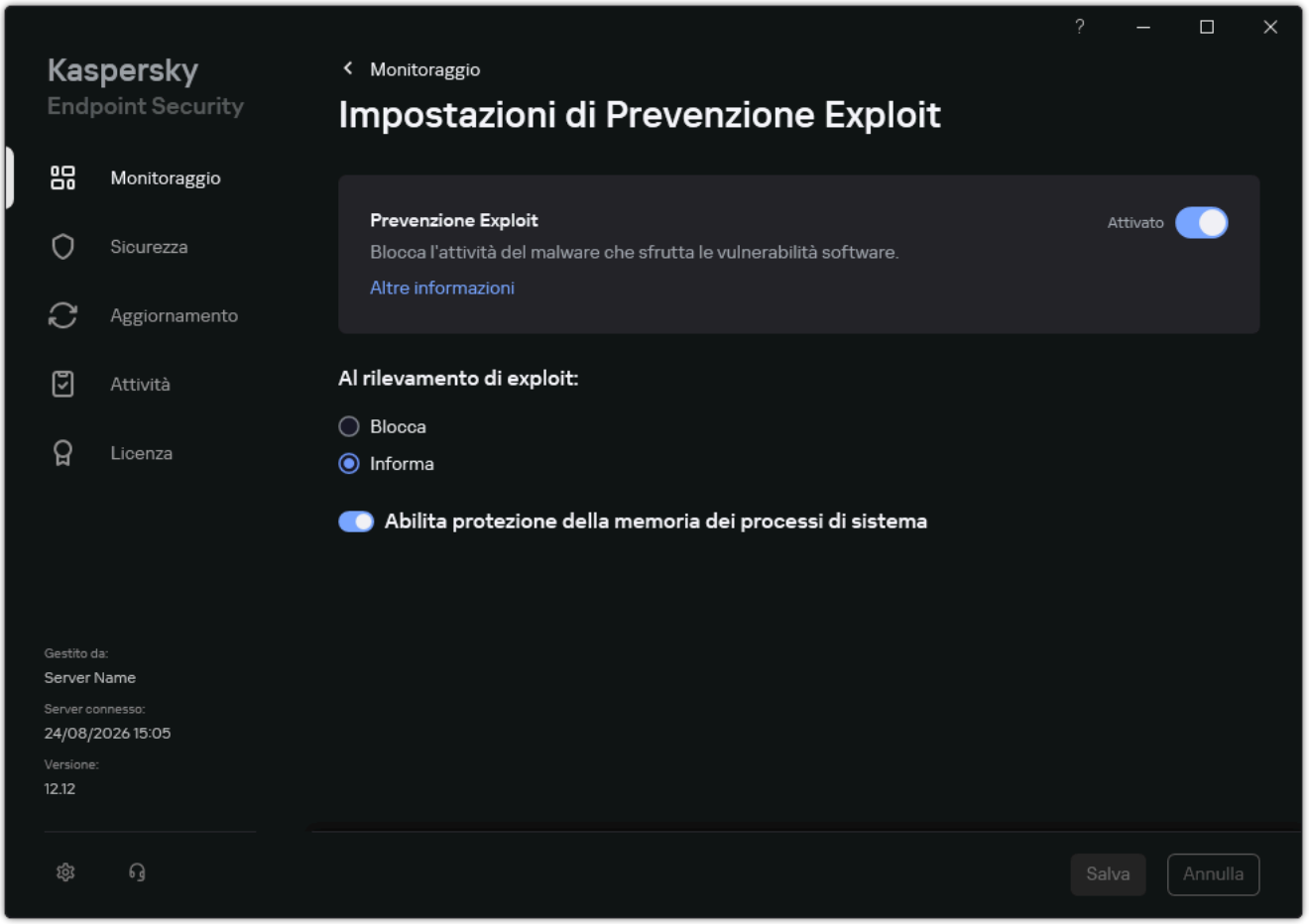
1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Analisi del comportamento** → **Prevenzione Exploit**.
5. Utilizzare l'interruttore **Prevenzione Exploit** per abilitare o disabilitare il componente.
6. Selezionare l'azione attinente nella sezione **Azione se viene rilevata una minaccia**:
   - **Blocca**. Se questo elemento è selezionato, quando viene rilevato un exploit Kaspersky Endpoint Security blocca le operazioni di questo exploit e crea una voce del registro con informazioni sull'exploit.
   - **Informa**. Se questo elemento è selezionato, quando Kaspersky Endpoint Security rileva un exploit registra una voce contenente le informazioni sull'exploit e aggiunge informazioni sull'exploit all'elenco delle minacce attive.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare Prevenzione Exploit nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Prevenzione Exploit**.



Impostazioni di Prevenzione Exploit

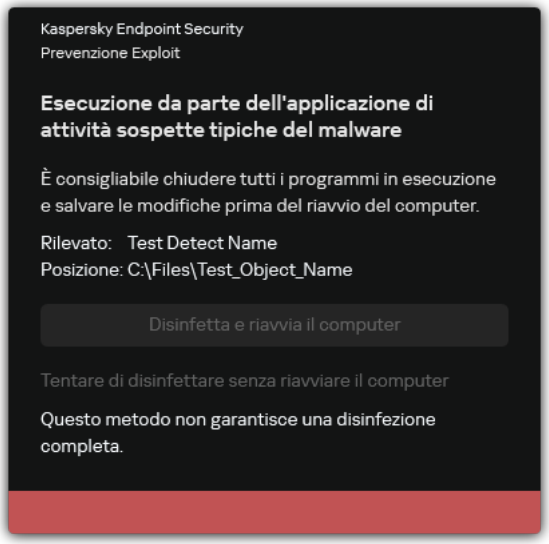
3. Utilizzare l'interruttore **Prevenzione Exploit** per abilitare o disabilitare il componente.

4. Selezionare l'azione attinente nella sezione **Al rilevamento di exploit**:

   - **Blocca**. Se questo elemento è selezionato, quando viene rilevato un exploit Kaspersky Endpoint Security blocca le operazioni di questo exploit e crea una voce del registro con informazioni sull'exploit.

   - **Informa**. Se questo elemento è selezionato, quando Kaspersky Endpoint Security rileva un exploit registra una voce contenente le informazioni sull'exploit e aggiunge informazioni sull'exploit all'elenco delle minacce attive.

5. Salvare le modifiche.



Notifica sulla minaccia attiva

Protezione della memoria dei processi di sistema

Per impostazione predefinita, la protezione della memoria dei processi di sistema è abilitata. Kaspersky Endpoint Security blocca i processi esterni che tentano di ottenere l'accesso ai processi di sistema.

Come abilitare o disabilitare la protezione della memoria dei processi di sistema in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Prevenzione Exploit**.

4. Utilizzare la casella di controllo **Abilita protezione della memoria dei processi di sistema** per abilitare o disabilitare l'opzione.

5. Salvare le modifiche.

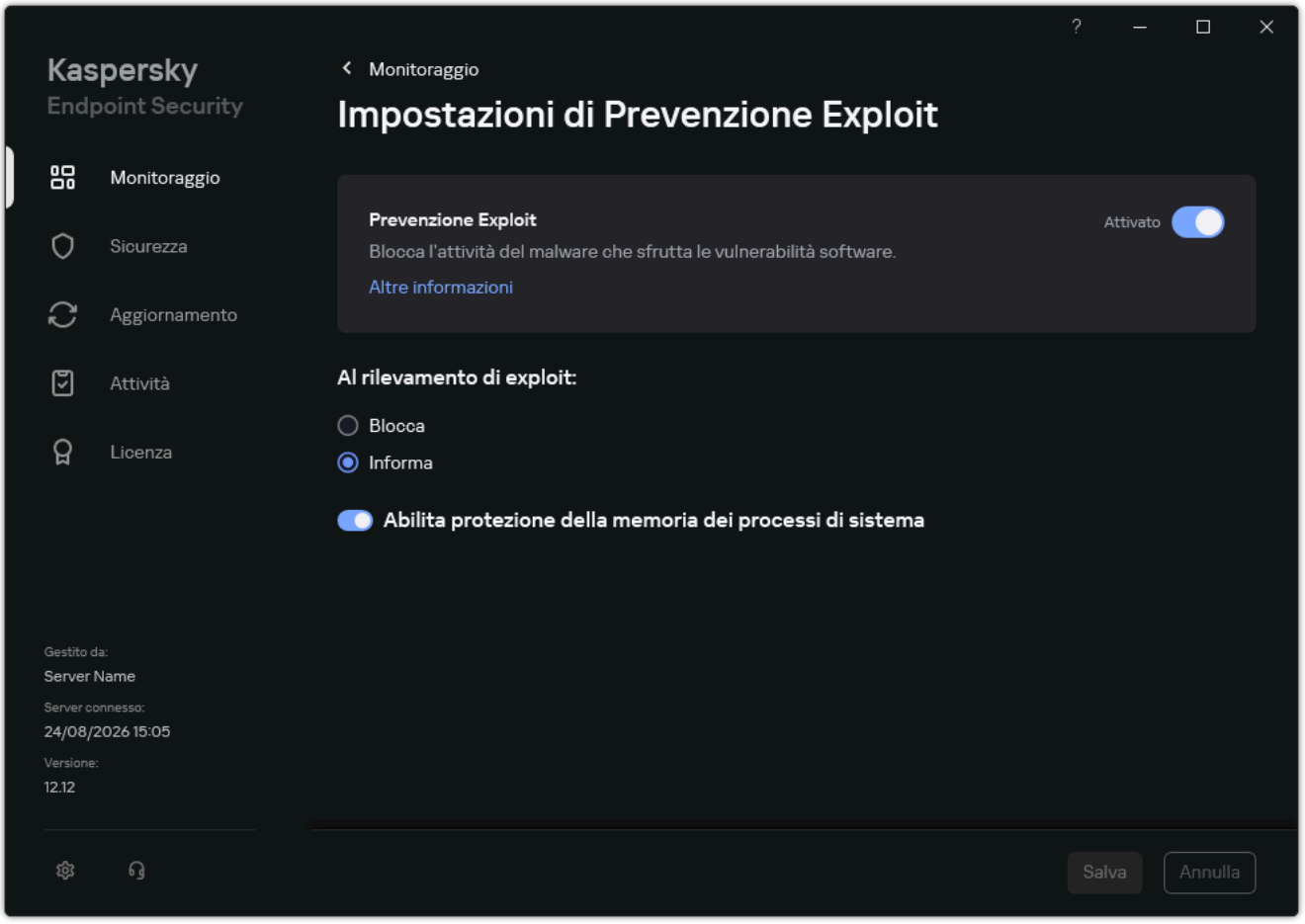
Come abilitare o disabilitare la protezione della memoria dei processi di sistema in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Analisi del comportamento** → **Prevenzione Exploit**.
5. Utilizzare l'interruttore **Protezione della memoria dei processi di sistema ABILITATA** per abilitare o disabilitare questa funzionalità.
6. Salvare le modifiche.

Come abilitare o disabilitare la protezione della memoria dei processi di sistema nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Prevenzione Exploit**.



Impostazioni di Prevenzione Exploit

3. Utilizzare l'interruttore **Abilita protezione della memoria dei processi di sistema** per abilitare o disabilitare questa funzionalità.
4. Salvare le modifiche.

Rilevamento del Comportamento

Il componente Rilevamento del Comportamento riceve dati sulle azioni delle applicazioni nel computer e fornisce tali informazioni ad altri componenti della protezione per migliorarne le prestazioni. Il componente Rilevamento del Comportamento utilizza le firme Behavior Stream Signatures (BSS) per le applicazioni. Se l'attività di un'applicazione corrisponde a uno schema BSS, Kaspersky Endpoint Security esegue l'azione di risposta selezionata. La funzionalità di Kaspersky Endpoint Security basata sugli schemi Behavior Stream Signatures e assicura una difesa proattiva del computer.

Il componente Rilevamento del Comportamento consente inoltre di monitorare le porte di rete alla ricerca di processi delle applicazioni che possono minacciare la sicurezza del computer. L'applicazione ottiene informazioni su tali processi con i database anti-virus.

Rilevamento del Comportamento è abilitato per impostazione predefinita e viene eseguito nella modalità consigliata dagli esperti Kaspersky. Quando vengono rilevate attività dannose, Kaspersky Endpoint Security elimina il file eseguibile dell'applicazione dannosa.

Non è consigliabile disabilitare Rilevamento del Comportamento a meno che non sia assolutamente necessario poiché questa operazione ridurrebbe l'efficacia dei componenti della protezione. I componenti della protezione possono richiedere i dati raccolti dal componente Rilevamento del Comportamento per rilevare le minacce.

Come abilitare o disabilitare Rilevamento del Comportamento in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Rilevamento del Comportamento**.
5. Utilizzare la casella di controllo **Rilevamento del Comportamento** per abilitare o disabilitare il componente.
6. Selezionare l'azione attinente nella sezione **Azione se viene rilevata un'attività malware**:
   - **Elimina**. Se questo elemento è selezionato, al rilevamento di attività dannose Kaspersky Endpoint Security elimina il file eseguibile dell'applicazione dannosa e crea una copia di backup del file in Backup.
   - **Blocca**. Se si seleziona questo elemento, Kaspersky Endpoint Security termina l'applicazione al momento del rilevamento dell'attività dannosa.
   - **Informa**. Se questo elemento è selezionato e vengono rilevate attività malware di un'applicazione, Kaspersky Endpoint Security aggiunge informazioni sulle attività malware dell'applicazione all'elenco delle minacce attive.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare Rilevamento del Comportamento in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

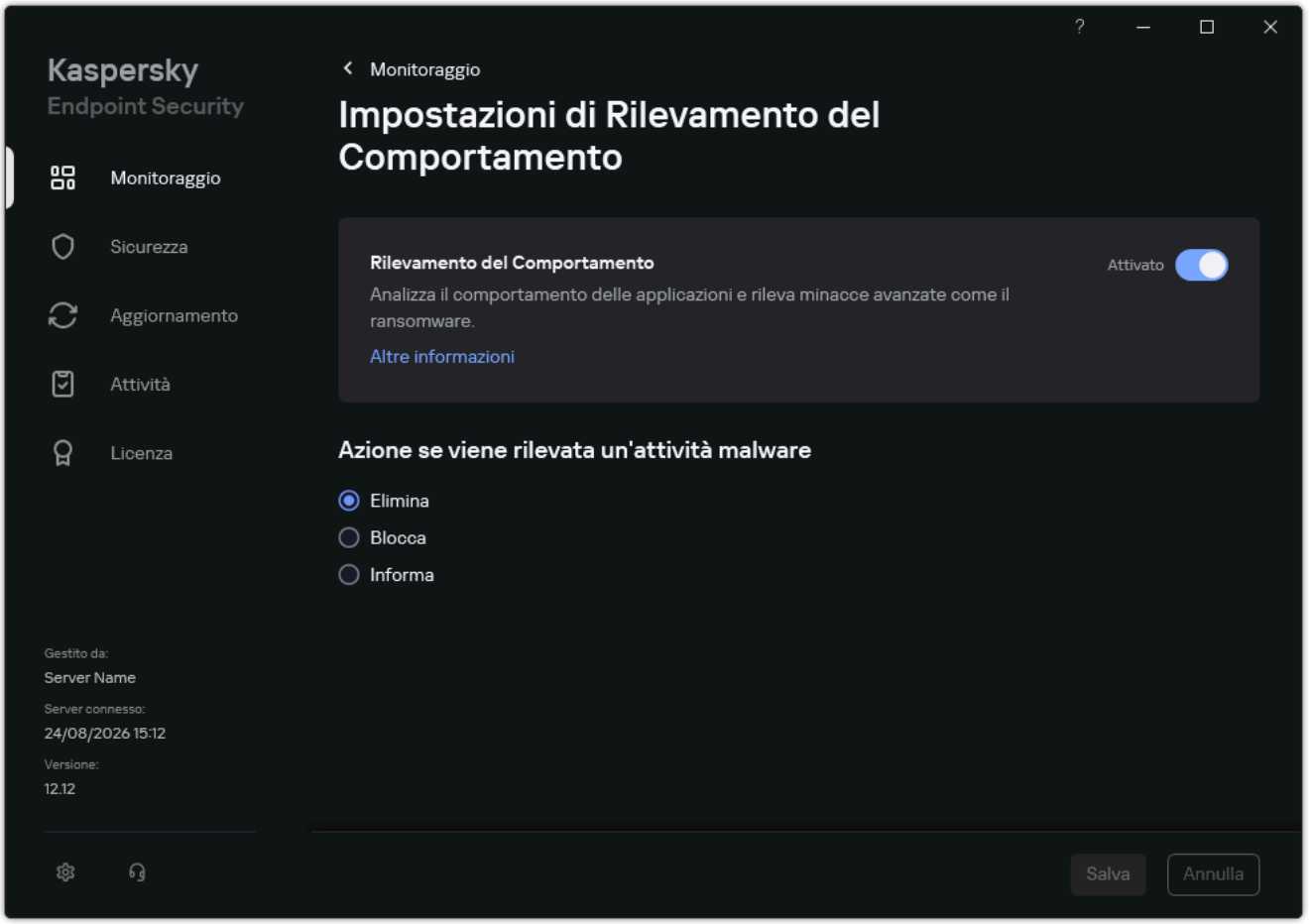
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Analisi del comportamento** → **Rilevamento del Comportamento**
5. Utilizzare l'interruttore **Rilevamento del Comportamento ABILITATO** per abilitare o disabilitare il componente.
6. Selezionare l'azione attinente nella sezione **Azione se viene rilevata una minaccia**:

   - **Elimina**. Se questo elemento è selezionato, al rilevamento di attività dannose Kaspersky Endpoint Security elimina il file eseguibile dell'applicazione dannosa e crea una copia di backup del file in Backup.
   - **Blocca**. Se si seleziona questo elemento, Kaspersky Endpoint Security termina l'applicazione al momento del rilevamento dell'attività dannosa.
   - **Informa**. Se questo elemento è selezionato e vengono rilevate attività malware di un'applicazione, Kaspersky Endpoint Security aggiunge informazioni sulle attività malware dell'applicazione all'elenco delle minacce attive.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare Rilevamento del Comportamento nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Rilevamento del Comportamento**.



Impostazioni di Rilevamento del Comportamento

3. Utilizzare l'interruttore **Rilevamento del Comportamento** per abilitare o disabilitare il componente.

4. Selezionare l'azione attinente nella sezione **Azione se viene rilevata un'attività malware**:

   - **Elimina**. Se questo elemento è selezionato, al rilevamento di attività dannose Kaspersky Endpoint Security elimina il file eseguibile dell'applicazione dannosa e crea una copia di backup del file in Backup.

   - **Blocca**. Se si seleziona questo elemento, Kaspersky Endpoint Security termina l'applicazione al momento del rilevamento dell'attività dannosa.

   - **Informa**. Se questo elemento è selezionato e vengono rilevate attività malware di un'applicazione, Kaspersky Endpoint Security aggiunge informazioni sulle attività malware dell'applicazione all'elenco delle minacce attive.

5. Salvare le modifiche.

Di conseguenza, se Rilevamento del comportamento è abilitato, Kaspersky Endpoint Security utilizzerà le firme BSS per analizzare l'attività delle applicazioni nel sistema operativo.

Anti-Cryptor

A partire da Kaspersky Endpoint Security 12.12 for Windows, la protezione delle cartelle condivise dal criptaggio esterno, precedentemente Rilevamento del Comportamento è un componente separato, Anti-Cryptor.

Il componente monitora le operazioni eseguite solo relativamente ai file che si trovano in dispositivi di archiviazione di massa con file system NTFS e che non sono criptati tramite EFS.

Il componente Anti-Cryptor analizza le attività nelle cartelle condivise. Se questa attività corrisponde a una firma BSS tipica del criptaggio esterno, Kaspersky Endpoint Security esegue l'azione selezionata.

Per il funzionamento del componente Anti-Cryptor, è necessario abilitare il componente Rilevamento del Comportamento.

Se Kaspersky Endpoint Security rileva un tentativo di modifica dei file nelle cartelle condivise, vengono eseguite le seguenti azioni:

- Blocca l'accesso alla modifica del file per la sessione che ha avviato l'attività dannosa (il file sarà di sola lettura).
- Crea copie di backup dei file che vengono modificati.
- Aggiunge una voce ai rapporti dell'interfaccia dell'applicazione locale e invia le informazioni sull'attività dannosa rilevata a Kaspersky Security Center.
- Inoltre, se il componente Motore di Remediation è abilitato, i file modificati vengono ripristinati dalle copie di backup.

Abilitazione e disabilitazione della protezione delle cartelle condivise dal criptaggio esterno

Per impostazione predefinita, la protezione delle cartelle condivise dal criptaggio esterno è abilitata e funziona come consigliato dagli esperti di Kaspersky. Per configurare questa funzionalità, è possibile creare un ambito di protezione e configurare le esclusioni, se necessario. Per impostazione predefinita, l'applicazione identifica automaticamente le cartelle condivise e monitora le attività sui file in tutte le cartelle. Quando viene rilevato un tentativo di criptare esternamente i file nelle cartelle condivise, Kaspersky Endpoint Security blocca la sessione dell'utente remoto per un'ora (per impostazione predefinita).

In seguito all'installazione di Kaspersky Endpoint Security, la protezione delle cartelle condivise dal criptaggio esterno sarà limitata fino al riavvio del computer.

Come abilitare o disabilitare la protezione delle cartelle condivise con il criptaggio esterno in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Anti-Cryptor**.
4. Utilizzare la casella di controllo **Anti-Cryptor** per abilitare o disabilitare il rilevamento delle attività tipiche del criptaggio esterno.
5. Selezionare l'azione pertinente che verrà eseguita dall'applicazione quando viene rilevato un tentativo di modifica dei file nelle cartelle condivise:
   - **Blocca connessione per N min**. Se questa opzione è selezionata, quando Kaspersky Endpoint Security rileva un tentativo di modifica dei file nelle cartelle condivise, blocca l'accesso alla modifica dei file per la sessione che ha avviato l'attività dannosa e crea copie di backup dei file modificati.

     Se il componente Motore di Remediation è abilitato e l'opzione **Blocca connessione per N min** è selezionata, i file modificati vengono ripristinati dalle copie di backup.

   - **Informa**. Se questa opzione è selezionata, al rilevamento di un tentativo di modifica dei file nelle cartelle condivise, Kaspersky Endpoint Security aggiunge le informazioni su questo tentativo di modifica nell'elenco delle minacce attive, aggiunge una voce ai rapporti dell'interfaccia dell'applicazione locale e invia le informazioni sull'attività dannosa rilevata a Kaspersky Security Center.
6. Se necessario, modificare un ambito di protezione e definire le esclusioni.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare la protezione delle cartelle condivise con il criptaggio esterno in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host → Analisi del comportamento → Anti-Cryptor**.
5. Utilizzare il pulsante **Anti-Cryptor ABILITATO** per abilitare o disabilitare il rilevamento delle attività tipiche del criptaggio esterno.

6. Selezionare l'azione pertinente che verrà eseguita dall'applicazione quando viene rilevato un tentativo di modifica dei file nelle cartelle condivise:

   - **Blocca la connessione per (min) N min**. Se questa opzione è selezionata, quando Kaspersky Endpoint Security rileva un tentativo di modifica dei file nelle cartelle condivise, blocca l'accesso alla modifica dei file per la sessione che ha avviato l'attività dannosa e crea copie di backup dei file modificati.

     Se il componente Motore di Remediation è abilitato e l'opzione **Blocca la connessione per (min) N min** è selezionata, i file modificati vengono ripristinati dalle copie di backup.

   - **Informa**. Se questa opzione è selezionata, al rilevamento di un tentativo di modifica dei file nelle cartelle condivise, Kaspersky Endpoint Security aggiunge le informazioni su questo tentativo di modifica nell'elenco delle minacce attive, aggiunge una voce ai rapporti dell'interfaccia dell'applicazione locale e invia le informazioni sull'attività dannosa rilevata a Kaspersky Security Center.

7. Se necessario, modificare un ambito di protezione e definire le esclusioni.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare la protezione delle cartelle condivise con il criptaggio esterno nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Anti-Cryptor**.

3. Utilizzare la casella di controllo **Protezione delle cartelle condivise dal criptaggio esterno** per abilitare o disabilitare il rilevamento delle attività tipiche del criptaggio esterno.

4. Utilizzare la casella di controllo **Protezione delle cartelle condivise dal criptaggio esterno** per abilitare o disabilitare il rilevamento delle attività tipiche del criptaggio esterno.

5. Selezionare l'azione pertinente che verrà eseguita dall'applicazione quando viene rilevato un tentativo di modifica dei file nelle cartelle condivise:

   - **Blocca connessione per (min) N min**. Se questa opzione è selezionata, quando Kaspersky Endpoint Security rileva un tentativo di modifica dei file nelle cartelle condivise, blocca l'accesso alla modifica dei file per la sessione che ha avviato l'attività dannosa e crea copie di backup dei file modificati.

     Se il componente Motore di Remediation è abilitato e l'opzione **Blocca connessione per (min) N min** è selezionata, i file modificati vengono ripristinati dalle copie di backup.

   - **Informa**. Se questa opzione è selezionata, al rilevamento di un tentativo di modifica dei file nelle cartelle condivise, Kaspersky Endpoint Security aggiunge le informazioni su questo tentativo di modifica nell'elenco delle minacce attive, aggiunge una voce ai rapporti dell'interfaccia dell'applicazione locale e invia le informazioni sull'attività dannosa rilevata a Kaspersky Security Center.

6. Se necessario, modificare un ambito di protezione e definire le esclusioni.

7. Salvare le modifiche.

Configurazione del periodo di blocco di un computer non attendibile

Un *computer non attendibile* è un computer remoto impegnato in attività dannose o criptaggio dei dati. Per impostazione predefinita, Kaspersky Endpoint Security blocca la sessione dell'utente remoto per un'ora. Allo scadere del periodo di blocco, Kaspersky Endpoint Security rimuove il computer dall'elenco di blocco e ripristina l'accesso alla cartella condivisa.

Come configurare il periodo di blocco di un computer non attendibile in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Anti-Cryptor**.
4. Nel blocco **Azione se viene rilevata una minaccia**, selezionare **Blocca connessione per N min**.
5. Configurare il periodo di blocco di un computer non attendibile coinvolto in attività dannose o criptaggio dei dati.
6. Salvare le modifiche.

Come configurare il periodo di blocco di un computer non attendibile in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host → Analisi del comportamento → Anti-Cryptor**.
5. In **Azione se viene rilevata una minaccia**, configurare il periodo di blocco di un computer non attendibile coinvolto in attività dannose o criptaggio dei dati.
6. Salvare le modifiche.

Come configurare il periodo di blocco di un computer non attendibile nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Anti-Cryptor**.
3. Nel blocco **Azione se viene rilevata una minaccia**, selezionare **Blocca connessione per (min)**.
4. Configurare il periodo di blocco di un computer non attendibile coinvolto in attività dannose o criptaggio dei dati.
5. Salvare le modifiche.

In seguito a questa operazione, il computer remoto verrà bloccato. Per sbloccare il computer remoto, è possibile riavviare Kaspersky Endpoint Security.

Modifica dell'ambito di protezione

L'*ambito di protezione* è un elenco di percorsi delle cartelle condivise in cui Kaspersky Endpoint Security monitora le attività sui file. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. Per impostazione predefinita, l'applicazione identifica automaticamente le cartelle condivise e monitora le attività sui file in tutte le cartelle.

L'esclusione di una cartella dall'ambito di protezione può ridurre la quantità di falsi positivi se l'organizzazione utilizza il criptaggio dei dati durante lo scambio di file tramite cartelle condivise. Ad esempio, Rilevamento del Comportamento può generare falsi positivi quando l'utente utilizza file con estensione ENC in una cartella condivisa. Tale attività corrisponde a uno schema comportamentale tipico del criptaggio esterno. Se sono presenti file criptati in una cartella condivisa per proteggere i dati, aggiungere tale cartella alle esclusioni.

> È anche possibile escludere i computer da cui non è necessario gestire i tentativi di criptaggio esterni.

Come modificare un ambito di protezione in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Anti-Cryptor**.
4. Nel blocco **Ambito della protezione**, selezionare **Solo cartelle condivise specificate**.
5. Nell'elenco delle cartelle, fare clic su **Aggiungi**.
6. Questo apre una finestra; in tale finestra, immettere il percorso della cartella condivisa che si desidera includere nell'ambito di protezione (ad esempio `C:\Share`).

   > Per aggiungere una cartella condivisa all'ambito di protezione, utilizzare un percorso locale.

7. Fare clic su **OK**.
8. Se necessario, definire le esclusioni dell'ambito di protezione:
   a. Nel blocco **Esclusioni dalla scansione**, fare clic sul pulsante **In base alla maschera**.
   b. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.
   c. Nella finestra visualizzata specificare un'estensione per il file nel formato `*.<file extension>` o il percorso di una cartella. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:

      L'applicazione non supporta alcune estensioni file di esclusione. Pertanto, è possibile specificare un'esclusione come `*.docx` o `**\Folder\**`.

È possibile escludere un oggetto dalle scansioni senza rimuoverlo dall'elenco degli oggetti nell'ambito della protezione. A tale scopo, deselezionare la casella di controllo accanto all'oggetto.

9. Salvare le modifiche.

Come modificare un'ambito di protezione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Analisi del comportamento** → **Anti-Cryptor**.
5. Nel blocco **Ambito della protezione**, selezionare **Solo cartelle condivise specificate**.
6. Nell'elenco delle cartelle, fare clic su **Aggiungi**.
7. Questo apre una finestra; in tale finestra, immettere il percorso della cartella condivisa che si desidera includere nell'ambito di protezione (ad esempio `C:\Share`).

   > Per aggiungere una cartella condivisa all'ambito di protezione, utilizzare un percorso locale.

8. Fare clic su **OK**.
9. Se necessario, definire le esclusioni dell'ambito di protezione:

   a. Nella parte superiore della finestra, fare clic sul collegamento **Esclusioni dalla scansione**.

   b. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.

   c. Nella finestra visualizzata specificare un'estensione per il file nel formato `*.<file extension>` o il percorso di una cartella. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:

      L'applicazione non supporta alcune estensioni file di esclusione. Pertanto, è possibile specificare un'esclusione come `*.docx` o `**\Folder\**`.

   È possibile escludere un oggetto dalle scansioni senza rimuoverlo dall'elenco degli oggetti nell'ambito della protezione. A tale scopo, deselezionare la casella di controllo accanto all'oggetto.

10. Salvare le modifiche.

Come modificare un ambito di protezione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Anti-Cryptor**.
3. Nel blocco **Ambito della protezione**, selezionare **Solo cartelle condivise specificate**.
4. Nell'elenco delle cartelle, fare clic su **Aggiungi**.

5. Questo apre una finestra; in tale finestra, immettere il percorso della cartella condivisa che si desidera includere nell'ambito di protezione (ad esempio `C:\Share`).

   Per aggiungere una cartella condivisa all'ambito di protezione, utilizzare un percorso locale.

6. Fare clic su **OK**.

7. Se necessario, definire le esclusioni dell'ambito di protezione:

   a. Nella parte superiore della finestra, fare clic sul collegamento **Esclusioni in base alla maschera**.

   b. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.

   c. Nella finestra visualizzata specificare un'estensione per il file nel formato `*.<file extension>` o il percorso di una cartella. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:

      L'applicazione non supporta alcune estensioni file di esclusione. Pertanto, è possibile specificare un'esclusione come `*.docx` o `**\Folder\**`.

   È possibile escludere un oggetto dalle scansioni senza rimuoverlo dall'elenco degli oggetti nell'ambito della protezione. A tale scopo, deselezionare la casella di controllo accanto all'oggetto.

8. Salvare le modifiche.

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali → Esclusioni e tipi di oggetti rilevati**.

3. Nella sezione **Esclusioni**, fare clic sul collegamento **Gestisci esclusioni**.

4. Fare clic su **Aggiungi**.

5. Fare clic su **Sfoglia** e selezionare la cartella condivisa.

   È inoltre possibile immettere il percorso manualmente. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:

   - Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

   - Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

   - Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

È possibile utilizzare le maschere all'inizio, al centro o alla fine del percorso file. Ad esempio, se si desidera aggiungere una cartella per tutti gli utenti alle esclusioni, immettere la maschera `?:\Users\*\Folder\`.

6. Nel blocco **Componenti della protezione**, selezionare il componente **Rilevamento del Comportamento**.

7. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.

8. Selezionare lo stato **Attivo** per l'esclusione.

   È possibile utilizzare l'interruttore per interrompere un'esclusione in qualsiasi momento.

9. Salvare le modifiche.

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare alla sezione **Area attendibile**.

5. Nella finestra visualizzata, fare clic sul collegamento **Esclusioni dalla scansione malware**.

6. Selezionare la casella di controllo **Unisci i valori quando vengono ereditati** se si desidera creare un elenco consolidato di esclusioni per tutti i computer dell'azienda. Gli elenchi delle esclusioni nei criteri padre e figlio verranno uniti. Gli elenchi verranno uniti a condizione che l'unione dei valori durante l'ereditarietà sia abilitata. Le esclusioni dal criterio padre vengono visualizzate nei criteri figlio in una visualizzazione di sola lettura. Non è possibile modificare o eliminare le esclusioni del criterio padre.

7. Selezionare la casella di controllo **Consenti l'utilizzo delle esclusioni locali** se si desidera consentire all'utente di creare un elenco locale di esclusioni. In questo modo un utente può creare il proprio elenco locale di esclusioni oltre all'elenco generale di esclusioni generato nel criterio. Un amministratore può utilizzare Kaspersky Security Center per visualizzare, aggiungere, modificare o eliminare gli elementi dell'elenco nelle proprietà del computer.

   Se la casella di controllo è deselezionata, l'utente può accedere solo all'elenco generale delle esclusioni generato nel criterio. Inoltre, se questa casella di controllo è deselezionata, Kaspersky Endpoint Security nasconde l'elenco consolidato delle esclusioni dalle scansioni nell'interfaccia utente dell'applicazione.

8. Fare clic su **Aggiungi** e selezionare un'azione:

   - **Categoria**. È possibile raggruppare le esclusioni dalle scansioni in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'esclusione dalle scansioni alla categoria.

   - **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova esclusione dalle scansioni alla radice dell'elenco.

   - **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include le *esclusioni dalla scansione predefinite*. Sono state inoltre aggiunte esclusioni dalla scansione predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le esclusioni dalle scansioni predefinite a seconda dello scopo del server protetto.

9. Selezionare le modalità di aggiunta dell'esclusione **Percorso del file o della cartella**.

10. Immettere il percorso della cartella condivisa.

È inoltre possibile immettere il percorso manualmente. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:

- Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

- Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

- Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

È possibile utilizzare le maschere all'inizio, al centro o alla fine del percorso file. Ad esempio, se si desidera aggiungere una cartella per tutti gli utenti alle esclusioni, immettere la maschera `C:\Users\*\Folder\`.

11. Nel blocco **Applica esclusione a**, selezionare il componente **Rilevamento del Comportamento**.

12. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.

13. Selezionare lo stato **Aggiungi alle esclusioni** per l'esclusione.

    È possibile utilizzare l'interruttore per interrompere un'esclusione in qualsiasi momento.

14. Salvare le modifiche.

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.

4. Nel blocco **Esclusioni dalla scansione e applicazioni attendibili** → **Esclusioni dalla scansione**, fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata una finestra contenente un elenco di esclusioni.

5. Selezionare la casella di controllo **Unisci i valori quando vengono ereditati** se si desidera creare un elenco consolidato di esclusioni per tutti i computer dell'azienda. Gli elenchi delle esclusioni nei criteri padre e figlio verranno uniti. Gli elenchi verranno uniti a condizione che l'unione dei valori durante l'ereditarietà sia abilitata. Le esclusioni dal criterio padre vengono visualizzate nei criteri figlio in una visualizzazione di sola lettura. Non è possibile modificare o eliminare le esclusioni del criterio padre.

6. Selezionare la casella di controllo **Consenti l'utilizzo delle esclusioni locali** se si desidera consentire all'utente di creare un elenco locale di esclusioni. In questo modo un utente può creare il proprio elenco locale di esclusioni oltre all'elenco generale di esclusioni generato nel criterio. Un amministratore può utilizzare Kaspersky Security Center per visualizzare, aggiungere, modificare o eliminare gli elementi dell'elenco nelle proprietà del computer.

   Se la casella di controllo è deselezionata, l'utente può accedere solo all'elenco generale delle esclusioni generato nel criterio. Inoltre, se questa casella di controllo è deselezionata, Kaspersky Endpoint Security nasconde l'elenco consolidato delle esclusioni dalle scansioni nell'interfaccia utente dell'applicazione.

7. Fare clic su **Aggiungi** e selezionare un'azione:

   - **Categoria**. È possibile raggruppare le esclusioni dalle scansioni in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'esclusione dalle scansioni alla categoria.

   - **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova esclusione dalle scansioni alla radice dell'elenco.

   - **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include le *esclusioni dalla scansione predefinite*. Sono state inoltre aggiunte esclusioni dalla scansione predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le esclusioni dalle scansioni predefinite a seconda dello scopo del server protetto.

8. Fare clic su **Aggiungi**.

9. Nella sezione **Proprietà** selezionare la casella di controllo **File o cartella**.

10. Fare clic sul collegamento **Selezionare un file o una cartella** nel blocco **Descrizione dell'esclusione dalla scansione (fare clic sui termini sottolineati per modificarli)** per aprire la finestra **Nome del file o della cartella**.

11. Fare clic su **Sfoglia** e selezionare la cartella condivisa.

    È inoltre possibile immettere il percorso manualmente. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:

    - Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

    - Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

    - Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

    È possibile utilizzare le maschere all'inizio, al centro o alla fine del percorso file. Ad esempio, se si desidera aggiungere una cartella per tutti gli utenti alle esclusioni, immettere la maschera `?:\Users\*\Folder\`.

12. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.

13. Fare clic sul collegamento nel blocco **Descrizione dell'esclusione dalla scansione (fare clic sui termini sottolineati per modificarli)** per aprire la finestra **Componenti della protezione**.

14. Selezionare la casella di controllo accanto al componente **Rilevamento del Comportamento**.

15. Salvare le modifiche.

Aggiunta di computer attendibili per il criptaggio dei dati esterni

Se l'organizzazione utilizza il criptaggio dei dati esterni nel flusso di lavoro di scambio dei file, è necessario creare un elenco di computer attendibili. Kaspersky Endpoint Security non monitora il criptaggio dei dati da parte dei computer attendibili.

Il servizio Controlla Accesso deve essere abilitato per abilitare le esclusioni degli indirizzi dalla protezione delle cartelle condivise dal criptaggio esterno. Per impostazione predefinita, il servizio Controlla Accesso è disabilitato (per informazioni dettagliate sull'abilitazione del servizio Controlla Accesso, visitare il sito Web Microsoft).

La funzionalità per l'esclusione degli indirizzi dalla protezione delle cartelle condivise non funziona in un computer remoto se questo è stato acceso prima dell'avvio di Kaspersky Endpoint Security. È possibile riavviare il computer remoto dopo l'avvio di Kaspersky Endpoint Security per fare in modo che la funzionalità per l'esclusione degli indirizzi dalla protezione delle cartelle condivise funzioni in questo computer remoto.

Come aggiungere un computer attendibile per il criptaggio dei dati esterni in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Protezione minacce avanzata** → **Anti-Cryptor**.
5. Nel blocco **Esclusioni dalla scansione**, fare clic sul pulsante **In base al nome o all'indirizzo IP**.
6. Nella finestra visualizzata, fare clic sul pulsante **In base al nome o all'indirizzo IP**.
7. Immettere gli indirizzi IP, l'intervallo di indirizzi IP o i nomi dei computer da cui non devono essere gestiti gli attacchi di criptaggio esterno.

   Esempi:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come aggiungere un computer attendibile per il criptaggio esterno dei dati in Kaspersky Security Center Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare alla sezione **Area attendibile**.
5. Nella parte destra della finestra, fare clic sul collegamento **Esclusioni di Anti-Cryptor**.
6. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.
7. Immettere gli indirizzi IP, l'intervallo di indirizzi IP o i nomi dei computer da cui non devono essere gestiti gli attacchi di criptaggio esterno.

   Esempi:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come aggiungere un computer attendibile per il criptaggio dei dati esterni nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Anti-Cryptor**.
3. Nella parte superiore della finestra, fare clic sul collegamento **Esclusioni in base al nome o all'indirizzo IP**.
4. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.
5. Immettere gli indirizzi IP, l'intervallo di indirizzi IP o i nomi dei computer da cui non devono essere gestiti gli attacchi di criptaggio esterno.

   Esempi:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`

- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

6. Salvare le modifiche.

Esportazione e importazione di un elenco di esclusioni dalla protezione delle cartelle condivise dal criptaggio esterno

È possibile esportare l'elenco delle esclusioni in un file XML. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di indirizzi dello stesso tipo. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco delle esclusioni o per eseguire la migrazione dell'elenco in un server diverso.

Come esportare e importare un elenco di esclusioni in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata** → **Anti-Cryptor**.
4. Nel blocco **Esclusioni dalla scansione**, fare clic sul pulsante **In base al nome o all'indirizzo IP**.
5. Per esportare l'elenco delle regole:
   a. Selezionare le esclusioni che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.
      Se non è stata selezionata alcuna esclusione, Kaspersky Endpoint Security esporterà tutte le esclusioni.
   b. Fare clic sul pulsante → **Esporta**.
   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle esclusioni e selezionare la cartella in cui si desidera salvare il file.
   d. Salvare il file.
      Kaspersky Endpoint Security esporta l'intero elenco di esclusioni nel file XML.
6. Per importare l'elenco delle esclusioni:
   a. Fare clic sul pulsante → **Importa**.
   b. Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle esclusioni.
   c. Aprire il file.
      Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.
7. Salvare le modifiche.

Come esportare e importare un elenco di esclusioni in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Analisi del comportamento** → **Anti-Cryptor**.
5. Fare clic sul collegamento **Esclusioni in base al nome o all'indirizzo IP**.
6. Per esportare l'elenco delle regole:
   a. Selezionare le esclusioni che si desidera esportare.
   b. Fare clic sul pulsante → **Esporta**.

      Kaspersky Endpoint Security esporta l'elenco delle esclusioni in un file JSON nella cartella dei download predefinita.
7. Per importare l'elenco delle esclusioni:
   a. Fare clic sul pulsante → **Importa**.

      Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco delle esclusioni.
   b. Aprire il file.

      Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.
8. Salvare le modifiche.

Motore di Remediation

Il componente Motore di Remediation consente a Kaspersky Endpoint Security di eseguire il rollback delle azioni eseguite dal malware nel sistema operativo.

Durante il rollback dell'attività del malware nel sistema operativo, Kaspersky Endpoint Security gestisce i seguenti tipi di attività del malware:

- **Attività sui file**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Elimina i file eseguibili creati dal malware (in tutti i supporti eccetto le unità di rete).
  - Elimina i file eseguibili creati da programmi in cui si è verificata un'infiltrazione di malware.
  - Ripristina i file modificati o eliminati dal malware.

  La funzionalità di ripristino dei file prevede diverse limitazioni.

- **Attività sul registro di sistema**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Elimina le chiavi del registro di sistema create dal malware.
  - Non ripristina le chiavi del registro di sistema modificate o eliminate dal malware.

- **Attività sul sistema**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Termina i processi avviati dal malware.
  - Termina i processi in cui è penetrata un'applicazione dannosa.
  - Non riprende i processi che sono stati arrestati dal malware.

- **Attività di rete**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Blocca l'attività di rete del malware.
  - Blocca l'attività di rete dei processi in cui si è verificata un'infiltrazione di malware.

Il rollback delle azioni del malware può essere avviato dal componente Protezione minacce file o Rilevamento del Comportamento o nel corso di una scansione malware.

La procedura di rollback delle operazioni del malware influisce su un set di dati ben definito. Il rollback non ha alcun effetto indesiderato sul sistema operativo o sull'integrità dei dati del computer.

Come abilitare o disabilitare il componente Motore di Remediation in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Motore di Remediation**.
4. Utilizzare la casella di controllo **Motore di Remediation** per abilitare o disabilitare il componente.
5. Salvare le modifiche.

Come abilitare o disabilitare il componente Motore di Remediation in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host → Analisi del comportamento → Motore di Remediation**.
5. Utilizzare l'interruttore **Motore di Remediation ABILITATO** per abilitare o disabilitare il componente.
6. Salvare le modifiche.

Come abilitare o disabilitare il componente Motore di Remediation nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Motore di Remediation**.
3. Utilizzare l'interruttore **Motore di Remediation** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Di conseguenza, se Motore di Remediation è abilitato, Kaspersky Endpoint Security eseguirà il rollback delle azioni eseguite dalle applicazioni dannose nel sistema operativo.

Kaspersky Security Network



Per proteggere il computer in modo più efficace, Kaspersky Endpoint Security utilizza dati ricevuti dagli utenti di tutto il mondo. L'acquisizione di questi dati viene eseguita tramite Kaspersky Security Network.

La funzionalità KSN potrebbe non essere disponibile nell'applicazione negli Stati Uniti.

Kaspersky Security Network (KSN) è un'infrastruttura di servizi cloud che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce risposte più rapide da parte di Kaspersky Endpoint Security alle nuove minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi positivi. Se si partecipa a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla reputazione degli indirizzi Web scansionati, nonché informazioni sulla categoria e sulla reputazione dei file scansionati. Per ulteriori dettagli sulla configurazione dell'accesso a KSN, consultare la Guida di Kaspersky Security Center.

L'utilizzo di Kaspersky Security Network è facoltativo. L'applicazione richiede di utilizzare KSN durante la configurazione iniziale dell'applicazione. Gli utenti possono aderire al servizio o interrompere la partecipazione a KSN in qualsiasi momento.

Per informazioni più dettagliate sull'invio a Kaspersky delle informazioni statistiche generate durante la partecipazione a KSN, nonché sull'archiviazione e l'eliminazione di tali informazioni, fare riferimento all'Informativa di Kaspersky Security Network e al sito Web di Kaspersky. Il file ksn_<ID lingua>.txt con il testo dell'Informativa di Kaspersky Security Network è incluso nel kit di distribuzione dell'applicazione.

L'infrastruttura dei database di reputazione di Kaspersky

Kaspersky Endpoint Security supporta le seguenti soluzioni di infrastruttura per l'utilizzo dei database di reputazione di Kaspersky:

- *Kaspersky Security Network (KSN)* è la soluzione utilizzata dalla maggior parte delle applicazioni Kaspersky. I partecipanti KSN ricevono le informazioni da Kaspersky e inviano a Kaspersky le informazioni sugli oggetti rilevati nel computer dell'utente per un'analisi aggiuntiva da parte degli analisti di Kaspersky e per essere incluse nei database statistici e della reputazione.

- *Kaspersky Private Security Network (KPSN)* è una soluzione che consente agli utenti di computer che ospitano Kaspersky Endpoint Security o altre applicazioni Kaspersky di ottenere l'accesso ai database di reputazione di Kaspersky e ad altri dati statistici senza inviare dati a Kaspersky dai propri computer. KPSN è progettato per i clienti aziendali che non sono in grado di partecipare a Kaspersky Security Network per uno dei seguenti motivi:

  - Le workstation locali non sono connesse a Internet.

  - La trasmissione dei dati al di fuori del paese o al di fuori della LAN aziendale è vietato dalla legge o sottoposto a restrizioni in base ai criteri di protezione aziendali.

Abilitazione e disabilitazione dell'utilizzo di Kaspersky Security Network

Per impostazione predefinita, Kaspersky Endpoint Security utilizza l'impostazione Modalità KSN estesa. *Modalità KSN estesa* è una modalità in cui Kaspersky Endpoint Security invia dati aggiuntivi a Kaspersky.

Come abilitare o disabilitare Uso KSN in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Kaspersky Security Network**.

4. Utilizzare l'interruttore **Kaspersky Security Network** per abilitare o disabilitare il componente.

   Se è stato abilitato l'uso di KSN, Kaspersky Endpoint Security visualizzerà l'Informativa di Kaspersky Security Network. Leggere e accettare le condizioni per l'utilizzo dell'Informativa su Kaspersky Security Network (KSN), se si concorda con queste.

5. Se necessario, deselezionare la casella di controllo **Abilita modalità KSN estesa**. Per impostazione predefinita, la modalità KSN estesa è abilitata.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare Uso KSN in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali → Kaspersky Security Network**.
5. Utilizzare l'interruttore **Utilizzo di Kaspersky Security Network (KSN) ABILITATO** per abilitare o disabilitare il componente.

   Se è stato abilitato l'uso di KSN, Kaspersky Endpoint Security visualizzerà l'Informativa di Kaspersky Security Network. Leggere e accettare le condizioni per l'utilizzo dell'Informativa su Kaspersky Security Network (KSN), se si concorda con queste.
6. Se necessario, disattivare l'interruttore **Usa modalità KSN estesa**. Per impostazione predefinita, la modalità KSN estesa è abilitata.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare Uso KSN nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Kaspersky Security Network**.
3. Utilizzare l'interruttore **Kaspersky Security Network** per abilitare o disabilitare il componente.

   Se è stato abilitato l'uso di KSN, Kaspersky Endpoint Security visualizzerà l'Informativa di Kaspersky Security Network. Leggere e accettare le condizioni per l'utilizzo dell'Informativa su Kaspersky Security Network (KSN), se si concorda con queste.
4. Se necessario, disattivare l'interruttore **Abilita modalità KSN estesa**. Per impostazione predefinita, la modalità KSN estesa è abilitata.
5. Salvare le modifiche.

Di conseguenza, se l'uso di KSN è abilitato, Kaspersky Endpoint Security utilizza le informazioni sulla reputazione di file, risorse Web e applicazioni ricevute da Kaspersky Security Network.

Limitazioni di Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) è una soluzione che consente agli utenti di computer che ospitano Kaspersky Endpoint Security o altre applicazioni Kaspersky di ottenere l'accesso ai database di reputazione di Kaspersky e ad altri dati statistici senza inviare dati a Kaspersky dai propri computer. Kaspersky Private Security Network consente di utilizzare il proprio database di reputazione locale per verificare la reputazione degli oggetti (file o indirizzi Web). La reputazione di un oggetto aggiunto al database di reputazione locale ha una priorità maggiore di quella aggiunta a KSN/KPSN. Immaginare ad esempio che Kaspersky Endpoint Security esegua la scansione di un computer e richieda la reputazione di un file in KSN/KPSN. Se il file ha una reputazione *Non attendibili* nel database di reputazione locale ma ha una reputazione *Attendibili* in KSN/KPSN, Kaspersky Endpoint Security rileverà il file come *Non attendibili* e intraprenderà l'azione definita per le minacce rilevate.

Tuttavia, in alcuni casi Kaspersky Endpoint Security potrebbe non richiedere la reputazione di un oggetto in KSN/KPSN. In tal caso, Kaspersky Endpoint Security non riceverà i dati dal database di reputazione locale di KPSN. Kaspersky Endpoint Security potrebbe non richiedere la reputazione di un oggetto in KSN/KPSN per i seguenti motivi:

- Le applicazioni Kaspersky utilizzano database di reputazione offline. I database di reputazione offline sono progettati per ottimizzare le risorse durante il funzionamento delle applicazioni Kaspersky e per proteggere gli oggetti di importanza critica nel computer. I database di reputazione offline vengono creati dagli esperti Kaspersky sulla base dei dati di Kaspersky Security Network. Le applicazioni Kaspersky aggiornano i database della reputazione offline con i database anti-virus dell'applicazione specifica. Se i database di reputazione offline contengono informazioni su un oggetto sottoposto a scansione, l'applicazione non richiede la reputazione di questo oggetto a KSN/KPSN.

- Le esclusioni dalla scansione (area attendibile) vengono configurate nelle impostazioni dell'applicazione. In questo caso, l'applicazione non tiene conto della reputazione dell'oggetto nel database della reputazione locale.

- L'applicazione utilizza tecnologie di ottimizzazione della scansione, come iSwift o iChecker, oppure memorizza nella cache le richieste di reputazione in KSN/KPSN. In tal caso, l'applicazione potrebbe non richiedere la reputazione di oggetti precedentemente esaminati.

- Per ottimizzare il carico di lavoro, l'applicazione esegue la scansione di file di un determinato formato e dimensione. L'elenco dei formati rilevanti e dei limiti di dimensione sono determinati dagli esperti di Kaspersky. Questo elenco viene aggiornato con i database anti-virus dell'applicazione. È inoltre possibile configurare le impostazioni di ottimizzazione della scansione nell'interfaccia dell'applicazione, ad esempio per il componente Protezione minacce file.

- Kaspersky Endpoint Security in modalità Light Agent comunica con i server KSN tramite un server proxy KSN. La comunicazione diretta con KSN non è supportata.

Abilitazione e disabilitazione della modalità cloud per i componenti della protezione

La *Modalità cloud* fa riferimento alla modalità operativa dell'applicazione in cui Kaspersky Endpoint Security utilizza una versione leggera dei database anti-virus. Kaspersky Security Network supporta il funzionamento dell'applicazione con l'utilizzato dei database anti-virus leggeri. La versione leggera dei database anti-virus consente di utilizzare circa la metà della RAM del computer che altrimenti verrebbe utilizzata con i database standard. Se non si partecipa a Kaspersky Security Network o se la modalità cloud è disabilitata, Kaspersky Endpoint Security scarica la versione completa dei database anti-virus dai server di Kaspersky.

Quando si utilizza Kaspersky Private Security Network, la funzionalità modalità cloud è disponibile a partire da Kaspersky Private Security Network versione 3.0.

Se l'applicazione funziona in modalità Light Agent, la modalità Cloud non è disponibile.

Come abilitare o disabilitare la modalità cloud per i componenti della protezione in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Kaspersky Security Network**.
4. Utilizzare la casella di controllo **Abilita modalità cloud** per abilitare o disabilitare il componente.
5. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare la modalità cloud per i componenti della protezione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali → Kaspersky Security Network**.
5. Utilizzare l'interruttore **Usa modalità cloud** per abilitare o disabilitare il componente.
6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare o disabilitare la modalità cloud per i componenti della protezione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata → Kaspersky Security Network**.
3. Utilizzare l'interruttore **Abilita modalità cloud** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Di conseguenza, Kaspersky Endpoint Security scarica una versione parziale o una versione completa dei database anti-virus durante il successivo aggiornamento.

Se la versione light dei database anti-virus non è disponibile per l'utilizzo, Kaspersky Endpoint Security passa automaticamente alla versione premium dei database anti-virus.

Impostazioni proxy KSN

I computer degli utenti gestiti tramite Kaspersky Security Center Administration Server possono interagire direttamente con KSN o tramite il servizio KSN Proxy.

Se l'applicazione è in esecuzione in modalità Light Agent, la comunicazione diretta con KSN non è supportata. Kaspersky Endpoint Security comunica con i server KSN tramite un server proxy KSN.

Il servizio KSN Proxy fornisce le seguenti funzionalità:

- Il computer dell'utente può eseguire query in KSN e inviare informazioni a KSN, anche senza accesso diretto a Internet.
- Il servizio KSN Proxy memorizza nella cache i dati elaborati, riducendo il carico sul canale di comunicazione di rete esterna e velocizzando la ricezione delle informazioni richieste dal computer dell'utente.

Per impostazione predefinita, dopo l'abilitazione di KSN e l'accettazione dell'Informativa KSN, l'applicazione utilizza un server proxy per connettersi a Kaspersky Security Network. Il server proxy utilizzato dall'applicazione è Kaspersky Security Center Administration Server tramite la porta TCP 13111. Pertanto, se il proxy KSN non è disponibile, è necessario verificare quanto segue:

- Il servizio `ksnproxy` è in esecuzione in Administration Server.
- Il firewall sul computer non blocca la porta 13111.

È possibile configurare l'uso del KSN Proxy come segue: abilitare o disabilitare il KSN Proxy e configurare la porta per la connessione. A tale scopo, è necessario aprire le proprietà di Administration Server. Per ulteriori dettagli sulla configurazione di KSN Proxy, consultare la Guida di Kaspersky Security Center. È inoltre possibile abilitare o disabilitare il KSN Proxy per i singoli computer nel criterio di Kaspersky Endpoint Security.

Come abilitare o disabilitare il proxy KSN in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Protezione minacce avanzata → Kaspersky Security Network**.
4. Nel blocco **Impostazioni proxy KSN**, utilizzare la casella di controllo **Usa Administration Server come server proxy KSN** per abilitare o disabilitare il proxy KSN.
5. Se necessario, selezionare la casella di controllo **Usa i server di Kaspersky Security Network se il server proxy KSN non è disponibile**.

   Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza i server KSN quando il servizio KSN Proxy non è disponibile. I server KSN possono essere gestiti sia da Kaspersky che da terzi (quando si utilizza Kaspersky Private Security Network).
6. Salvare le modifiche.

Come abilitare o disabilitare il proxy KSN in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali → Kaspersky Security Network**.
5. Utilizzare la casella di controllo **Usa Administration Server come server proxy KSN** per abilitare o disabilitare KSN Proxy.

6. Se necessario, selezionare la casella di controllo **Usa i server di Kaspersky Security Network se il server proxy KSN non è disponibile**.

   Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza i server KSN quando il servizio KSN Proxy non è disponibile. I server KSN possono essere gestiti sia da Kaspersky che da terzi (quando si utilizza Kaspersky Private Security Network). Per impostazione predefinita, la casella di controllo è deselezionata.

7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

L'indirizzo del KSN Proxy corrisponde all'indirizzo di Administration Server. Quando il nome di dominio di Administration Server viene modificato, è necessario aggiornare manualmente l'indirizzo del KSN Proxy.

Per configurare l'indirizzo del proxy KSN:

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare la cartella **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.
3. Nel menu di scelta rapida della cartella **Pacchetti di installazione**, selezionare **Proprietà**.
4. Nella scheda **Generali** nella finestra aperta, specificare il nuovo indirizzo del server proxy KSN.
5. Salvare le modifiche.

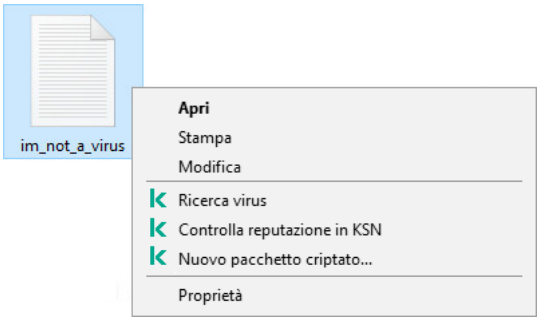
Controllo della reputazione di un file in Kaspersky Security Network

In caso di dubbi sulla sicurezza di un file, è possibile verificarne la reputazione in Kaspersky Security Network.

È possibile verificare la reputazione di un file se sono stati accettati i termini dell'Informativa di Kaspersky Security Network.

Per controllare la reputazione di un file in Kaspersky Security Network:

Aprire il menu di scelta rapida del file e selezionare l'opzione **Controlla reputazione in KSN** (vedere la figura seguente).



Menu di scelta rapida del file

Kaspersky Endpoint Security visualizza la reputazione del file:

Attendibile (Kaspersky Security Network). L'applicazione considera attendibile un file se vengono soddisfatte una o più delle seguenti condizioni:

- il file è firmato digitalmente da un fornitore attendibile;
- il file ha una reputazione attendibile in Kaspersky Security Network;
- il file è stato inserito dall'utente nel gruppo Attendibile.

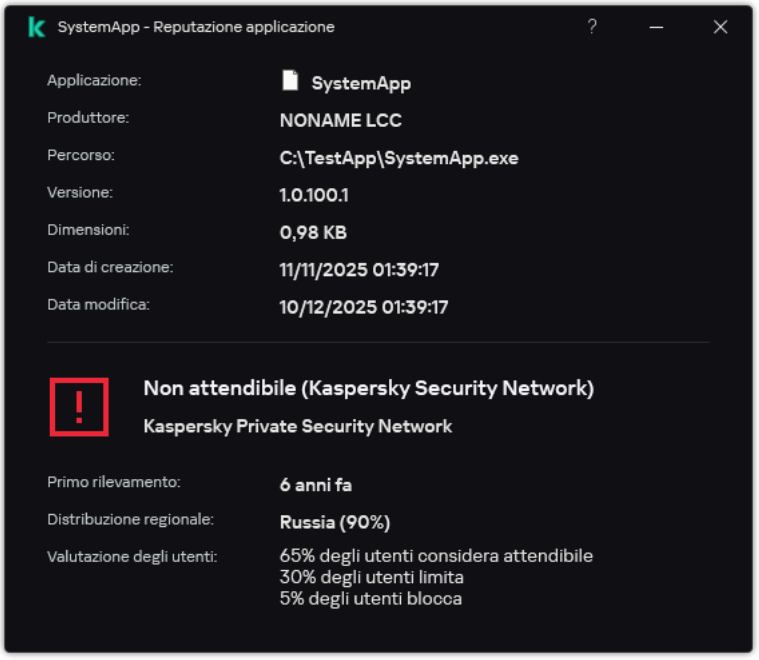
Software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali. Benché non presentino funzioni pericolose, le applicazioni di questo tipo possono essere sfruttate dagli utenti malintenzionati. Per ulteriori dettagli sul software legittimo utilizzabile da utenti malintenzionati per danneggiare il computer o i dati personali di un utente, consultare il sito Web dell'Enciclopedia IT di Kaspersky. È possibile aggiungere queste applicazioni all'elenco delle applicazioni attendibili.

Non attendibile (Kaspersky Security Network). Un virus o un'altra applicazione che rappresenta una minaccia.

Sconosciuto (Kaspersky Security Network). Kaspersky Security Network non dispone di informazioni sul file. È possibile eseguire la scansione di un file utilizzando i database anti-virus (l'opzione **Ricerca virus** nel menu di scelta rapida).

Kaspersky Endpoint Security mostra la soluzione KSN utilizzata per determinare la reputazione del file: *Kaspersky Security Network* o *Kaspersky Private Security Network*.

Kaspersky Endpoint Security visualizza anche ulteriori informazioni sul file (vedere la figura seguente).



Reputazione di un file in Kaspersky Security Network

Scansione delle connessioni criptate

Dopo l'installazione, Kaspersky Endpoint Security aggiunge un certificato Kaspersky all'archivio di sistema per i certificati attendibili (archivio certificati Windows). Kaspersky Endpoint Security utilizza questo certificato per esaminare le connessioni criptate. Kaspersky Endpoint Security include anche l'utilizzo dell'archivio di sistema dei certificati attendibili in Firefox e Thunderbird per esaminare il traffico di queste applicazioni.

I componenti Controllo Web, Protezione minacce di posta, Protezione minacce Web, Rilevamento del Comportamento e Prevenzione Exploit possono decriptare ed esaminare il traffico di rete trasmesso tramite connessioni criptate utilizzando i seguenti protocolli:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Abilitazione della scansione delle connessioni criptate

Per impostazione predefinita, Kaspersky Endpoint Security non sempre esegue la scansione delle connessioni criptate, ma solo quando richiesto dai componenti della protezione.

Come abilitare la scansione delle connessioni criptate in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni di rete**.
5. Nel blocco **Scansione delle connessioni criptate**, selezionare la modalità di scansione delle connessioni criptate:
   - **Esegui scansione delle connessioni criptate**. Kaspersky Endpoint Security non avrà accesso ai contenuti dei siti Web i cui indirizzi iniziano con `https://`.
   - **Esamina le connessioni criptate su richiesta da parte dei componenti della protezione**. Kaspersky Endpoint Security esaminerà il traffico criptato solo quando richiesto dai componenti Protezione minacce Web, Protezione minacce di posta e Controllo Web.
   - **Esamina sempre le connessioni criptate**. Kaspersky Endpoint Security esaminerà il traffico di rete criptato anche se i componenti della protezione sono disabilitati.

Kaspersky Endpoint Security non esegue la scansione delle connessioni criptate stabilite da applicazioni attendibili per le quali la scansione del traffico è disabilitata. Kaspersky Endpoint Security non esegue la scansione delle connessioni criptate dall'elenco predefinito di siti Web attendibili. L'elenco predefinito di siti Web attendibili viene creato dagli esperti di Kaspersky. Questo elenco viene aggiornato con i database anti-virus dell'applicazione. È possibile visualizzare l'elenco predefinito di siti Web attendibili esclusivamente nell'interfaccia di Kaspersky Endpoint Security. Non è possibile visualizzare l'elenco in Kaspersky Security Center Console.

6. Se necessario, aggiungere esclusioni dalla scansione: indirizzi e applicazioni attendibili.
7. Configurare le impostazioni per la scansione delle connessioni criptate (vedere la tabella seguente).
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare la scansione delle connessioni criptate in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di rete**.
5. In **Scansione delle connessioni criptate**, attivare l'interruttore **Scansione delle connessioni criptate ABILITATA**.

   Se l'interruttore è disattivato, Kaspersky Endpoint Security non avrà accesso ai contenuti dei siti Web i cui indirizzi iniziano con `https://`.
6. Fare clic su **Impostazioni** e selezionare la modalità di scansione delle connessioni criptate:

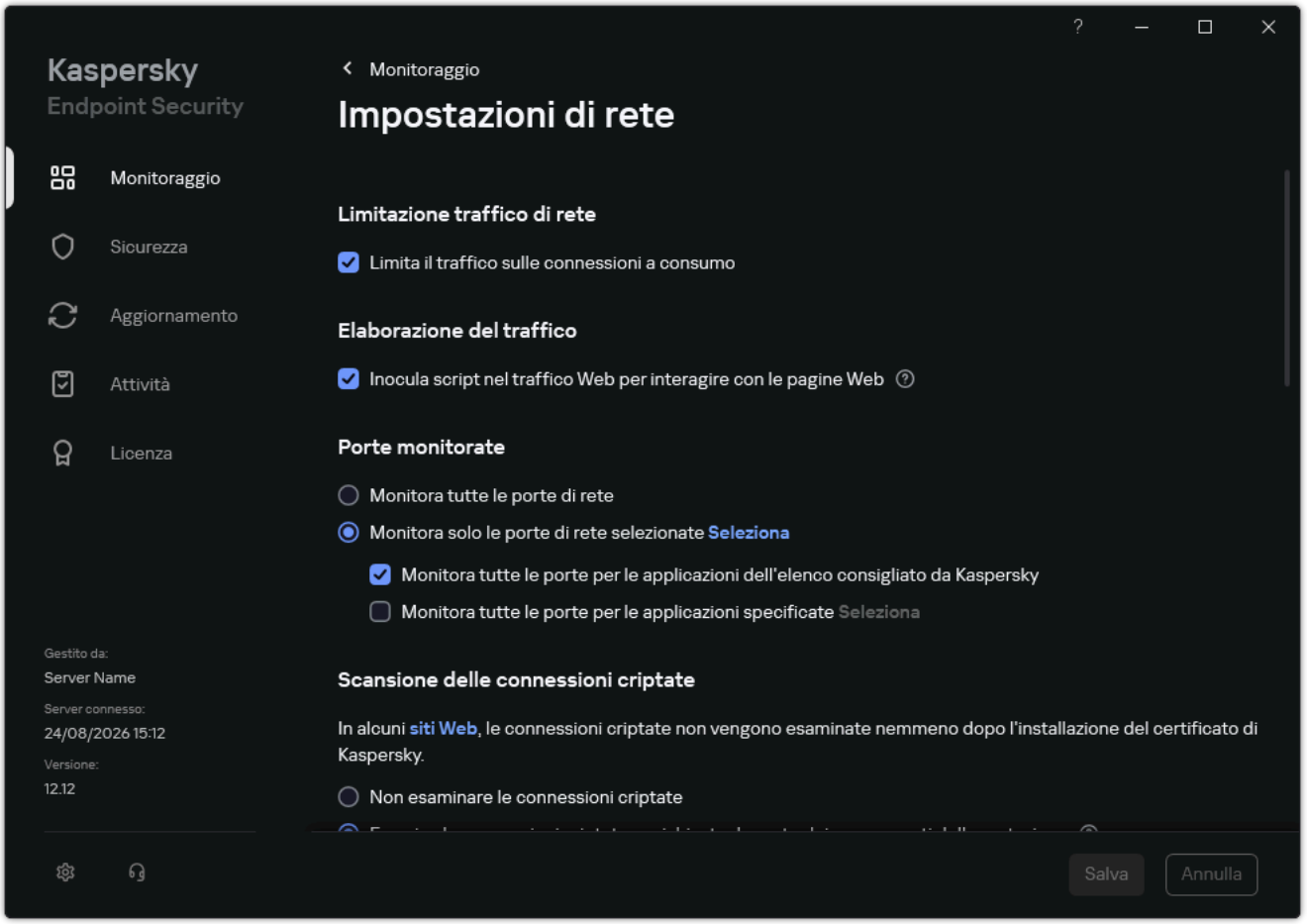
   - **Esamina le connessioni criptate su richiesta da parte dei componenti della protezione**. Kaspersky Endpoint Security esaminerà il traffico criptato solo quando richiesto dai componenti Protezione minacce Web, Protezione minacce di posta e Controllo Web.
   - **Esamina sempre le connessioni criptate**. Kaspersky Endpoint Security esaminerà il traffico di rete criptato anche se i componenti della protezione sono disabilitati.

Kaspersky Endpoint Security non esegue la scansione delle connessioni criptate stabilite da applicazioni attendibili per le quali la scansione del traffico è disabilitata. Kaspersky Endpoint Security non esegue la scansione delle connessioni criptate dall'elenco predefinito di siti Web attendibili. L'elenco predefinito di siti Web attendibili viene creato dagli esperti di Kaspersky. Questo elenco viene aggiornato con i database anti-virus dell'applicazione. È possibile visualizzare l'elenco predefinito di siti Web attendibili esclusivamente nell'interfaccia di Kaspersky Endpoint Security. Non è possibile visualizzare l'elenco in Kaspersky Security Center Console.

7. Se necessario, aggiungere esclusioni dalla scansione: indirizzi e applicazioni attendibili.
8. Configurare le impostazioni per la scansione delle connessioni criptate (vedere la tabella seguente).
9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare la scansione delle connessioni criptate nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.



Impostazioni di scansione delle connessioni criptate

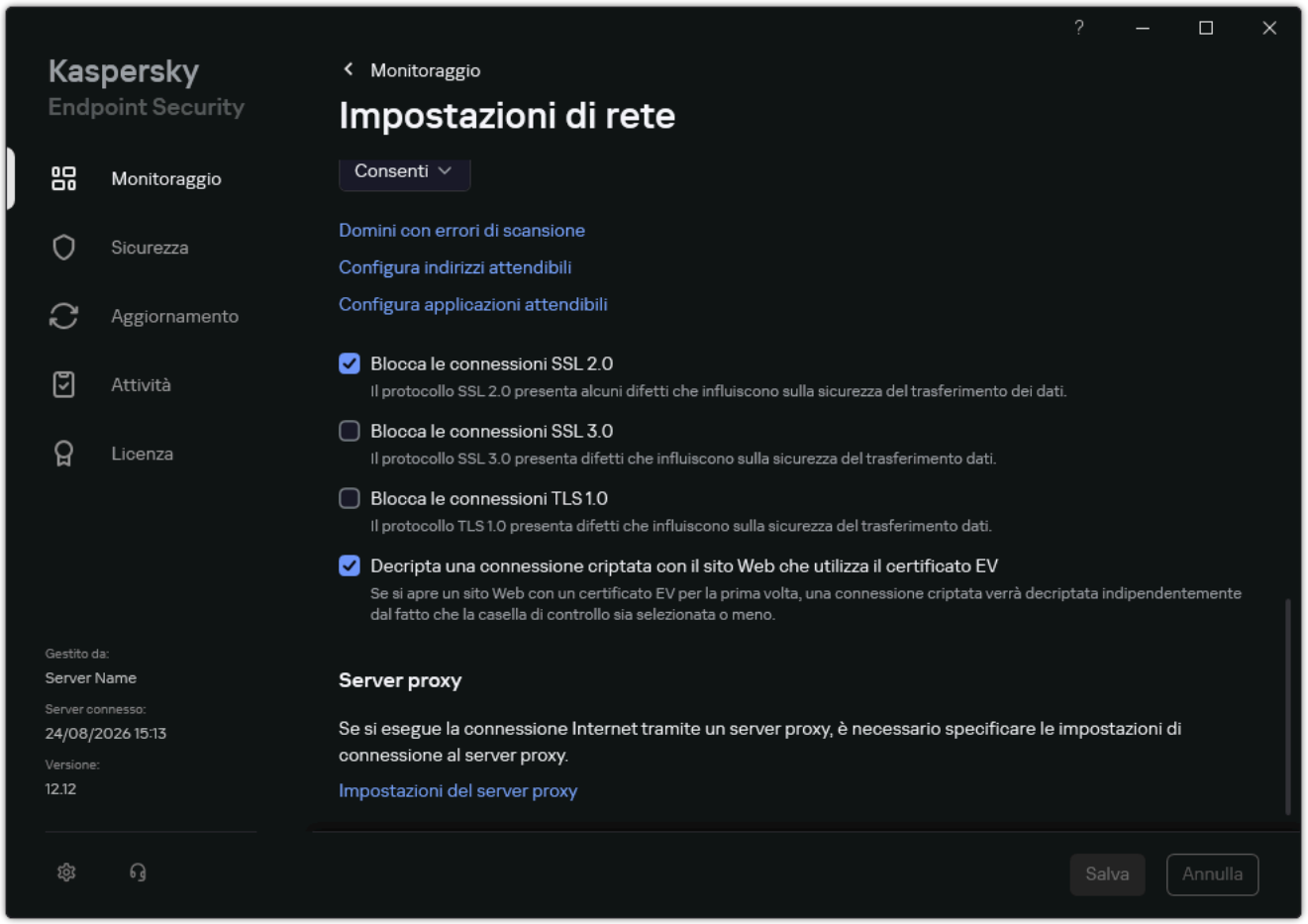
3. Nel blocco **Scansione delle connessioni criptate**, selezionare la modalità di scansione delle connessioni criptate:

   - **Non esaminare le connessioni criptate**. Kaspersky Endpoint Security non avrà accesso ai contenuti dei siti Web i cui indirizzi iniziano con `https://`.
   - **Esamina le connessioni criptate su richiesta da parte dei componenti della protezione**. Kaspersky Endpoint Security esaminerà il traffico criptato solo quando richiesto dai componenti Protezione minacce Web, Protezione minacce di posta e Controllo Web.
   - **Esamina sempre le connessioni criptate**. Kaspersky Endpoint Security esaminerà il traffico di rete criptato anche se i componenti della protezione sono disabilitati.

   Kaspersky Endpoint Security non esegue la scansione delle connessioni criptate stabilite da applicazioni attendibili per le quali la scansione del traffico è disabilitata. Kaspersky Endpoint Security non esegue la scansione delle connessioni criptate dall'elenco predefinito di siti Web attendibili. L'elenco predefinito di siti Web attendibili viene creato dagli esperti di Kaspersky. Questo elenco viene aggiornato con i database anti-virus dell'applicazione. È possibile visualizzare l'elenco predefinito di siti Web attendibili esclusivamente nell'interfaccia di Kaspersky Endpoint Security. Non è possibile visualizzare l'elenco in Kaspersky Security Center Console.

4. Se necessario, aggiungere esclusioni dalla scansione: indirizzi e applicazioni attendibili.

5. Configurare le impostazioni per la scansione delle connessioni criptate (vedere la tabella seguente).



Impostazioni aggiuntive per la scansione delle connessioni criptate

6. Salvare le modifiche.

Impostazioni di scansione delle connessioni criptate

Parametro	Descrizione
Certificati radice attendibili	Elenco dei certificati radice attendibili. Kaspersky Endpoint Security consente di installare i certificati radice attendibili nei computer degli utenti se, ad esempio, è necessario distribuire un nuovo centro di certificazione. L'applicazione consente di aggiungere un certificato a uno speciale archivio certificati di Kaspersky Endpoint Security. In questo caso, il certificato viene considerato attendibile solo per l'applicazione Kaspersky Endpoint Security. In altre parole, l'utente può accedere a un sito Web con il nuovo certificato nel browser. Se un'altra applicazione tenta di accedere al sito Web, è possibile che si verifichi un errore di connessione a causa di un problema di certificato. Per aggiungere all'archivio certificati di sistema, è possibile utilizzare i criteri di gruppo di Active Directory.
Visita di un dominio con un certificato non attendibile	• **Consenti**. Quando si visita un dominio con un certificato non attendibile, Kaspersky Endpoint Security consente la connessione di rete. Quando si apre un dominio con un certificato non attendibile in un browser, Kaspersky Endpoint Security visualizza una pagina HTML con un avviso e il motivo per cui è consigliabile non visitare il dominio. Un utente può fare clic sul collegamento dalla pagina HTML di avviso per ottenere l'accesso alla risorsa Web richiesta. Se un'applicazione o un servizio di terzi stabilisce una connessione con un dominio dotato di un certificato non attendibile, Kaspersky Endpoint Security crea il proprio certificato per esaminare il traffico. Il nuovo certificato presenta lo stato *Non attendibili*. Ciò è necessario per avvisare l'applicazione di terzi della connessione non attendibile perché in questo caso la pagina HTML non può essere visualizzata e la connessione può essere stabilita in background. • **Blocca**. Quando si visita un dominio con un certificato non attendibile, Kaspersky Endpoint Security blocca la connessione di rete. Quando si apre un dominio con un certificato non attendibile in un browser, Kaspersky Endpoint Security visualizza una pagina HTML con il motivo per cui il dominio è bloccato.
Visita di un dominio con un errore di scansione delle connessioni criptate	• **Blocca**. Se si verifica un errore di scansione delle connessioni criptate, Kaspersky Endpoint Security blocca la connessione di rete. • **Consenti e aggiungi dominio alle esclusioni**. Se si verifica un errore di scansione delle connessioni criptate, Kaspersky Endpoint Security aggiunge il dominio che ha generato l'errore all'elenco dei domini con errori di scansione e non monitora il traffico di rete criptato quando viene visitato questo dominio. È possibile visualizzare un elenco dei domini con errori di scansione delle connessioni criptate solo nell'interfaccia locale dell'applicazione. Per cancellare i contenuti dell'elenco è necessario selezionare **Blocca**. Kaspersky Endpoint Security genera anche un evento per l'errore di scansione della connessione criptata.

Parametro	Descrizione
Blocca le connessioni SSL 2.0	Se la casella di controllo è selezionata, l'applicazione monitora e blocca le connessioni di rete stabilite tramite il protocollo SSL 2.0. Se la casella di controllo è deselezionata, l'applicazione non blocca le connessioni di rete stabilite tramite il protocollo SSL 2.0. L'applicazione tuttavia non monitora il traffico di rete su questo protocollo.
Blocca le connessioni SSL 3.0	Se la casella di controllo è selezionata, l'applicazione blocca le connessioni di rete stabilite tramite il protocollo SSL 3.0. Se la casella di controllo è deselezionata, l'applicazione non blocca le connessioni di rete stabilite tramite il protocollo SSL 3.0. L'applicazione monitora il traffico di rete tramite questo protocollo. Tutti i componenti dell'applicazione funzionano senza restrizioni.
Blocca le connessioni TLS 1.0	Se la casella di controllo è selezionata, l'applicazione blocca le connessioni di rete stabilite tramite il protocollo TLS 1.0. Se la casella di controllo è deselezionata, l'applicazione non blocca le connessioni di rete stabilite tramite il protocollo TLS 1.0. L'applicazione monitora il traffico di rete tramite questo protocollo. Tutti i componenti dell'applicazione funzionano senza restrizioni.
Decripta una connessione criptata con il sito Web che utilizza il certificato EV	I certificati EV (Extended Validation Certificate) confermano l'autenticità dei siti Web e ottimizzano la sicurezza della connessione. I browser utilizzano un'icona a forma di lucchetto nella barra degli indirizzi per indicare che un sito Web dispone di un certificato EV. I browser possono inoltre colorare in modo parziale o completo la barra degli indirizzi di verde. Se la casella di controllo è selezionata, l'applicazione decripta e monitora le connessioni criptate con siti Web che utilizzano un certificato EV. Se la casella di controllo è deselezionata, l'applicazione non ha accesso ai contenuti del traffico HTTPS. Per questo motivo l'applicazione monitora il traffico HTTPS solo in base all'indirizzo del sito Web, ad esempio `https://bing.com`. Se si apre un sito Web con un certificato EV per la prima volta, la connessione criptata verrà decriptata indipendentemente dal fatto che la casella di controllo sia selezionata o meno.

Installazione di certificati radice attendibili

Kaspersky Endpoint Security consente di installare i certificati radice attendibili nei computer degli utenti se, ad esempio, è necessario distribuire un nuovo centro di certificazione. L'applicazione consente di aggiungere un certificato a uno speciale archivio certificati di Kaspersky Endpoint Security. In questo caso, il certificato viene considerato attendibile solo per l'applicazione Kaspersky Endpoint Security. In altre parole, l'utente può accedere a un sito Web con il nuovo certificato nel browser. Se un'altra applicazione tenta di accedere al sito Web, è possibile che si verifichi un errore di connessione a causa di un problema di certificato. Per aggiungere all'archivio certificati di sistema, è possibile utilizzare i criteri di gruppo di Active Directory.

Come installare i certificati radice attendibili in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni di rete**.
4. Nel blocco **Certificati radice attendibili**, fare clic sul pulsante **Aggiungi**.
5. Viene visualizzata una finestra, che consente di selezionare un certificato radice attendibile.

   Kaspersky Endpoint Security supporta certificati con estensioni PEM, DER e CRT.
6. Salvare le modifiche.

Come installare i certificati radice attendibili in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di rete**.
5. Fare clic sul collegamento **Certificati radice attendibili**.
6. Viene visualizzata una finestra; in tale finestra, fare clic su **Aggiungi** e selezionare un certificato radice attendibile.

   Kaspersky Endpoint Security supporta certificati con estensioni PEM, DER e CRT.
7. Salvare le modifiche.

Come installare i certificati radice attendibili nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.
3. Nel blocco **Scansione delle connessioni criptate**, fare clic sul pulsante **Mostra certificati**.
4. Viene visualizzata una finestra; in tale finestra, fare clic su **Aggiungi** e selezionare un certificato radice attendibile.

   Kaspersky Endpoint Security supporta certificati con estensioni PEM, DER e CRT.
5. Salvare le modifiche.

Di conseguenza, durante la scansione del traffico, oltre all'archivio certificati di sistema, Kaspersky Endpoint Security utilizza il proprio archivio certificati.

Scansione delle connessioni criptate con un certificato non attendibile

Dopo l'installazione, Kaspersky Endpoint Security aggiunge un certificato Kaspersky all'archivio di sistema per i certificati attendibili (archivio certificati Windows). Kaspersky Endpoint Security utilizza questo certificato per esaminare le connessioni criptate. Quando si visita un dominio con un certificato non attendibile, è possibile consentire o negare l'accesso dell'utente a tale dominio (consultare le istruzioni riportate di seguito).

Se all'utente è stato consentito di visitare domini con certificati non attendibili, Kaspersky Endpoint Security esegue le seguenti azioni:

- Quando si visita un dominio con un certificato non attendibile nel *browser*, Kaspersky Endpoint Security utilizza il certificato Kaspersky per eseguire la scansione del traffico. Kaspersky Endpoint Security mostra una pagina HTML con un avviso e informazioni sul motivo per cui non è consigliabile visitare il dominio pertinente (vedere la figura seguente). Un utente può fare clic sul collegamento dalla pagina HTML di avviso per ottenere l'accesso alla risorsa Web richiesta. Dopo aver fatto clic su questo collegamento, durante la successiva ora Kaspersky Endpoint Security non visualizzerà avvisi su un certificato non attendibile quando si visitano altre risorse nello stesso dominio. Kaspersky Endpoint Security genera anche un evento relativo alla creazione di una connessione criptata con un certificato non attendibile.

  In alcuni casi, Kaspersky Endpoint Security non può tecnicamente mostrare una pagina HTML con un avviso nel browser (vedere la figura di seguito). Se ad esempio una risorsa Web utilizza una versione obsoleta di un protocollo di rete e una porta non standard. In questi casi, Kaspersky Endpoint Security blocca l'accesso al dominio e il browser mostrerà la finestra `ERR_CONNECTION_RESET` standard. Per accedere a una risorsa Web, è possibile aggiungere il dominio alle esclusioni o utilizzare un certificato attendibile.

- Se *un'applicazione o un servizio di terzi* stabilisce una connessione con un dominio dotato di un certificato non attendibile, Kaspersky Endpoint Security crea il proprio certificato per esaminare il traffico. Il nuovo certificato presenta lo stato *Non attendibile*. Ciò è necessario per avvisare l'applicazione di terzi della connessione non attendibile perché in questo caso la pagina HTML non può essere visualizzata e la connessione può essere stabilita in background. Pertanto, se un'applicazione di terzi dispone di strumenti di verifica dei certificati integrati, la connessione potrebbe essere interrotta. In tal caso, è necessario contattare il proprietario del dominio e configurare una connessione attendibile. Se non è possibile configurare una connessione attendibile, è possibile aggiungere tale applicazione di terzi all'elenco delle applicazioni attendibili. Kaspersky Endpoint Security genera anche un evento relativo alla creazione di una connessione criptata con un certificato non attendibile.

Come configurare la scansione delle connessioni criptate con un certificato non attendibile in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni di rete**.
4. Nel blocco **Scansione delle connessioni criptate**, fare clic sul pulsante **Impostazioni avanzate**.
5. Nella finestra visualizzata, selezionare la modalità operativa dell'applicazione quando si visita un dominio con un certificato non attendibile: **Consenti** o **Blocca**.
6. Salvare le modifiche.

Come configurare la scansione delle connessioni criptate con un certificato non attendibile in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Impostazioni di rete**.
5. Nella sezione **Scansione delle connessioni criptate**, fare clic sul collegamento **Impostazioni**.
6. Nella finestra visualizzata, selezionare la modalità operativa dell'applicazione quando si visita un dominio con un certificato non attendibile: **Consenti connessione** o **Blocca connessione**.
7. Salvare le modifiche.

Come configurare la scansione delle connessioni criptate con un certificato non attendibile nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.
3. Nel blocco **Scansione delle connessioni criptate**, selezionare la modalità operativa dell'applicazione quando si visita un dominio con un certificato non attendibile: **Consenti** o **Blocca**.
4. Salvare le modifiche.



Avviso sulla visita di un dominio con un certificato non attendibile

Aggiunta del certificato Kaspersky al proprio archivio certificati

Browser e client di posta utilizzano il certificato per verificare la sicurezza e l'autenticità delle risorse Web. Il certificato fornisce anche il criptaggio dei dati tra le risorse Web e l'utente. La maggior parte dei browser e dei client di posta utilizza l'archivio certificati attendibile (archivio certificati di Windows). Ad esempio, Google Chrome. Alcuni browser e client di posta utilizzano il proprio archivio certificati per impostazione predefinita anziché l'archivio certificati di Windows. Ad esempio, Firefox e Thunderbird.

Dopo l'installazione, Kaspersky Endpoint Security aggiunge un certificato Kaspersky all'archivio di sistema per i certificati attendibili (archivio certificati Windows). Se Kaspersky Security Center è distribuito nell'organizzazione e viene applicato un criterio a un computer, Kaspersky Endpoint Security abilita automaticamente l'uso dell'archivio certificati di Windows nei browser e nei client di posta per analizzare il traffico di queste applicazioni. Se un criterio non viene applicato al computer, è possibile scegliere l'archivio certificati che verrà utilizzato dai browser e dai client di posta. Se è stato selezionato il proprio archivio certificati, aggiungere manualmente il certificato Kaspersky all'archivio. Ciò consentirà di evitare errori durante l'utilizzo del traffico HTTPS.

Per esaminare il traffico nel browser Mozilla Firefox e nel client di posta Thunderbird, è necessario abilitare Scansione delle connessioni criptate. Se Scansione delle connessioni criptate è disabilitata, l'applicazione non esamina il traffico nel browser Mozilla Firefox e nel client di posta Thunderbird. La scansione delle connessioni criptate deve inoltre essere abilitata per eseguire la scansione del traffico nei client di posta MyOffice Mail e R7-Office Organizer.

Prima di aggiungere un certificato all'archivio certificati del browser o dell'agente di posta, esportare il certificato Kaspersky dal Pannello di controllo di Windows (Proprietà Internet). È possibile ottenere ulteriori informazioni sull'aggiunta di un certificato all'archivio, ad esempio nel sito Web dell'assistenza tecnica di Mozilla.

È possibile scegliere l'archivio certificati solo nell'interfaccia locale dell'applicazione.

Per scegliere un archivio certificati per la scansione delle connessioni criptate nei browsere e nei client di posta:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.
3. Nella sezione **Scansione delle connessioni criptate** selezionare la casella di controllo **Per eseguire la scansione delle connessioni criptate nelle applicazioni con il proprio archivio certificati, utilizzare**.
4. Selezionare un archivio certificati:
   - **Archivio certificati Windows (scelta consigliata)**. Il certificato radice di Kaspersky viene aggiunto a questo archivio durante l'installazione di Kaspersky Endpoint Security.
   - **Archivio certificati personali**. Mozilla Firefox e Thunderbird utilizzano i propri archivi di certificati. Se è selezionato l'archivio certificati Mozilla, è necessario aggiungere manualmente il certificato radice Kaspersky a questo archivio tramite le proprietà del browser.

     Anche i client di posta MyOffice Mail e R7-Office Organizer utilizzano il proprio archivio certificati.
5. Salvare le modifiche.

Esclusione delle connessioni criptate dalla scansione

La maggior parte delle risorse Web utilizza connessioni criptate. Gli esperti di Kaspersky consigliano di abilitare Scansione delle connessioni criptate. Se la scansione delle connessioni criptate interferisce con l'attività lavorativa, è possibile aggiungere un sito Web alle esclusioni denominate *indirizzi attendibili*. In questo caso, Kaspersky Endpoint Security non esamina il traffico HTTPS degli indirizzi Web attendibili quando i componenti Protezione minacce Web, Protezione minacce di posta e Controllo Web sono in esecuzione.

Se un'applicazione attendibile utilizza una connessione criptata, è possibile disabilitare la scansione delle connessioni criptate per questa applicazione. È ad esempio possibile disabilitare la scansione delle connessioni criptate per le applicazioni di archiviazione cloud che utilizzano l'autenticazione a due fattori con il proprio certificato.

Come escludere un indirizzo Web dalle scansioni delle connessioni criptate in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni di rete**.
5. Nel blocco **Scansione delle connessioni criptate**, fare clic sul pulsante **Configura indirizzi attendibili**.
6. Fare clic su **Aggiungi**.
7. Se non si desidera che Kaspersky Endpoint Security esegua la scansione delle connessioni criptate stabilite quando si visita un dominio, immettere un nome di dominio o un indirizzo IP.

   Kaspersky Endpoint Security supporta il carattere `*` per l'immissione di una maschera nel nome di dominio.

   > Kaspersky Endpoint Security non supporta il simbolo `*` per gli indirizzi IP. È possibile selezionare un intervallo di indirizzi IP usando una maschera di sottorete (ad esempio 198.51.100.0/24).

   Esempi:

   - `domain.com` - Il record comprende i seguenti indirizzi: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Il record è esclusivo dei sottodomini (ad esempio, `subdomain.domain.com`).
   - `subdomain.domain.com` - Il record comprende i seguenti indirizzi: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Il record è esclusivo del dominio `domain.com`.
   - `*.domain.com` - Il record comprende i seguenti indirizzi: `https://movies.domain.com`, `https://images.domain.com/page123`. Il record è esclusivo del dominio `domain.com`.
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come escludere un indirizzo Web dalle scansioni delle connessioni criptate in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di rete**.
5. Nel blocco **Scansione delle connessioni criptate**, fare clic sul pulsante **Domini attendibili**.
6. Fare clic su **Aggiungi**.

7. Se non si desidera che Kaspersky Endpoint Security esegua la scansione delle connessioni criptate stabilite quando si visita un dominio, immettere un nome di dominio o un indirizzo IP.

   Kaspersky Endpoint Security supporta il carattere `*` per l'immissione di una maschera nel nome di dominio.

   > Kaspersky Endpoint Security non supporta il simbolo `*` per gli indirizzi IP. È possibile selezionare un intervallo di indirizzi IP usando una maschera di sottorete (ad esempio 198.51.100.0/24).

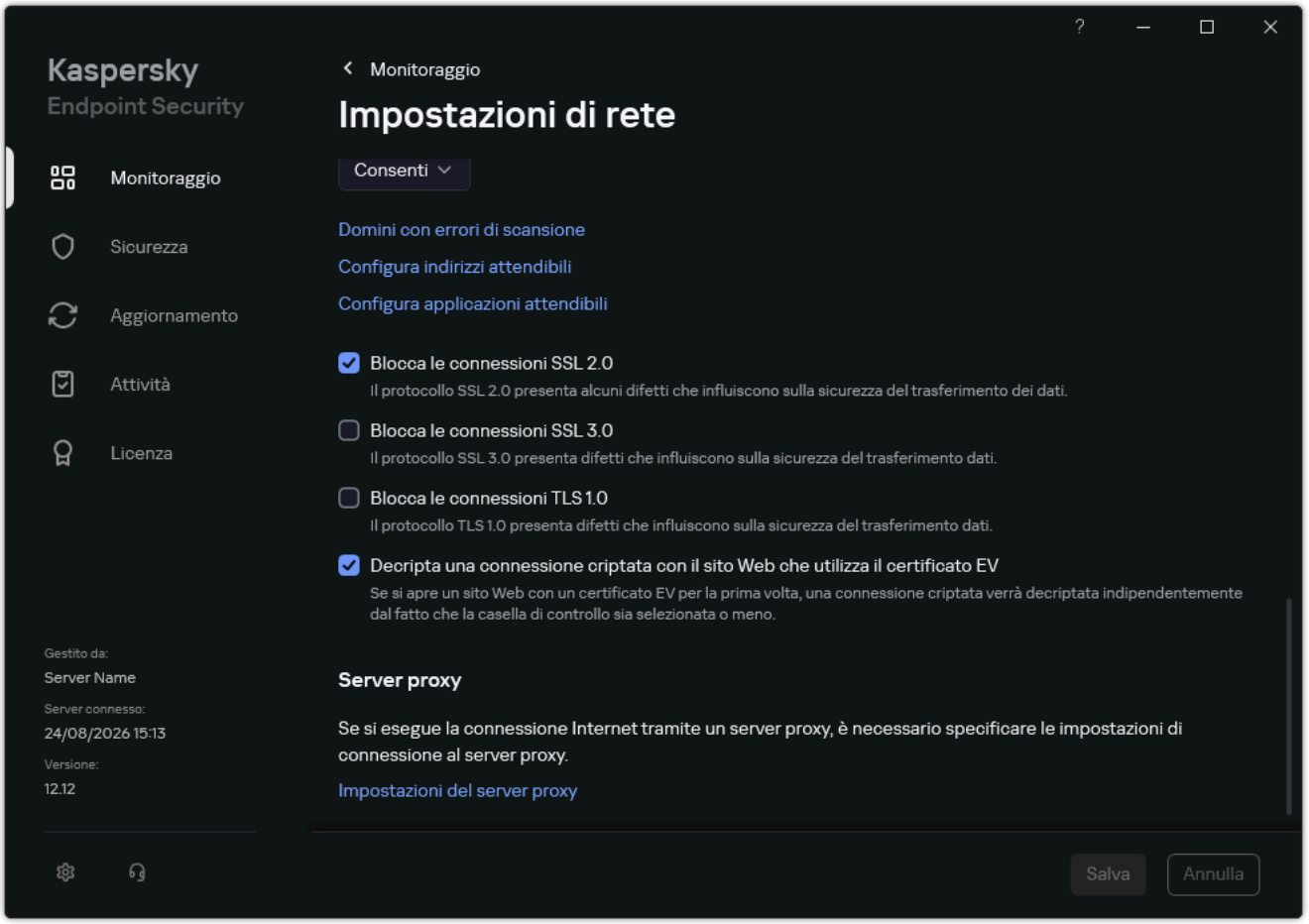
   Esempi:

   - `domain.com` - Il record comprende i seguenti indirizzi: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Il record è esclusivo dei sottodomini (ad esempio, `subdomain.domain.com`).
   - `subdomain.domain.com` - Il record comprende i seguenti indirizzi: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Il record è esclusivo del dominio `domain.com`.
   - `*.domain.com` - Il record comprende i seguenti indirizzi: `https://movies.domain.com`, `https://images.domain.com/page123`. Il record è esclusivo del dominio `domain.com`.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come escludere un indirizzo Web dalle scansioni delle connessioni criptate nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.



Impostazioni della rete delle applicazioni

3. Nel blocco **Scansione delle connessioni criptate**, fare clic sul pulsante **Configura indirizzi attendibili**.

4. Fare clic su **Aggiungi**.

5. Se non si desidera che Kaspersky Endpoint Security esegua la scansione delle connessioni criptate stabilite quando si visita un dominio, immettere un nome di dominio o un indirizzo IP.

   Kaspersky Endpoint Security supporta il carattere `*` per l'immissione di una maschera nel nome di dominio.

   > Kaspersky Endpoint Security non supporta il simbolo `*` per gli indirizzi IP. È possibile selezionare un intervallo di indirizzi IP usando una maschera di sottorete (ad esempio 198.51.100.0/24).

   Esempi:

   - `domain.com` - Il record comprende i seguenti indirizzi: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Il record è esclusivo dei sottodomini (ad esempio, `subdomain.domain.com`).
   - `subdomain.domain.com` - Il record comprende i seguenti indirizzi: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Il record è esclusivo del dominio `domain.com`.
   - `*.domain.com` - Il record comprende i seguenti indirizzi: `https://movies.domain.com`, `https://images.domain.com/page123`. Il record è esclusivo del dominio `domain.com`.

6. Salvare le modifiche.

Per impostazione predefinita, Kaspersky Endpoint Security non esegue la scansione delle connessioni criptate quando si verificano errori e aggiunge il sito Web a uno speciale elenco di *Domini con errori di scansione*. Kaspersky Endpoint Security compila un elenco separato per ciascun utente e non invia dati a Kaspersky Security Center. È possibile abilitare il blocco della connessione quando si verifica un errore di scansione. È possibile visualizzare un elenco dei domini con errori di scansione delle connessioni criptate solo nell'interfaccia locale dell'applicazione.

Per visualizzare l'elenco dei domini con errori di scansione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.

3. Nel blocco **Scansione delle connessioni criptate**, fare clic sul pulsante **Domini con errori di scansione**.

   Verrà visualizzato un elenco di domini con errori di scansione. Per ripristinare l'elenco, abilitare il blocco della connessione quando si verificano errori di scansione nel criterio, applicare il criterio, quindi ripristinare il parametro al valore iniziale e applicare nuovamente il criterio.

Gli specialisti Kaspersky creano un elenco di *eccezioni globali*: siti Web attendibili che Kaspersky Endpoint Security non controlla indipendentemente dalle impostazioni dell'applicazione.

Per visualizzare le esclusioni globali dalle scansioni del traffico criptato:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.
3. Nel blocco **Scansione delle connessioni criptate**, fare clic sul collegamento dell'elenco dei siti Web attendibili.

   Verrà visualizzato un elenco dei siti Web compilato dagli esperti di Kaspersky. Kaspersky Endpoint Security non esegue la scansione delle connessioni protette per i siti Web nell'elenco. L'elenco può essere aggiornato quando i moduli e i database di Kaspersky Endpoint Security vengono aggiornati.

Blocco dell'accesso ai domini con certificati non attendibili

In alcuni casi, quando viene bloccato l'accesso a un dominio con un certificato non attendibile, Kaspersky Endpoint Security visualizza nel browser una pagina di avviso HTML priva del collegamento alla risorsa Web richiesta.

Ciò può accadere per i seguenti motivi:

- L'amministratore ha bloccato l'accesso a un dominio con un certificato non attendibile.
- Il dominio dispone di un certificato non attendibile o non valido e il server Web utilizza il meccanismo HTTP Strict Transport Security (HSTS). *HSTS* è un meccanismo di sicurezza che impone l'utilizzo del protocollo HTTPS sicuro per la comunicazione tra un client e un server Web. In questo caso, non è possibile accedere al dominio anche se è stato aggiunto all'elenco degli indirizzi attendibili. Il meccanismo HSTS è descritto in RFC 6797.

  In alcuni casi, il sito Web può essere aperto direttamente in un browser senza utilizzare Kaspersky Endpoint Security. I browser non sempre rilevano i certificati revocati, mentre Kaspersky Endpoint Security verifica online se un certificato è stato revocato quando stabilisce una connessione. Ciò consente all'applicazione di rilevare un problema con il certificato prima del browser e di visualizzare il messaggio di errore corrispondente.



Avviso sulla visita di un dominio con un certificato non attendibile

Cancella dati

Kaspersky Endpoint Security consente di utilizzare un'attività per eliminare in remoto i dati dai computer degli utenti.

Kaspersky Endpoint Security elimina i dati nel modo seguente:

- in modalità automatica;
- nei dischi rigidi e nelle unità rimovibili;
- per tutti gli account utente nel computer.

Kaspersky Endpoint Security esegue l'attività *Cancella dati* indipendentemente dal tipo di licenza utilizzato, anche dopo la scadenza della licenza.

Modalità di Cancellazione dati

Questa attività consente di eliminare i dati nelle seguenti modalità:

- Eliminazione immediata dei dati.

  In questa modalità è possibile, ad esempio, eliminare i dati obsoleti per liberare spazio sul disco.

- Eliminazione dei dati posticipata.

  Questa modalità è destinata, ad esempio, a proteggere i dati in un laptop in caso di furto o smarrimento. È possibile configurare l'eliminazione automatica dei dati se il laptop si trova al di fuori della rete aziendale e non viene sincronizzato con Kaspersky Security Center da molto tempo.

Non è possibile impostare una pianificazione per l'eliminazione dei dati nelle proprietà dell'attività. È possibile eliminare i dati solo subito dopo aver avviato l'attività manualmente oppure configurare l'eliminazione posticipata dei dati se non è disponibile una connessione con Kaspersky Security Center.

Limitazioni

La cancellazione dati presenta le seguenti limitazioni:

- Solo un amministratore di Kaspersky Security Center può gestire l'attività *Cancella dati* Non è possibile configurare o avviare un'attività nell'interfaccia locale di Kaspersky Endpoint Security.
- Per il file system NTFS, Kaspersky Endpoint Security elimina solo i nomi dei principali flussi di dati. I nomi dei flussi di dati alternativi non possono essere eliminati.
- Quando si elimina un file di collegamento simbolico, Kaspersky Endpoint Security elimina anche i file i cui percorsi sono specificati nel collegamento simbolico.

Creazione di un'attività Cancella dati

Per eliminare i dati nei computer degli utenti:

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Cancella dati**.

   c. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Cancella dati (Antifurto)*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

   > Se vengono aggiunti nuovi computer a un gruppo di amministrazione all'interno dell'ambito dell'attività, l'attività di eliminazione immediata dei dati viene eseguita nei nuovi computer solo se viene completata entro 5 minuti dall'aggiunta dei nuovi computer.

5. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

6. Fare clic sull'attività **Cancella dati** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

7. Selezionare la scheda **Impostazioni applicazione**.

8. Selezionare il metodo di eliminazione dei dati:

   - **Elimina tramite il sistema operativo**. Kaspersky Endpoint Security utilizza le risorse del sistema operativo per eliminare i file senza inviarli al cestino.
   - **Elimina completamente, nessun ripristino possibile**. Kaspersky Endpoint Security sovrascrive i file con dati casuali. È praticamente impossibile ripristinare i dati in seguito all'eliminazione.

9. Se si desidera posticipare l'eliminazione dei dati, selezionare la casella di controllo **Cancella automaticamente i dati quando la connessione a Kaspersky Security Center si interrompe per più di N giorni**. Definire il numero di giorni.

   > L'attività di eliminazione posticipata dei dati verrà eseguita ogni volta che non viene stabilita una connessione a Kaspersky Security Center per il periodo di tempo definito.

Quando si configura l'eliminazione posticipata dei dati, tenere presente che i dipendenti potrebbero avere pianificazioni di lavoro diverse. È inoltre necessario considerare la pianificazione lavorativa degli utenti offline. Per informazioni dettagliate sull'utilizzo dei computer offline e sugli utenti fuori sede, consultare la Guida di Kaspersky Security Center.

Se il computer è spento e la connessione è assente per più del periodo configurato, dopo l'accensione del computer Kaspersky Endpoint Security non elimina immediatamente i dati. L'applicazione attende la sincronizzazione con Kaspersky Security Center per un'ora. Questo è necessario per impedire l'eliminazione non autorizzata dei dati nei computer degli utenti che hanno spento i computer, ad esempio prima di andare in ferie.

Se la casella di controllo è deselezionata, l'attività verrà eseguita subito dopo la sincronizzazione con Kaspersky Security Center.

10. Creare un elenco di oggetti da eliminare:

- **Cartelle**. Kaspersky Endpoint Security elimina tutti i file nella cartella e nelle relative sottocartelle. Kaspersky Endpoint Security non supporta le maschere e le variabili di ambiente per l'immissione del percorso di una cartella.
- **File per estensione**. Kaspersky Endpoint Security cerca i file con le estensioni specificate in tutte le unità del computer, incluse le unità rimovibili. Utilizzare i caratteri "`;` o `,`" per specificare più estensioni.
- **Ambito predefinito**. Kaspersky Endpoint Security eliminerà i file dalle seguenti aree:
  - **Documenti**. File nella cartella *Documenti* standard del sistema operativo e relative sottocartelle.
  - **Cookie**. File in cui il browser salva i dati dei siti Web visitati dall'utente (come i dati di autorizzazione dell'utente).
  - **Desktop**. File nella cartella *Desktop* standard del sistema operativo e relative sottocartelle.
  - **File temporanei di Internet Explorer**. File temporanei relativi all'esecuzione di Internet Explorer, come copie di pagine Web, immagini e file multimediali.
  - **File temporanei**. File temporanei relativi all'esecuzione delle applicazioni installate nel computer. Le applicazioni di Microsoft Office creano ad esempio file temporanei contenenti copie di backup dei documenti.
  - **File di Outlook**. File relativi all'esecuzione del client di posta di Outlook: file di dati (PST), file di dati offline (OST), file della rubrica offline (OAB) e file della rubrica personale (PAB).
  - **Profilo utente**. Set di file e cartelle in cui vengono archiviate le impostazioni del sistema operativo per l'account utente locale.

È possibile creare un elenco di oggetti da eliminare in ciascuna scheda. Kaspersky Endpoint Security creerà un elenco consolidato ed eliminerà i file da questo elenco al completamento di un'attività.

Non è possibile eliminare i file necessari per il funzionamento di Kaspersky Endpoint Security.

11. Salvare le modifiche.

12. Selezionare la casella di controllo accanto all'attività.

13. Fare clic su **Avvia**.

Di conseguenza, i dati nei computer degli utenti verranno eliminati in base alla modalità selezionata: subito o in mancanza di connessione. Se Kaspersky Endpoint Security non riesce a eliminare un file, ad esempio quando un utente sta utilizzando un file, l'applicazione non tenta di eliminarlo nuovamente. Per completare l'eliminazione dei dati, eseguire di nuovo l'attività.

Controllo del computer

Controllo Web

Controllo Web gestisce l'accesso degli utenti alle risorse Web. Questo consente di ridurre il traffico e l'utilizzo inappropriato dell'orario di lavoro. Quando un utente tenta di aprire un sito Web sottoposto a restrizioni da Controllo Web, Kaspersky Endpoint Security bloccherà l'accesso o mostrerà un avviso (vedere la figura seguente).

Per utilizzare Controllo Web, è necessario completare la configurazione iniziale dell'applicazione:

- Per il monitoraggio del traffico HTTPS, abilitare la scansione delle connessioni criptate (abilitata per impostazione predefinita).
- Selezionare le porte che Kaspersky Endpoint Security deve monitorare (per impostazione predefinita, l'applicazione monitora tutte le porte).
- Selezionare le applicazioni il cui traffico si desidera venga monitorato da Kaspersky Endpoint Security. La maggior parte dei browser è già presente nell'elenco delle applicazioni consigliate da Kaspersky. Se il browser non è presente nell'elenco, aggiungerlo manualmente.
- Si consiglia di inoculare lo script per l'interazione con le pagine Web nel traffico Web (per impostazione predefinita, l'inserimento dello script è disabilitato). Questo script consente la registrazione degli eventi di Controllo Web per il registro eventi dell'applicazione, il registro eventi del sistema operativo e i rapporti.

Metodi per la gestione dell'accesso ai siti Web

Controllo Web consente di configurare l'accesso ai siti Web utilizzando i seguenti metodi:

- **Categoria di siti Web**. I siti Web vengono suddivisi in categorie in base al servizio cloud di Kaspersky Security Network, all'analisi euristica e al database dei siti Web noti (inclusi nei database delle applicazioni). È ad esempio possibile limitare l'accesso degli utenti alla categoria *Social network* o ad altre categorie.
- **Tipo di dati**. È ad esempio possibile limitare l'accesso degli utenti ai dati di un sito Web e nascondere le immagini. Kaspersky Endpoint Security determina il tipo di dati in base al formato di file e non in base alla relativa estensione.

  > Kaspersky Endpoint Security non esegue la scansione dei file all'interno degli archivi. Se ad esempio i file di immagini sono stati inseriti in un archivio, Kaspersky Endpoint Security identifica il tipo di dati *Archivi* e non *Grafica*.

- **A singoli indirizzi**. È possibile inserire un indirizzo Web o usare le maschere.

È possibile utilizzare diversi metodi contemporaneamente per regolare l'accesso ai siti Web. È ad esempio possibile limitare l'accesso al tipo di dati *Applicazioni Office* solo per la categoria di siti Web *E-mail basata sul Web*.

Regole di accesso ai siti Web

Controllo Web gestisce l'accesso dell'utente ai siti Web utilizzando le *regole di accesso*. È possibile configurare le seguenti impostazioni avanzate per una regola di accesso ai siti Web:

- Utenti ai quali si applica la regola.

  È ad esempio possibile limitare l'accesso a Internet tramite un browser per tutti gli utenti dell'azienda ad eccezione del dipartimento IT.

- Pianificazione regola.

  È ad esempio possibile limitare l'accesso a Internet tramite un browser solo durante l'orario di lavoro.

Priorità delle regole di accesso

Ogni regola ha una priorità. Più alta è la posizione di una regola nell'elenco, maggiore è la priorità. Se un sito Web è stato aggiunto a più regole, Controllo Web regola l'accesso al sito Web in base alla regola con la massima priorità. Ad esempio, Kaspersky Endpoint Security potrebbe identificare un portale aziendale come social network. Per limitare l'accesso ai social network e fornire l'accesso al portale Web aziendale, creare due regole: una regola di blocco per la categoria di siti Web *Social network* e una regola di permesso per il portale Web aziendale. La regola di accesso per il portale Web aziendale deve avere una priorità più elevata rispetto alla regola di accesso per i social network.





Messaggi di Controllo Web

Aggiunta di una regola di accesso alle risorse Web

Una *regola di accesso alle risorse Web* è un insieme di filtri e azioni che Kaspersky Endpoint Security applica quando gli utenti visitano le risorse Web. Le regole di accesso possono includere una pianificazione delle regole.

Non è consigliabile creare più di 1000 regole di accesso alle risorse Web, poiché questo può comportare l'instabilità del sistema.

Una regola di accesso alle risorse Web è un set di filtri e azioni eseguiti da Kaspersky Endpoint Security quando un utente visita le risorse Web descritte nella regola durante l'intervallo di tempo specificato nella pianificazione della regola. I filtri consentono di specificare con esattezza un pool di risorse Web per cui l'accesso deve essere controllato dal componente Controllo Web.

Sono disponibili i seguenti filtri:

- **Filtro per contenuti**. Controllo Web categorizza le risorse Web per contenuto e tipo di dati. È possibile controllare l'accesso degli utenti alle risorse Web con contenuti e dati che rientrano nei tipi definiti da queste categorie. Quando gli utenti visitano le risorse Web che appartengono alla categoria di contenuti e/o di tipi di dati selezionata, Kaspersky Endpoint Security esegue l'azione specificata nella regola.

- **Filtro per indirizzi di risorse Web**. È possibile controllare l'accesso degli utenti a tutti gli indirizzi di risorse Web oppure a singoli indirizzi di risorse Web e/o a gruppi di indirizzi di risorse Web.

  Se sono specificati filtri in base al contenuto e in base agli indirizzi di risorse Web e gli indirizzi e/o i gruppi di indirizzi di risorse Web specificati appartengono alle categorie di contenuti o di tipi di dati selezionate, Kaspersky Endpoint Security non controlla l'accesso a tutte le risorse Web nelle categorie di contenuti e/o di tipi di dati selezionate. L'applicazione controlla invece solo l'accesso agli indirizzi e/o ai gruppi di indirizzi di risorse Web specificati.

- **Filtro in base ai nomi di utenti e gruppi di utenti**. È possibile specificare i nomi degli utenti e dei gruppi di utenti per cui l'accesso alle risorse Web viene controllato in base alla regola.

- **Pianificazione regola**. È possibile specificare la pianificazione della regola. La pianificazione della regola determina il periodo di tempo durante il quale Kaspersky Endpoint Security monitora l'accesso alle risorse Web coperte dalla regola.

Dopo l'installazione di Kaspersky Endpoint Security, l'elenco delle regole del componente Controllo Web non è vuoto. La *Regola predefinita* è preimpostata. Questa regola viene applicata a tutte le risorse Web a cui non si applicano altre regole e consente o blocca l'accesso a tali risorse Web per tutti gli utenti.

Ogni regola ha una priorità. Più alta è la posizione di una regola nell'elenco, maggiore è la priorità. Se un sito Web è stato aggiunto a più regole, Controllo Web regola l'accesso al sito Web in base alla regola con la massima priorità. Ad esempio, Kaspersky Endpoint Security potrebbe identificare un portale aziendale come social network. Per limitare l'accesso ai social network e fornire l'accesso al portale Web aziendale, creare due regole: una regola di blocco per la categoria di siti Web *Social network* e una regola di permesso per il portale Web aziendale. La regola di accesso per il portale Web aziendale deve avere una priorità più elevata rispetto alla regola di accesso per i social network.

Come aggiungere una regola di accesso alle risorse Web in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo Web**.
4. Selezionare la casella di controllo **Controllo Web**.
5. Nel blocco **Impostazioni di Controllo Web**, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Regola di accesso alle risorse Web**.
6. Configurare la regola di accesso alle risorse Web (vedere la tabella seguente).
7. Se si desidera che Controllo Web termini la connessione con la risorsa Web vietata subito dopo l'applicazione del criterio, selezionare la casella di controllo **Termina le sessioni browser attive dopo l'applicazione della regola**.

   > Controllo Web consente di disconnettere immediatamente le risorse Web solo nei browser Web. Per le altre applicazioni, Controllo Web limita solo le nuove connessioni.

   Se la casella di controllo è deselezionata, Controllo Web limita solo le nuove connessioni alle risorse Web vietate. Controllo Web non termina le connessioni attive.
8. Salvare le modifiche.

Come aggiungere una regola di accesso alle risorse Web in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza → Controllo Web**.

5. Attivare l'interruttore **Controllo Web ABILITATO**.

6. Nel blocco **Elenco di regole**, fare clic sul pulsante **Aggiungi**.

7. Configurare la regola di accesso alle risorse Web (vedere la tabella seguente).

8. Se si desidera che Controllo Web termini la connessione con la risorsa Web vietata subito dopo l'applicazione del criterio, selezionare la casella di controllo **Termina le sessioni browser attive dopo l'applicazione della regola**.

   Controllo Web consente di disconnettere immediatamente le risorse Web solo nei browser Web. Per le altre applicazioni, Controllo Web limita solo le nuove connessioni.

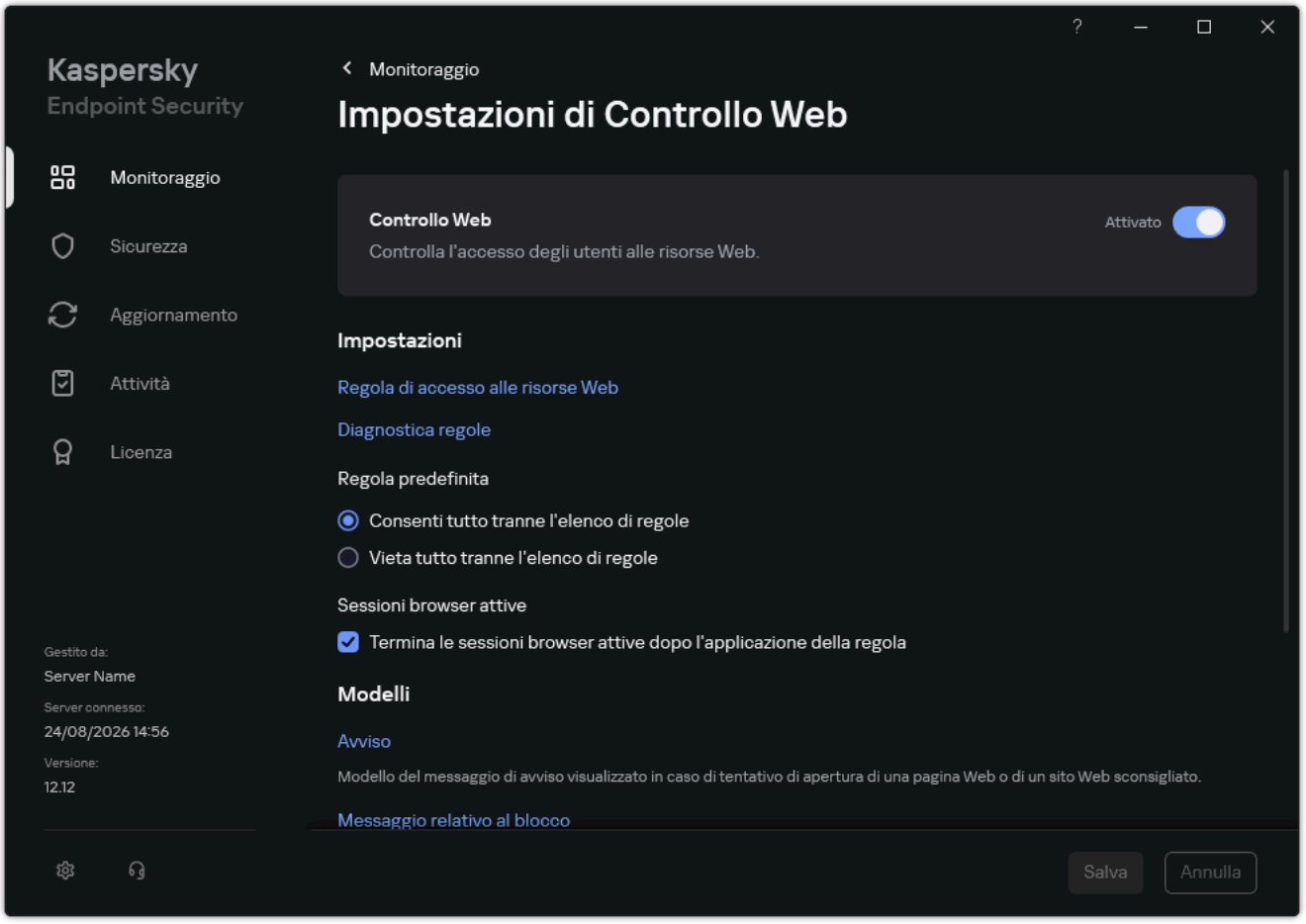
   Se la casella di controllo è deselezionata, Controllo Web limita solo le nuove connessioni alle risorse Web vietate. Controllo Web non termina le connessioni attive.

9. Salvare le modifiche.

Come aggiungere una regola di accesso alle risorse Web nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza → Controllo Web**.



Impostazioni di Controllo Web

3. Attivare l'interruttore **Controllo Web**.

4. Nel blocco **Impostazioni**, fare clic sul pulsante **Regola di accesso alle risorse Web**.

5. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Regola di accesso alle risorse Web**.

6. Configurare la regola di accesso alle risorse Web (vedere la tabella seguente).

7. Se si desidera che Controllo Web termini la connessione con la risorsa Web vietata subito dopo l'applicazione del criterio, selezionare la casella di controllo **Termina le sessioni browser attive dopo l'applicazione della regola**.

   Controllo Web consente di disconnettere immediatamente le risorse Web solo nei browser Web. Per le altre applicazioni, Controllo Web limita solo le nuove connessioni.

   Se la casella di controllo è deselezionata, Controllo Web limita solo le nuove connessioni alle risorse Web vietate. Controllo Web non termina le connessioni attive.

8. Salvare le modifiche.

Di conseguenza, la nuova regola di Controllo Web viene aggiunta all'elenco. Se necessario, modificare la priorità della regola di Controllo Web. È inoltre possibile utilizzare l'interruttore per disabilitare la regola di accesso alle risorse Web in qualsiasi momento senza rimuoverla dall'elenco.

Parametri della regola di Controllo Web

Parametro	Descrizione
Nome regola	Nome della regola di Controllo Web.
Stato	• **Attivato**. • **Disattivato**. È possibile utilizzare l'interruttore per disabilitare la regola di accesso alle risorse Web in qualsiasi momento.
Azione	• **Consenti**. Controllo Web consente l'accesso alle risorse Web che corrispondono ai parametri della regola. • **Blocca**. Controllo Web blocca l'accesso alle risorse Web che corrispondono ai parametri della regola e mostra un messaggio di accesso negato al sito Web. • **Avvisa**. Quando l'utente tenta di accedere a una risorsa Web che corrisponde alla regola, Controllo Web mostra un avviso che informa che è sconsigliabile visitare la risorsa Web. Utilizzando i collegamenti nel messaggio di avviso, l'utente può ottenere l'accesso alla risorsa Web richiesta.
Contenuti del filtro	• **Per categorie di contenuti**. È possibile controllare l'accesso degli utenti alle risorse Web per categoria (ad esempio la categoria *Social network*). • **Per tipi di dati**. È possibile controllare l'accesso degli utenti alle risorse Web in base al tipo specifico dei dati pubblicati (ad esempio *Grafica*).
Indirizzi	• **A tutti gli indirizzi**. Controllo Web non filtrerà le risorse Web in base all'indirizzo. • **A singoli indirizzi**. Controllo Web filtrerà solo gli indirizzi delle risorse Web presenti nell'elenco. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio. Se la Scansione delle connessioni criptate è disabilitata, per il protocollo HTTPS è possibile filtrare solo in base al nome del server.
Utenti	• **A tutti gli utenti**. Controllo Web non filtrerà le risorse Web per utenti specifici. • **A singoli utenti e / o gruppi**. Controllo Web filtrerà le risorse Web solo per utenti specifici. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.
Pianificazione regola	La pianificazione della regola determina il periodo di tempo durante il quale Kaspersky Endpoint Security monitora l'accesso alle risorse Web coperte dalla regola. È ad esempio possibile limitare l'accesso a Internet tramite un browser solo durante l'orario di lavoro.

Filtro in base agli indirizzi delle risorse Web

Per controllare l'accesso alle singole risorse Web, è necessario creare una regola di Controllo Web, creare un elenco di indirizzi Web e selezionare un'azione Controllo Web. Quando si crea un elenco di indirizzi Web, è possibile inserire indirizzi URL o utilizzare maschere.

Le regole possono includere una pianificazione delle regole e un elenco di utenti a cui si applica la regola. Ad esempio, è possibile limitare l'accesso ai siti Web solo durante l'orario di lavoro o consentire la visita dei siti Web agli utenti di determinati gruppi.

Come abilitare un filtro degli indirizzi delle risorse Web in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo Web**.
4. Selezionare la casella di controllo **Controllo Web**.
5. Nel blocco **Impostazioni di Controllo Web**, fare clic sul pulsante **Aggiungi**.
   Verrà visualizzata la finestra **Regola di accesso alle risorse Web**.
6. Configurare la regola di accesso alle risorse Web:
   a. Nel campo **Nome** immettere il nome della regola.
   b. Nell'elenco a discesa **Applica agli indirizzi**, selezionare **A singoli indirizzi**.
   c. Creare un elenco di indirizzi delle risorse Web. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT.

      Se la Scansione delle connessioni criptate è disabilitata, per il protocollo HTTPS è possibile filtrare solo in base al nome del server.

   d. Nell'elenco a discesa **Applica agli utenti**, selezionare il filtro pertinente per gli utenti:
      - **A tutti gli utenti**. Controllo Web non filtrerà le risorse Web in base all'indirizzo.
      - **A singoli utenti o gruppi**. Controllo Web filtrerà solo gli indirizzi delle risorse Web presenti nell'elenco. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

e. Nell'elenco a discesa **Azione**, selezionare un'opzione:

- **Consenti**. Controllo Web consente l'accesso alle risorse Web che corrispondono ai parametri della regola.
- **Blocca**. Controllo Web blocca l'accesso alle risorse Web che corrispondono ai parametri della regola e mostra un messaggio di accesso negato al sito Web.
- **Avvisa**. Quando l'utente tenta di accedere a una risorsa Web che corrisponde alla regola, Controllo Web mostra un avviso che informa che è sconsigliabile visitare la risorsa Web. Utilizzando i collegamenti nel messaggio di avviso, l'utente può ottenere l'accesso alla risorsa Web richiesta.

f. Nell'elenco a discesa **Pianificazione regola**, selezionare una pianificazione o creare una nuova pianificazione.

7. Se si desidera che Controllo Web termini la connessione con la risorsa Web vietata subito dopo l'applicazione del criterio, selezionare la casella di controllo **Termina le sessioni browser attive dopo l'applicazione della regola**.

   Controllo Web consente di disconnettere immediatamente le risorse Web solo nei browser Web. Per le altre applicazioni, Controllo Web limita solo le nuove connessioni.

   Se la casella di controllo è deselezionata, Controllo Web limita solo le nuove connessioni alle risorse Web vietate. Controllo Web non termina le connessioni attive.

8. Salvare le modifiche.

Come abilitare un filtro degli indirizzi delle risorse Web in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo Web**.
5. Attivare l'interruttore **Controllo Web ABILITATO**.
6. Nel blocco **Elenco di regole**, fare clic sul pulsante **Aggiungi**.
7. Configurare la regola di accesso alle risorse Web:

   a. Nel campo **Nome regola** immettere il nome della regola.

   b. Selezionare lo stato **Abilitato** per la regola di accesso alle risorse Web.

   È possibile utilizzare l'interruttore per disabilitare la regola di accesso alle risorse Web in qualsiasi momento senza rimuoverla dall'elenco.

c. Nel blocco **Azione**, selezionare l'opzione pertinente:

- **Consenti**. Controllo Web consente l'accesso alle risorse Web che corrispondono ai parametri della regola.
- **Blocca**. Controllo Web blocca l'accesso alle risorse Web che corrispondono ai parametri della regola e mostra un messaggio di accesso negato al sito Web.
- **Informa**. Quando l'utente tenta di accedere a una risorsa Web che corrisponde alla regola, Controllo Web mostra un avviso che informa che è sconsigliabile visitare la risorsa Web. Utilizzando i collegamenti nel messaggio di avviso, l'utente può ottenere l'accesso alla risorsa Web richiesta.

d. In **Ambito**, selezionare **Siti Web individuali**.

e. Configurare il filtro dei contenuti:

- **Indirizzo individuale**. Creare un elenco di indirizzi delle risorse Web. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT.

  > Se la Scansione delle connessioni criptate è disabilitata, per il protocollo HTTPS è possibile filtrare solo in base al nome del server.

- **Tipo di dati**. È possibile controllare l'accesso degli utenti alle risorse Web in base al tipo specifico dei dati pubblicati (ad esempio *Grafica*).

f. In **Utente o gruppo**, selezionare gli utenti a cui si desidera che Controllo Web applichi la regola.

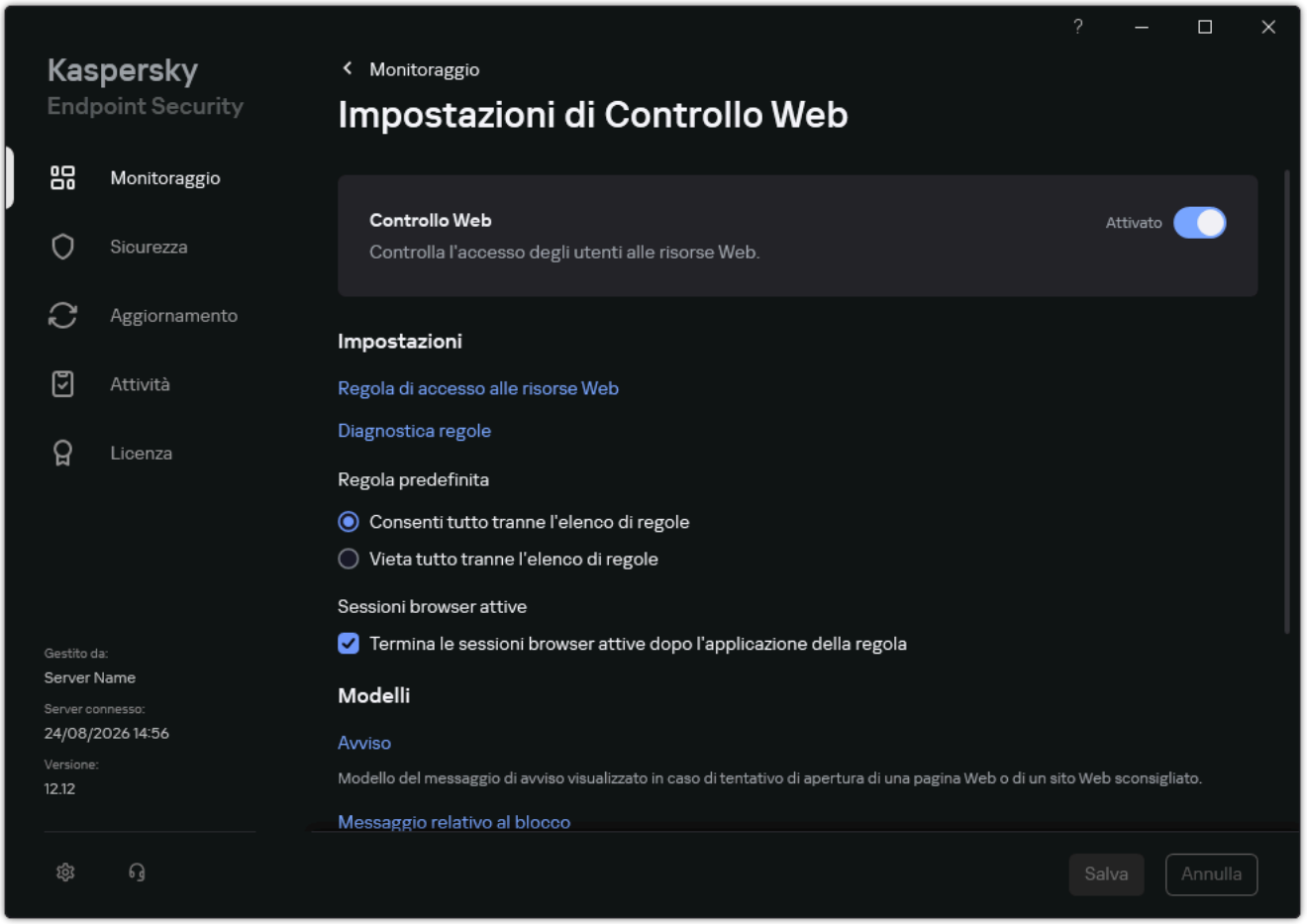
Controllo Web filtrerà solo gli indirizzi delle risorse Web presenti nell'elenco. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

g. Nel blocco **Pianificazione di accesso**, selezionare una pianificazione o creare una nuova pianificazione.

8. Salvare le modifiche.

Come abilitare un filtro degli indirizzi delle risorse Web nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo Web**.



Impostazioni di Controllo Web

3. Nel blocco **Impostazioni**, fare clic sul pulsante **Regola di accesso alle risorse Web**.
4. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Regola di accesso alle risorse Web**.
5. Nel campo **Nome regola** immettere il nome della regola.
6. Selezionare lo stato **Attivato** per la regola di accesso alle risorse Web.

   È possibile utilizzare l'interruttore per disabilitare la regola di accesso alle risorse Web in qualsiasi momento.
7. Nel blocco **Azione**, selezionare l'opzione pertinente:

   - **Consenti**. Controllo Web consente l'accesso alle risorse Web che corrispondono ai parametri della regola.
   - **Blocca**. Controllo Web blocca l'accesso alle risorse Web che corrispondono ai parametri della regola e mostra un messaggio di accesso negato al sito Web.
   - **Avvisa**. Quando l'utente tenta di accedere a una risorsa Web che corrisponde alla regola, Controllo Web mostra un avviso che informa che è sconsigliabile visitare la risorsa Web. Utilizzando i collegamenti nel messaggio di avviso, l'utente può ottenere l'accesso alla risorsa Web richiesta.
8. In **Indirizzi**, selezionare **A singoli indirizzi**.

Creare un elenco di indirizzi delle risorse Web. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT.

> Se la Scansione delle connessioni criptate è disabilitata, per il protocollo HTTPS è possibile filtrare solo in base al nome del server.

9. Nella sezione **Utenti** selezionare il filtro pertinente per gli utenti:

   - **A tutti gli utenti**. Controllo Web non filtrerà le risorse Web per utenti specifici.
   - **A singoli utenti e / o gruppi**. Controllo Web filtrerà solo gli indirizzi delle risorse Web presenti nell'elenco. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

10. Nell'elenco a discesa **Pianificazione regola**, selezionare una pianificazione o creare una nuova pianificazione.

11. Se si desidera che Controllo Web termini la connessione con la risorsa Web vietata subito dopo l'applicazione del criterio, selezionare la casella di controllo **Termina le sessioni browser attive dopo l'applicazione della regola**.

    > Controllo Web consente di disconnettere immediatamente le risorse Web solo nei browser Web. Per le altre applicazioni, Controllo Web limita solo le nuove connessioni.

    Se la casella di controllo è deselezionata, Controllo Web limita solo le nuove connessioni alle risorse Web vietate. Controllo Web non termina le connessioni attive.

12. Salvare le modifiche.

Di conseguenza, la nuova regola di Controllo Web viene aggiunta all'elenco. Se necessario, modificare la priorità della regola di Controllo Web. È inoltre possibile utilizzare l'interruttore per disabilitare la regola di accesso alle risorse Web in qualsiasi momento senza rimuoverla dall'elenco.

Filtro in base ai contenuti delle risorse Web

Per controllare l'accesso in base al contenuto delle risorse Web, Controllo Web fornisce un filtro di categoria e un filtro del tipo di dati.

I siti Web vengono suddivisi in categorie in base al servizio cloud di Kaspersky Security Network, all'analisi euristica e al database dei siti Web noti (inclusi nei database delle applicazioni). È ad esempio possibile limitare l'accesso degli utenti alla categoria *Social network* o ad altre categorie.

È possibile limitare l'accesso degli utenti a un sito Web in base al tipo di dati, ad esempio per nascondere le immagini. Kaspersky Endpoint Security determina il tipo di dati in base al formato di file e non in base alla relativa estensione. Controllo Web distingue i seguenti tipi di dati:

- Video
- Audio

- Applicazioni Office
- File eseguibili
- Archivi
- Grafica
- Script

Kaspersky Endpoint Security non esegue la scansione dei file all'interno degli archivi. Se ad esempio i file di immagini sono stati inseriti in un archivio, Kaspersky Endpoint Security identifica il tipo di dati *Archivi* e non *Grafica*.

Le regole possono includere una pianificazione delle regole e un elenco di utenti a cui si applica la regola. Ad esempio, è possibile limitare l'accesso ai siti Web solo durante l'orario di lavoro o consentire la visita dei siti Web agli utenti di determinati gruppi.

Come abilitare un filtro di contenuti delle risorse Web in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo Web**.
4. Selezionare la casella di controllo **Controllo Web**.
5. Nel blocco **Impostazioni di Controllo Web**, fare clic sul pulsante **Aggiungi**.
   Verrà visualizzata la finestra **Regola di accesso alle risorse Web**.
6. Configurare la regola di accesso alle risorse Web:
   a. Nel campo **Nome** immettere il nome della regola.
   b. Nell'elenco a discesa **Filtro contenuti**, selezionare il filtro del contenuto opportuno:
      - **Per categorie di contenuti**. È possibile controllare l'accesso degli utenti alle risorse Web per categoria (ad esempio la categoria *Social network*).
      - **Per tipi di dati**. È possibile controllare l'accesso degli utenti alle risorse Web in base al tipo specifico dei dati pubblicati (ad esempio *Grafica*).
      - **Per categorie di contenuti e tipi di dati**. Vengono abilitati i filtri in base alle categorie di contenuti e ai tipi di dati.

   Dopo aver selezionato i filtri, configurare i parametri degli stessi.

c. Nell'elenco a discesa **Applica agli utenti**, selezionare il filtro pertinente per gli utenti:

- **A tutti gli utenti**. Controllo Web non filtrerà le risorse Web in base all'indirizzo.
- **A singoli utenti o gruppi**. Controllo Web filtrerà solo gli indirizzi delle risorse Web presenti nell'elenco. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

d. Nell'elenco a discesa **Azione**, selezionare un'opzione:

- **Consenti**. Controllo Web consente l'accesso alle risorse Web che corrispondono ai parametri della regola.
- **Blocca**. Controllo Web blocca l'accesso alle risorse Web che corrispondono ai parametri della regola e mostra un messaggio di accesso negato al sito Web.
- **Avvisa**. Quando l'utente tenta di accedere a una risorsa Web che corrisponde alla regola, Controllo Web mostra un avviso che informa che è sconsigliabile visitare la risorsa Web. Utilizzando i collegamenti nel messaggio di avviso, l'utente può ottenere l'accesso alla risorsa Web richiesta.

e. Nell'elenco a discesa **Pianificazione regola**, selezionare una pianificazione o creare una nuova pianificazione.

7. Se si desidera che Controllo Web termini la connessione con la risorsa Web vietata subito dopo l'applicazione del criterio, selezionare la casella di controllo **Termina le sessioni browser attive dopo l'applicazione della regola**.

   Controllo Web consente di disconnettere immediatamente le risorse Web solo nei browser Web. Per le altre applicazioni, Controllo Web limita solo le nuove connessioni.

   Se la casella di controllo è deselezionata, Controllo Web limita solo le nuove connessioni alle risorse Web vietate. Controllo Web non termina le connessioni attive.

8. Salvare le modifiche.

Come abilitare un filtro di contenuti delle risorse Web in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo Web**.
5. Attivare l'interruttore **Controllo Web ABILITATO**.
6. Nel blocco **Elenco di regole**, fare clic sul pulsante **Aggiungi**.

7. Configurare la regola di accesso alle risorse Web:

   a. Nel campo **Nome regola** immettere il nome della regola.

   b. Selezionare lo stato **Abilitato** per la regola di accesso alle risorse Web.

      È possibile utilizzare l'interruttore per disabilitare la regola di accesso alle risorse Web in qualsiasi momento.

   c. Nel blocco **Azione**, selezionare l'opzione pertinente:

      - **Consenti**. Controllo Web consente l'accesso alle risorse Web che corrispondono ai parametri della regola.
      - **Blocca**. Controllo Web blocca l'accesso alle risorse Web che corrispondono ai parametri della regola e mostra un messaggio di accesso negato al sito Web.
      - **Informa**. Quando l'utente tenta di accedere a una risorsa Web che corrisponde alla regola, Controllo Web mostra un avviso che informa che è sconsigliabile visitare la risorsa Web. Utilizzando i collegamenti nel messaggio di avviso, l'utente può ottenere l'accesso alla risorsa Web richiesta.

   d. In **Ambito**, selezionare **Categoria di contenuti**.

   e. Configurare il filtro dei contenuti:

      - **Categoria di contenuti**. È possibile controllare l'accesso degli utenti alle risorse Web per categoria (ad esempio la categoria *Social network*).
      - **Tipo di dati**. È possibile controllare l'accesso degli utenti alle risorse Web in base al tipo specifico dei dati pubblicati (ad esempio *Grafica*).

   f. In **Utente o gruppo**, selezionare gli utenti a cui si desidera che Controllo Web applichi la regola.

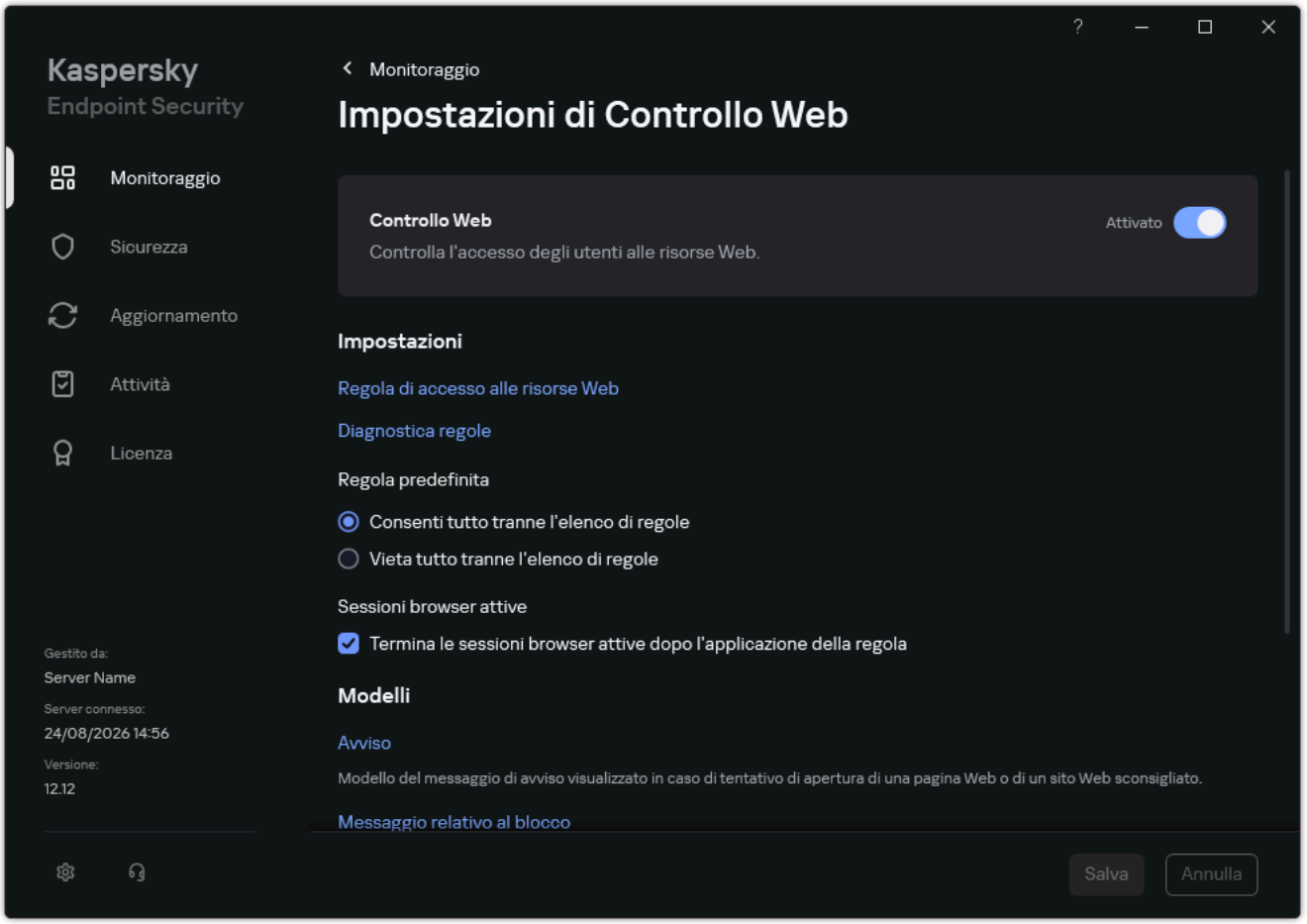
      Controllo Web filtrerà solo gli indirizzi delle risorse Web presenti nell'elenco. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

   g. Nel blocco **Pianificazione di accesso**, selezionare una pianificazione o creare una nuova pianificazione.

8. Salvare le modifiche.

Come abilitare un filtro di contenuti delle risorse Web nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo Web**.



Impostazioni di Controllo Web

3. Nel blocco **Impostazioni**, fare clic sul pulsante **Regola di accesso alle risorse Web**.
4. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Regola di accesso alle risorse Web**.
5. Nel campo **Nome regola** immettere il nome della regola.
6. Selezionare lo stato **Attivato** per la regola di accesso alle risorse Web.

   È possibile utilizzare l'interruttore per disabilitare la regola di accesso alle risorse Web in qualsiasi momento.
7. Nel blocco **Azione**, selezionare l'opzione pertinente:

   - **Consenti**. Controllo Web consente l'accesso alle risorse Web che corrispondono ai parametri della regola.
   - **Blocca**. Controllo Web blocca l'accesso alle risorse Web che corrispondono ai parametri della regola e mostra un messaggio di accesso negato al sito Web.
   - **Avvisa**. Quando l'utente tenta di accedere a una risorsa Web che corrisponde alla regola, Controllo Web mostra un avviso che informa che è sconsigliabile visitare la risorsa Web. Utilizzando i collegamenti nel messaggio di avviso, l'utente può ottenere l'accesso alla risorsa Web richiesta.

8. Nella sezione **Contenuti del filtro**, selezionare il filtro del contenuto opportuno:

   - **Per categorie di contenuti**. È possibile controllare l'accesso degli utenti alle risorse Web per categoria (ad esempio la categoria *Social network*).
   - **Per tipi di dati**. È possibile controllare l'accesso degli utenti alle risorse Web in base al tipo specifico dei dati pubblicati (ad esempio *Grafica*).

   Per configurare il filtro dei contenuti:

   a. Fare clic sul collegamento **Impostazioni**.

   b. Selezionare le caselle di controllo accanto ai nomi delle categorie di contenuti e/o tipi di dati desiderate.

   Selezionando la casella di controllo accanto al nome di una categoria di contenuti e/o tipi di dati, Kaspersky Endpoint Security applicherà la regola per il controllo dell'accesso alle risorse Web che appartengono alle categorie di contenuti e/o tipi di dati selezionate.

   c. Tornare alla finestra per la configurazione della regola di accesso alle risorse Web.

9. Nella sezione **Utenti** selezionare il filtro pertinente per gli utenti:

   - **A tutti gli utenti**. Controllo Web non filtrerà le risorse Web in base all'indirizzo.
   - **A singoli utenti e / o gruppi**. Controllo Web filtrerà solo gli indirizzi delle risorse Web presenti nell'elenco. È possibile inserire un indirizzo Web o usare le maschere. È inoltre possibile esportare un elenco di indirizzi di risorse Web da un file TXT. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio. Per creare un elenco di utenti a cui applicare la regola:

     a. Fare clic su **Aggiungi**.

     b. Nella finestra visualizzata, selezionare gli utenti o i gruppi di utenti a cui si desidera applicare la regola di accesso alle risorse Web.

     c. Tornare alla finestra per la configurazione della regola di accesso alle risorse Web.

10. Nell'elenco a discesa **Pianificazione regola** selezionare il nome della pianificazione desiderata oppure generare una nuova pianificazione basata sulla pianificazione della regola selezionata. A tale scopo:

    a. Fare clic su **Modifica o aggiungi nuovo**.

    b. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.

    c. Nella finestra visualizzata, immettere il nome della pianificazione della regola.

    d. Configurare la pianificazione di accesso alle risorse Web per gli utenti.

    e. Tornare alla finestra per la configurazione della regola di accesso alle risorse Web.

11. Se si desidera che Controllo Web termini la connessione con la risorsa Web vietata subito dopo l'applicazione del criterio, selezionare la casella di controllo **Termina le sessioni browser attive dopo l'applicazione della regola**.

Controllo Web consente di disconnettere immediatamente le risorse Web solo nei browser Web. Per le altre applicazioni, Controllo Web limita solo le nuove connessioni.

Se la casella di controllo è deselezionata, Controllo Web limita solo le nuove connessioni alle risorse Web vietate. Controllo Web non termina le connessioni attive.

12. Salvare le modifiche.

Di conseguenza, la nuova regola di Controllo Web viene aggiunta all'elenco. Se necessario, modificare la priorità della regola di Controllo Web. È inoltre possibile utilizzare l'interruttore per disabilitare la regola di accesso alle risorse Web in qualsiasi momento senza rimuoverla dall'elenco.

Verifica delle regole di accesso alle risorse Web

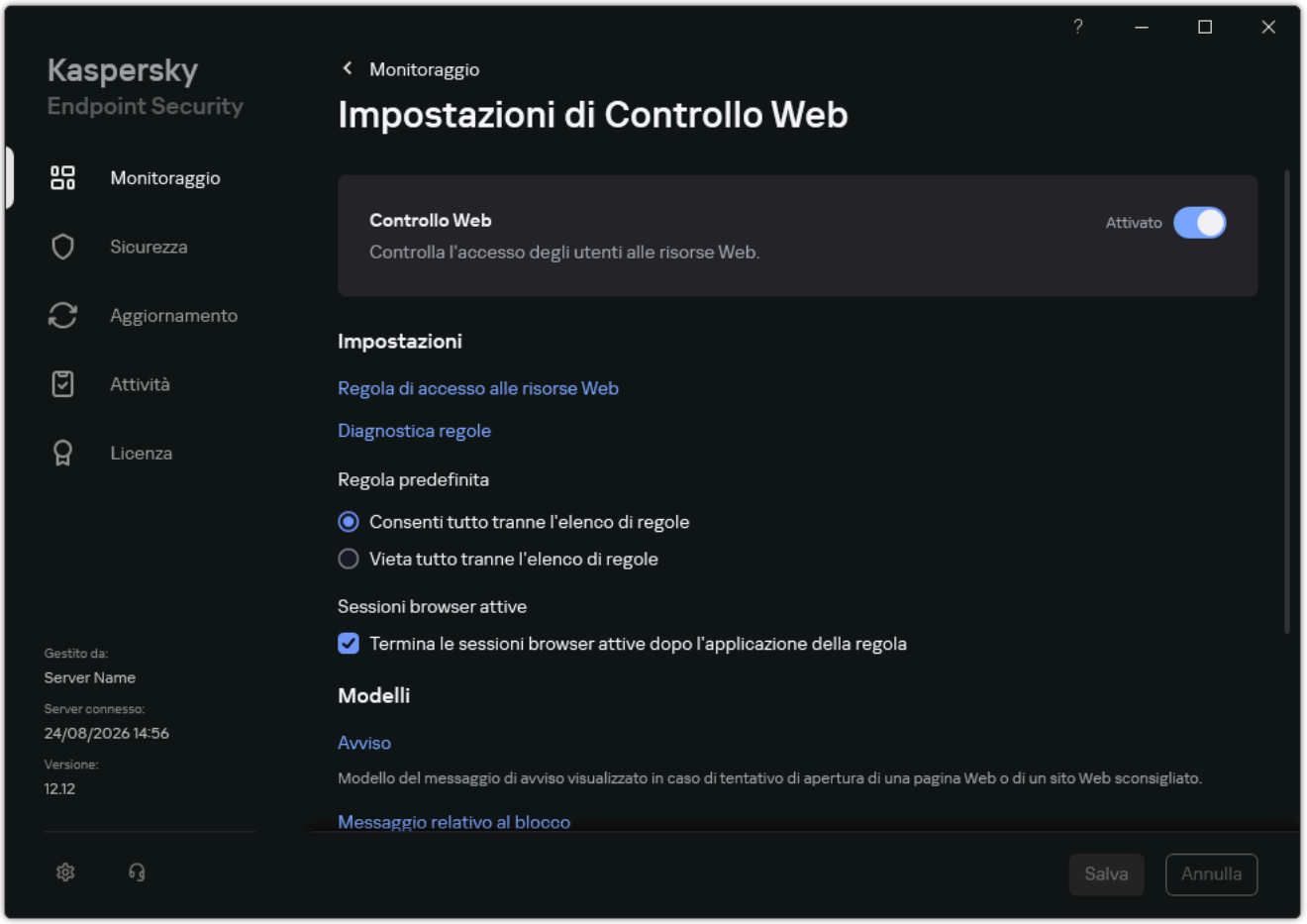
Quando si configura Controllo Web, è possibile che si blocchi inavvertitamente l'accesso alle risorse Web necessarie agli utenti per il proprio lavoro. Per scoprire quale regola di Controllo Web sta bloccando l'accesso alle risorse Web, è possibile utilizzare lo strumento di diagnostica *Regole di Controllo Web*. Lo strumento di diagnostica Regole di Controllo Web è disponibile solo nell'interfaccia di Kaspersky Endpoint Security. Nella console di Kaspersky Security Center, non è possibile scoprire quale regola di Controllo Web include una determinata risorsa.

Se l'utente ritiene che la risorsa Web sia stata bloccata per errore, può fare clic sul collegamento nel messaggio di notifica del blocco della risorsa Web per inviare un messaggio pre-generato all'amministratore della rete aziendale locale.

Per verificare le regole di accesso alle risorse Web:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo Web**.



Impostazioni di Controllo Web

3. Nella sezione **Impostazioni**, fare clic sul collegamento **Diagnostica regole**.

   Verrà visualizzata la finestra **Diagnostica regole**.

4. Se si desidera verificare le regole utilizzate da Kaspersky Endpoint Security per controllare l'accesso a una specifica risorsa Web, selezionare la casella di controllo **Specificare l'indirizzo**. Immettere l'indirizzo della risorsa Web nel campo sottostante.

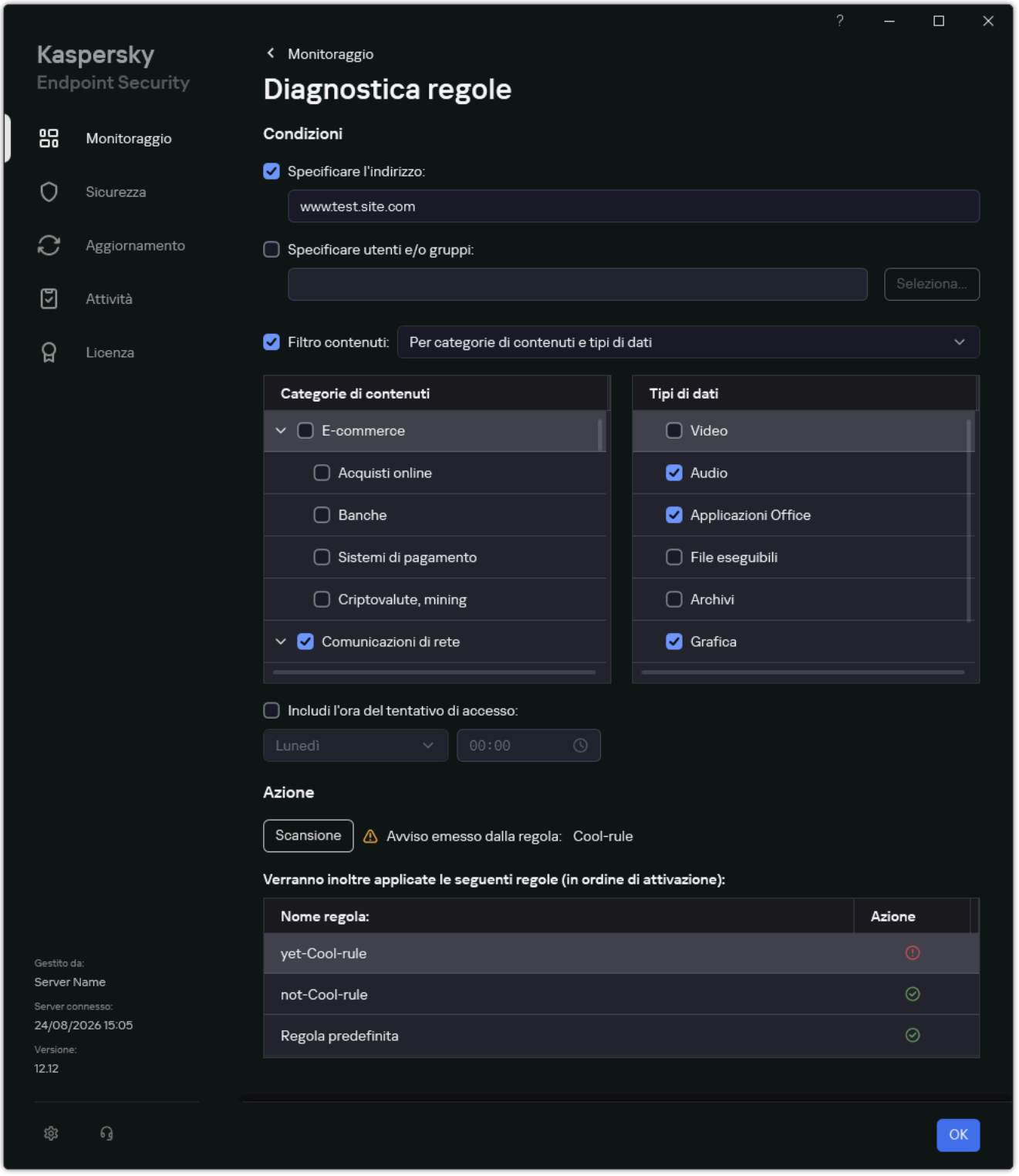
5. Se si desidera verificare le regole utilizzate da Kaspersky Endpoint Security per controllare l'accesso alle risorse Web per gli utenti e/o i gruppi di utenti specificati, specificare un elenco di utenti e/o gruppi di utenti.

6. Se si desidera verificare le regole utilizzate da Kaspersky Endpoint Security per controllare l'accesso alle risorse Web di alcune categorie di contenuti e/o categorie di tipi di dati, selezionare la casella di controllo **Filtro contenuti** e scegliere l'opzione desiderata nell'elenco a discesa (**Per categorie di contenuti**, **Per tipi di dati** o **Per categorie di contenuti e tipi di dati**).

7. Se si desidera verificare le regole tenendo conto dell'ora e del giorno della settimana del tentativo di accesso alla risorsa o alle risorse Web specificate nelle condizioni di diagnostica delle regole, selezionare la casella di controllo **Includi l'ora del tentativo di accesso**. Specificare quindi il giorno della settimana e l'ora.

8. Fare clic su **Scansione**.

Al termine della verifica, verrà visualizzato un messaggio con le informazioni sulle operazioni eseguite da Kaspersky Endpoint Security in base alla prima regola attivata durante il tentativo di accesso alla risorsa Web specificata (Consenti, Blocca o Avvisa). La prima regola che viene attivata è quella con una priorità superiore nell'elenco delle regole di Controllo Web rispetto alle altre regole che soddisfano le condizioni di diagnostica. Il messaggio è visualizzato a destra del pulsante **Scansione**. Nella seguente tabella sono elencate le regole attivate rimanenti, che specificano l'azione eseguita da Kaspersky Endpoint Security. Le regole sono elencate in ordine di priorità decrescente.



Esportazione e importazione delle regole di Controllo Web

È possibile esportare l'elenco delle regole di Controllo Web in un file XML o JSON. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di indirizzi dello stesso tipo. È possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco delle regole di Controllo Web o per eseguire la migrazione dell'elenco in un server diverso.

Come esportare e importare un elenco di regole di Controllo Web in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo Web**.
4. Per esportare l'elenco delle regole di Controllo Web:
   a. Selezionare le regole che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.
      Se non è stata selezionata alcuna regola, Kaspersky Endpoint Security esporterà tutte le regole.
   b. Fare clic sul collegamento **Esporta**.
   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle regole e selezionare la cartella in cui si desidera salvare il file.
   d. Salvare il file.
      Kaspersky Endpoint Security esporta l'intero elenco di regole nel file XML.
5. Per importare l'elenco delle regole di Controllo Web:
   a. Fare clic sul collegamento **Importa**.
      Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle regole.
   b. Aprire il file.
      Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.
6. Salvare le modifiche.

Come esportare e importare un elenco di regole di Controllo Web in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo Web**.

5. Per esportare l'elenco delle regole, nella sezione **Elenco di regole**:

   a. Selezionare le regole che si desidera esportare.

   b. Fare clic sul pulsante → **Esporta**.

      Kaspersky Endpoint Security esporta l'elenco delle regole in un file JSON nella cartella dei download predefinita.

6. Per importare l'elenco delle regole, nella sezione **Elenco di regole**:

   a. Fare clic sul pulsante → **Importa**.

      Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco delle regole.

   b. Aprire il file.

      Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

7. Salvare le modifiche.

Esportazione e importazione di indirizzi di risorse Web della regola di Controllo Web

Se è stato creato un elenco di indirizzi di risorse Web in una regola di accesso alle risorse Web, è possibile esportarlo in un file:

- In formato TXT in Administration Console (MMC)
- In formato JSON in Web Console
- In formato CSV nell'interfaccia dell'applicazione

È quindi possibile importare l'elenco da questo file per evitare di creare manualmente un nuovo elenco di indirizzi di risorse Web durante la configurazione di una regola di accesso. L'opzione per l'esportazione e l'importazione dell'elenco di indirizzi di risorse Web può essere ad esempio utile se si creano regole di accesso con parametri simili.

È inoltre possibile esportare/importare tutte le regole di Controllo Web e non solo gli indirizzi delle risorse Web di una singola regola.

Come esportare/importare gli indirizzi delle risorse Web della regola di Controllo Web in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo Web**.

5. Nel blocco **Impostazioni di Controllo Web**, selezionare la regola di cui si desidera importare o esportare l'elenco di indirizzi delle risorse Web.

   Vengono visualizzate le proprietà delle regole di Controllo Web.

6. Per esportare l'elenco delle risorse Web, eseguire le seguenti operazioni nell'elenco degli indirizzi:

   a. Selezionare gli indirizzi che si desidera esportare.

      Se non è stato selezionato alcun indirizzo, Kaspersky Endpoint Security esporterà tutti gli indirizzi.

   b. Fare clic sul pulsante .

   c. Nella finestra visualizzata, immettere il nome del file TXT in cui si desidera esportare l'elenco di indirizzi delle risorse Web e selezionare la cartella in cui si desidera salvare il file.

   d. Salvare il file.

      Kaspersky Endpoint Security esporta l'elenco di indirizzi di risorse Web in un file TXT.

7. Per importare l'elenco delle risorse Web, eseguire le seguenti operazioni nell'elenco degli indirizzi:

   a. Fare clic sul pulsante .

      Nella finestra visualizzata selezionare il file TXT da cui si desidera importare l'elenco delle risorse Web.

   b. Aprire il file.

      Se il computer dispone già di un elenco di indirizzi, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file TXT.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come esportare/importare gli indirizzi delle risorse Web della regola di Controllo Web in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza** → **Controllo Web**.

5. Nel blocco **Elenco di regole**, selezionare la regola di cui si desidera importare o esportare l'elenco di indirizzi delle risorse Web.

   Vengono visualizzate le proprietà delle regole di Controllo Web.

6. Nel blocco **Ambito** → **Siti Web individuali**, fare clic sul pulsante **Modifica**.

7. Per esportare l'elenco delle risorse Web, eseguire le seguenti operazioni nell'elenco degli indirizzi:

   a. Selezionare gli indirizzi che si desidera esportare.

   b. Fare clic sul pulsante → **Esporta**.

      Kaspersky Endpoint Security esporta l'elenco degli indirizzi delle risorse Web in un file JSON nella cartella dei download predefinita.

8. Per importare l'elenco delle risorse Web, eseguire le seguenti operazioni nell'elenco degli indirizzi:

   a. Fare clic sul pulsante → **Importa**.

      Nella finestra visualizzata, selezionare il file JSON da cui si desidera importare l'elenco degli indirizzi delle risorse Web.

   b. Aprire il file.

      Se il computer dispone già di un elenco di indirizzi, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

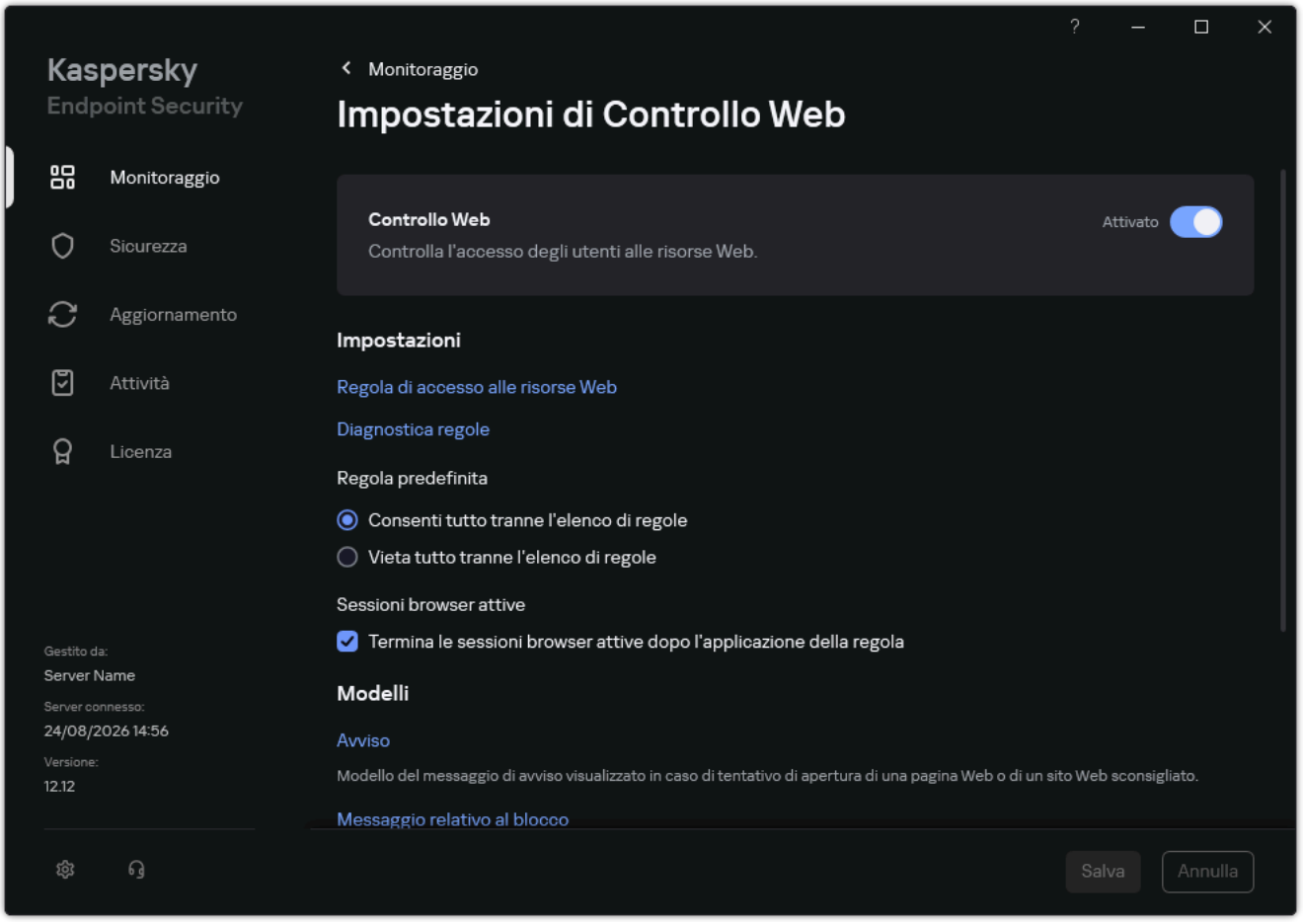
   È possibile esportare e importare gruppi di siti Web nello stesso modo.

9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come esportare/importare gli indirizzi delle risorse Web della regola di Controllo Web nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo Web**.



Impostazioni di Controllo Web

3. Nel blocco **Impostazioni**, fare clic sul pulsante **Regola di accesso alle risorse Web**.

4. Selezionare la regola di cui si desidera importare o esportare l'elenco di indirizzi delle risorse Web.

5. Per esportare l'elenco di indirizzi Web attendibili, eseguire le seguenti operazioni nella sezione **Indirizzi**:

   a. Selezionare gli indirizzi che si desidera esportare.

      Se non è stato selezionato alcun indirizzo, Kaspersky Endpoint Security esporterà tutti gli indirizzi.

   b. Fare clic su **Esporta**.

   c. Nella finestra visualizzata, immettere il nome del file CSV in cui si desidera esportare l'elenco di indirizzi delle risorse Web e selezionare la cartella in cui si desidera salvare il file.

   d. Salvare il file.

      Kaspersky Endpoint Security esporta l'elenco di indirizzi di risorse Web in un file CSV.

6. Per importare l'elenco delle risorse Web, eseguire le seguenti operazioni nella sezione **Indirizzi**:

   a. Fare clic su **Importa**.

      Nella finestra visualizzata selezionare il file CSV da cui si desidera importare l'elenco delle risorse Web.

   b. Aprire il file.

      Se il computer dispone già di un elenco di indirizzi, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file CSV.

7. Salvare le modifiche.

Monitoraggio dell'attività Internet dell'utente

Kaspersky Endpoint Security consente di registrare i dati sulle visite degli utenti a tutti i siti Web, inclusi i siti Web consentiti. Questo consente di ottenere la cronologia completa delle visualizzazioni del browser. Kaspersky Endpoint Security invia gli eventi sull'attività dell'utente a Kaspersky Security Center, al registro locale di Kaspersky Endpoint Security e al registro eventi di Windows. Per ricevere gli eventi in Kaspersky Security Center, è necessario configurare le impostazioni degli eventi in un criterio in Administration Console o Web Console. È inoltre possibile configurare la trasmissione degli eventi di Controllo Web tramite e-mail e la visualizzazione delle notifiche visualizzate nel computer dell'utente.

Browser che supportano la funzione di monitoraggio: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Il monitoraggio delle attività degli utenti non funziona in altri browser.

Kaspersky Endpoint Security crea i seguenti eventi sulle attività Internet degli utenti:

- Bloccare il sito Web (stato *Critico*).
- Visitare un sito Web non consigliato (stato *Avviso*).
- Visitare un sito Web consentito (stato *Informazioni*).

Prima di abilitare il monitoraggio dell'attività Internet dell'utente è necessario eseguire le seguenti operazioni:

- Inoculare lo script per l'interazione con le pagine Web nel traffico Web (vedere le istruzioni di seguito). Lo script consente la registrazione degli eventi di Controllo Web.
- Per il monitoraggio del traffico HTTPS è necessario abilitare la scansione delle connessioni criptate.

Inoculazione di uno script di interazione con la pagina Web

Come inoculare uno script di interazione con la pagina Web nel traffico Web in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni di rete**.
4. Nella sezione **Scansione delle connessioni criptate** selezionare la casella di controllo **Inocula script nel traffico Web per interagire con le pagine Web**.
5. Salvare le modifiche.

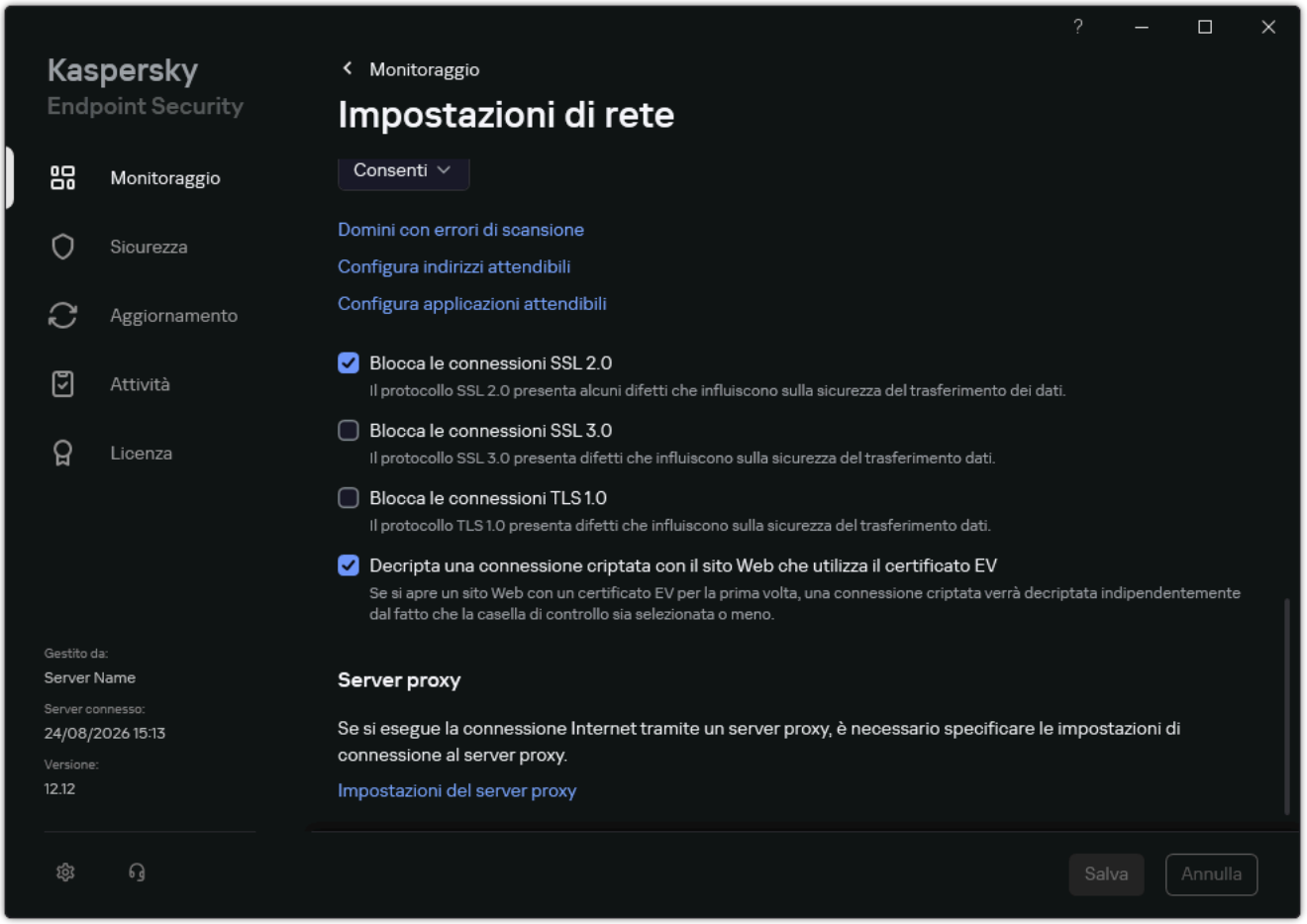
Come inoculare uno script di interazione con la pagina Web nel traffico Web in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni di rete**.
5. In **Monitoraggio delle connessioni Internet**, attivare l'interruttore **Monitoraggio delle connessioni Internet ABILITATO**.
6. Salvare le modifiche.

Come inoculare uno script di interazione con la pagina Web nel traffico Web nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.



Impostazioni della rete delle applicazioni

3. Nella sezione **Elaborazione del traffico** selezionare la casella di controllo **Inocula script nel traffico Web per interagire con le pagine Web**.
4. Salvare le modifiche.

Di conseguenza, Kaspersky Endpoint Security inoculerà uno script per l'interazione con le pagine Web nel traffico Web. Questo script consente la registrazione degli eventi di Controllo Web per il registro eventi dell'applicazione, il registro eventi del sistema operativo e i rapporti.

Configurazione della registrazione degli eventi di Controllo Web

Per configurare la registrazione degli eventi di Controllo Web nel computer dell'utente:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Interfaccia**.
3. Nel blocco **Notifiche**, fare clic sul pulsante **Configura notifiche**.

4. Nella finestra visualizzata, selezionare la sezione **Controllo Web**.

   Viene aperta la tabella con gli eventi di Controllo Web e i metodi di notifica.

5. Configurare il metodo di notifica per ogni evento: **Salva nel rapporto locale** o **Salva nel registro eventi di Windows**.

   Per registrare gli eventi sulle visite ai siti Web consentiti è inoltre necessario configurare Controllo Web (vedere le istruzioni di seguito).

   Nella tabella degli eventi è inoltre possibile abilitare una notifica visualizzata e una notifica e-mail. Per inviare le notifiche tramite e-mail è necessario configurare le impostazioni del server SMTP. Per informazioni dettagliate sull'invio delle notifiche tramite e-mail, consultare la Guida di Kaspersky Security Center.

6. Salvare le modifiche.

Di conseguenza, Kaspersky Endpoint Security inizia a registrare gli eventi sulle attività Internet degli utenti.

Controllo Web invia eventi sulle attività degli utenti a Kaspersky Security Center come segue:

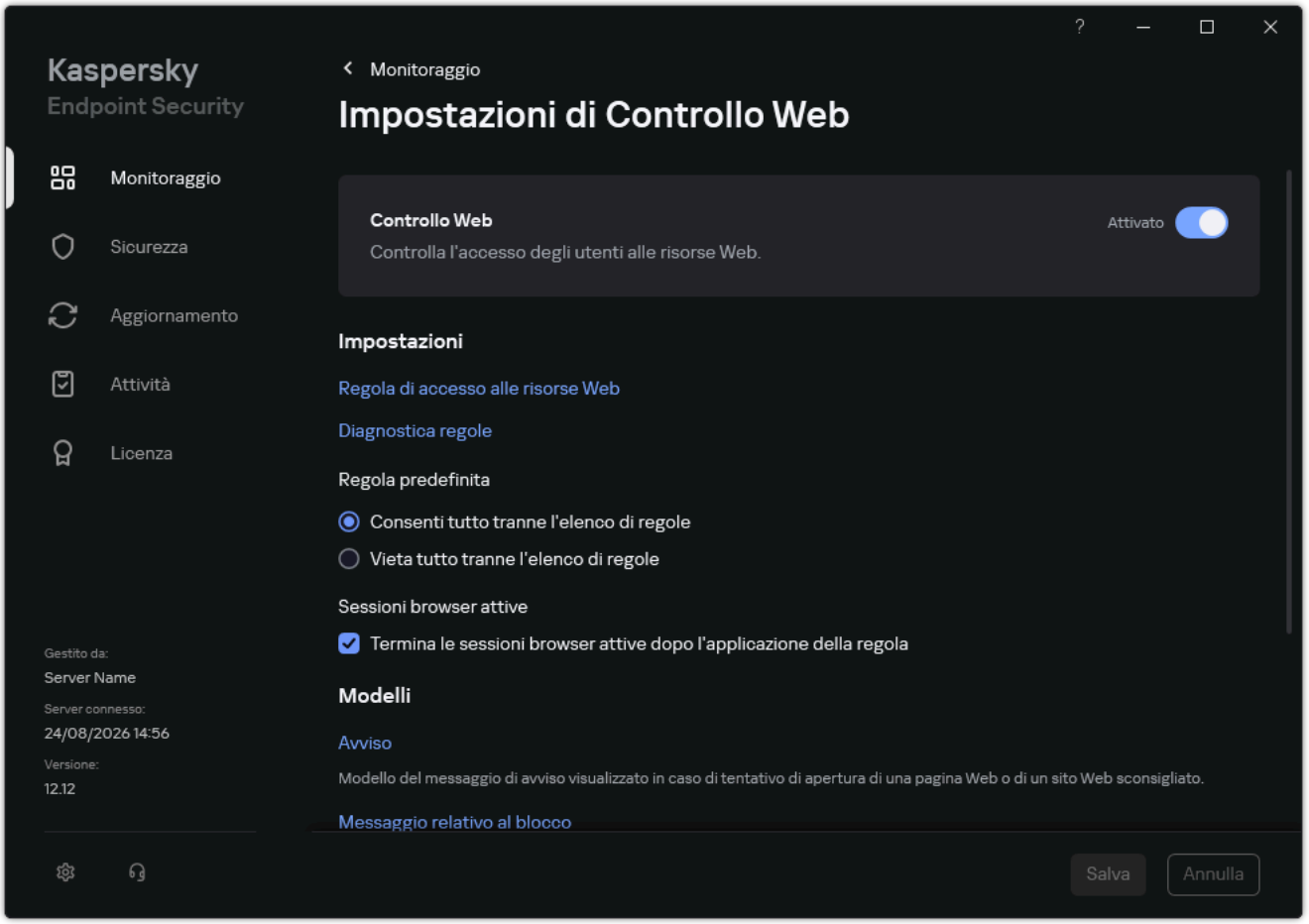
- Se si utilizza Kaspersky Security Center, Controllo Web invia eventi per tutti gli oggetti che compongono la pagina Web. Per questo motivo è possibile che vengano creati più eventi quando una pagina Web viene bloccata. Ad esempio, quando si blocca la pagina Web http://www.example.com, Kaspersky Endpoint Security può inviare gli eventi per i seguenti oggetti: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js, e così via.

- Se si utilizza Kaspersky Security Center Cloud Console, Controllo Web raggruppa gli eventi e invia solo il protocollo e il dominio del sito Web. Se ad esempio un utente visita le pagine Web non consigliate http://www.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, Kaspersky Endpoint Security invierà un solo evento con l'oggetto http://www.example.com.

Registrazione degli eventi quando si visitano i siti Web consentiti

Per abilitare la registrazione degli eventi quando si visitano i siti Web consentiti:

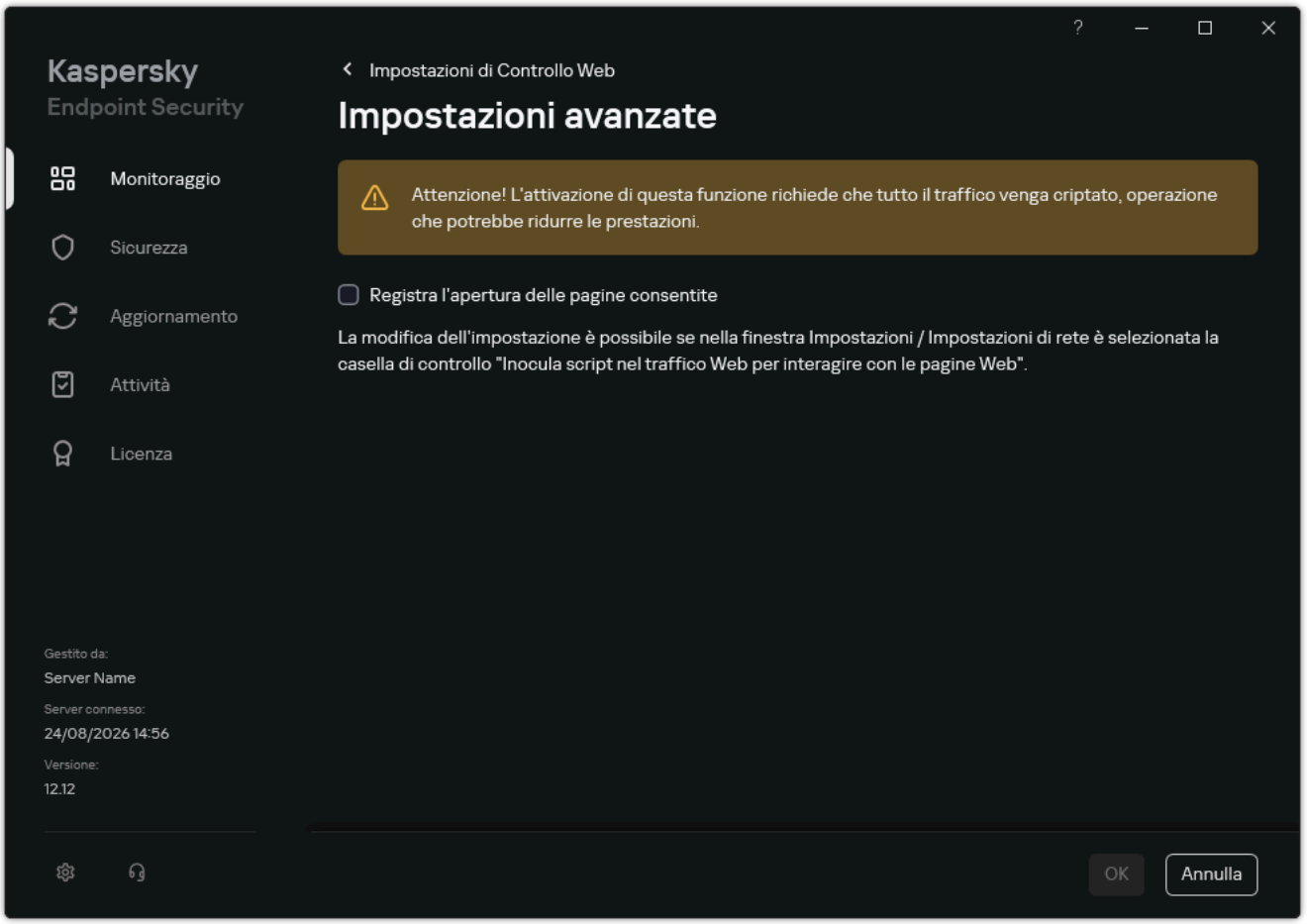
1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo Web**.



Impostazioni di Controllo Web

3. Nel blocco **Avanzate**, fare clic sul pulsante **Impostazioni avanzate**.

4. Nella finestra visualizzata, selezionare la casella di controllo **Registra l'apertura delle pagine consentite**.



Impostazioni avanzate di Controllo Web

5. Salvare le modifiche.

Di conseguenza l'utente sarà in grado di visualizzare la cronologia completa del browser.

Modifica dei modelli dei messaggi di Controllo Web

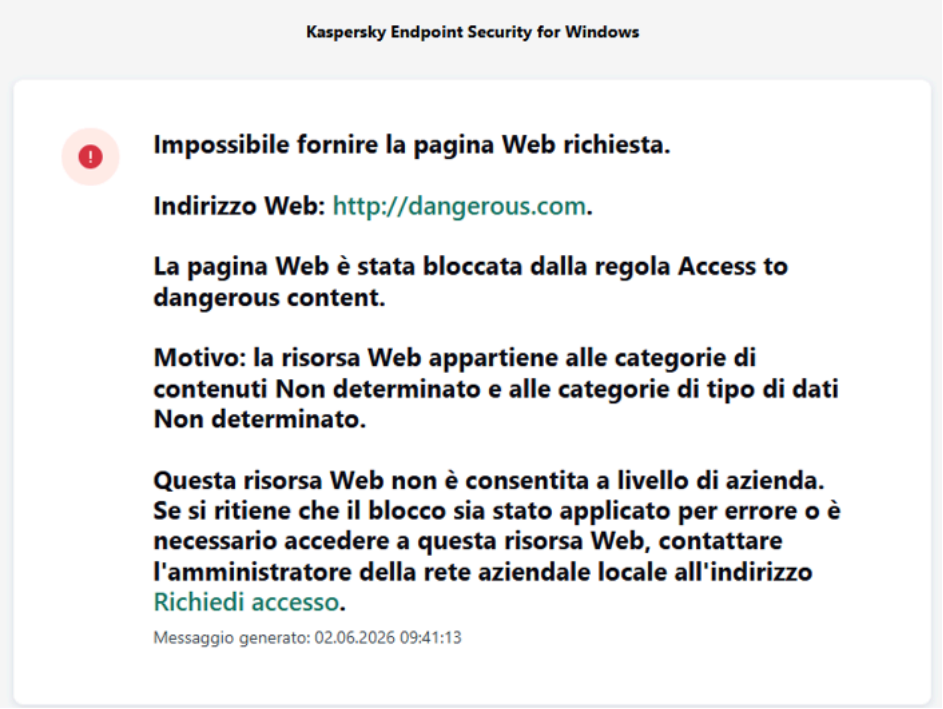
In base al tipo di azione specificata nelle proprietà delle regole di Controllo Web, Kaspersky Endpoint Security visualizza uno dei seguenti tipi di messaggio quando gli utenti tentano di accedere alle risorse Internet (l'applicazione sostituisce una pagina HTML con un messaggio per la risposta del server HTTP):

- Messaggio di avviso. Questo messaggio segnala all'utente che l'apertura della risorsa Web non è consigliata e/o viola i criteri di sicurezza aziendali. Kaspersky Endpoint Security mostra un messaggio di avviso se l'opzione **Avvisa** è selezionata nelle impostazioni della regola che descrive la risorsa Web.

  Se l'utente ritiene che l'avviso sia stato visualizzato per errore, può fare clic sul collegamento nell'avviso per inviare un messaggio pre-generato all'amministratore della rete aziendale locale.

- Messaggio informativo sul blocco di una risorsa Web. Kaspersky Endpoint Security mostra un messaggio che segnala che una risorsa Web è stata bloccata (vedere la figura riportata di seguito), se l'opzione **Blocca** è selezionata nelle impostazioni della regola che descrive la risorsa Web.

Se l'utente ritiene che la risorsa Web sia stata bloccata per errore, può fare clic sul collegamento nel messaggio di notifica del blocco della risorsa Web per inviare un messaggio pre-generato all'amministratore della rete aziendale locale.



Messaggio sul blocco delle risorse Web

Sono disponibili speciali modelli per il messaggio di avviso, il messaggio che segnala che una risorsa Web è stata bloccata e il messaggio inviato all'amministratore della rete LAN. Sono disponibili variabili speciali per la gestione del modello di messaggio (ad esempio `%USER_NAME%`). Le variabili consentono di utilizzare un unico modello di messaggio per computer diversi. Quando si genera un messaggio, Kaspersky Endpoint Security recupera il valore della variabile dalle impostazioni del sistema operativo e lo inserisce nel messaggio corrispondente al computer, all'utente e all'evento specifici.

Come modificare il modello di messaggio di Controllo Web in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo Web**.
4. Nel blocco **Impostazioni dei modelli di messaggio**, fare clic sul pulsante **Modelli**.

5. Configurare i modelli di messaggio di Controllo Web:

   - **Avviso**. Il campo di immissione contiene un modello del messaggio visualizzato se viene attivata una regola per la segnalazione dei tentativi di accesso a una risorsa Web indesiderata.

   - **Messaggio relativo al blocco**. Il campo di immissione contiene il modello del messaggio visualizzato se viene attivata una regola che blocca l'accesso a una risorsa Web.

   - **Messaggio all'amministratore**. Modello del messaggio da inviare all'amministratore della rete LAN se l'utente ritiene che il blocco sia stato applicato per errore. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'accesso a una pagina Web**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

   È anche possibile ripristinare il testo predefinito del modello utilizzando il pulsante **Predefinito**.

6. Salvare le modifiche.

Come modificare il modello di messaggio di Controllo Web in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza** → **Controllo Web**.

5. Nel blocco **Modelli di messaggi**, fare clic sul collegamento **Messaggio relativo al blocco dei siti Web** e configurare modelli per i messaggi di Controllo Web:

   - **Avviso**. Il campo di immissione contiene un modello del messaggio visualizzato se viene attivata una regola per la segnalazione dei tentativi di accesso a una risorsa Web indesiderata.

   - **Messaggio relativo al blocco**. Il campo di immissione contiene il modello del messaggio visualizzato se viene attivata una regola che blocca l'accesso a una risorsa Web.

   - **Messaggio all'amministratore**. Modello del messaggio da inviare all'amministratore della rete LAN se l'utente ritiene che il blocco sia stato applicato per errore. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'accesso a una pagina Web**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Aggiungi variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

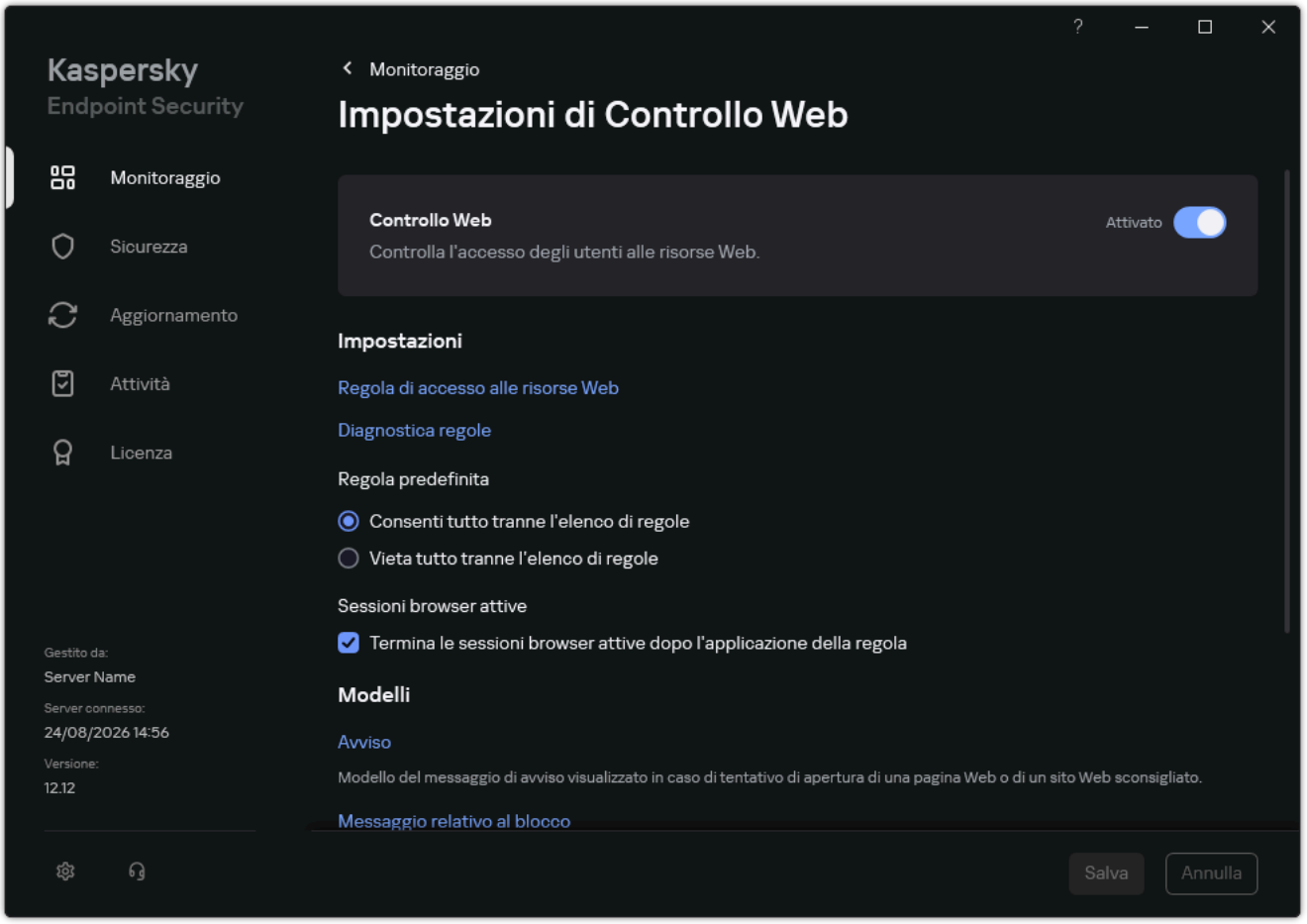
È anche possibile ripristinare il testo predefinito del modello utilizzando il pulsante **Ripristina condizioni originali**.

6. Salvare le modifiche.

Come modificare il modello di messaggio di Controllo Web nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo Web**.



Impostazioni di Controllo Web

3. Nel blocco **Modelli** configurare i modelli per i messaggi di Controllo Web:

   - **Avviso**. Il campo di immissione contiene un modello del messaggio visualizzato se viene attivata una regola per la segnalazione dei tentativi di accesso a una risorsa Web indesiderata.

   - **Messaggio relativo al blocco**. Il campo di immissione contiene il modello del messaggio visualizzato se viene attivata una regola che blocca l'accesso a una risorsa Web.

   - **Messaggio all'amministratore**. Modello del messaggio da inviare all'amministratore della rete LAN se l'utente ritiene che il blocco sia stato applicato per errore. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'accesso a una pagina Web**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Aggiungi variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

È anche possibile ripristinare il testo predefinito del modello utilizzando il pulsante **Reimposta**.

4. Salvare le modifiche.

Modifica delle maschere per gli indirizzi di risorse Web

L'utilizzo di una *maschera di indirizzi di risorse Web* (anche denominata "maschera di indirizzi") può essere utile se è necessario immettere numerosi indirizzi di risorse Web simili durante la creazione di una regola di accesso alle risorse Web. Se viene creata nel modo appropriato, una maschera di indirizzi può sostituire numerosi indirizzi di risorse Web.

Durante la creazione di una maschera di indirizzi, attenersi alle seguenti regole:

1. Il carattere `*` sostituisce qualsiasi sequenza di zero o più caratteri.

   Se ad esempio si immette una maschera di indirizzi `*abc*`, la regola di accesso viene applicata a tutte le risorse Web che contengono la sequenza `abc`. Esempio: `http://www.example.com/page_0-9abcdef.html`.

2. Una sequenza di caratteri `*.` (nota come *maschera di domini*) consente di selezionare tutti i domini di un indirizzo. La maschera di domini `*.` rappresenta qualsiasi nome di dominio, nome di sottodominio o riga vuota.

   Esempio: la maschera `*.example.com` rappresenta i seguenti indirizzi:

   - `http://pictures.example.com`. La maschera di domini `*.` rappresenta `pictures.`
   - `http://user.pictures.example.com`. La maschera di domini `*.` rappresenta `pictures.` e `user.`
   - `http://example.com`. La maschera di domini `*.` viene interpretato come una riga vuota.

3. La sequenza di caratteri `www.` all'inizio di una maschera di indirizzi viene interpretata come una sequenza `*.`.

   Esempio: la maschera di indirizzi `www.example.com` viene gestita come `*.example.com`. Questa maschera include gli indirizzi `www2.example.com` e `www.pictures.example.com`.

4. Se una maschera di indirizzi non inizia con il carattere `*`, il contenuto della maschera di indirizzi è equivalente allo stesso contenuto con il prefisso `*.`.

5. Se una maschera di indirizzi termina con un carattere diverso da `/` o `*`, il contenuto della maschera di indirizzi è equivalente allo stesso contenuto con il suffisso `/*`.

   Esempio: la maschera di indirizzi `http://www.example.com` include indirizzi come `http://www.example.com/abc`, dove `a`, `b`, e `c` possono essere qualsiasi carattere.

6. Se una maschera di indirizzi termina con il carattere `/`, il contenuto della maschera di indirizzi è equivalente allo stesso contenuto con il suffisso `/*`.

7. La sequenza di caratteri `/*` alla fine di una maschera di indirizzi viene interpretata come `/*` o come una stringa vuota.

8. Gli indirizzi delle risorse Web vengono verificati rispetto a una maschera di indirizzi, tenendo conto del protocollo (http o https):

   - Se la maschera di indirizzi non contiene alcun protocollo di rete, la maschera di indirizzi include gli indirizzi con qualsiasi protocollo di rete.

     Esempio: la maschera dell'indirizzo `example.com` copre gli indirizzi `http://example.com` e `https://example.com`.

- Se la maschera di indirizzi contiene un protocollo di rete, la maschera di indirizzi include solo gli indirizzi con il protocollo di rete specificato.

  Esempio: la maschera di indirizzi `http://*.example.com` include l'indirizzo `http://www.example.com`, ma non l'indirizzo `https://www.example.com`.

9. Una maschera di indirizzi tra virgolette viene trattata senza considerare alcuna sostituzione aggiuntiva, tranne il carattere `*` se è stato inizialmente incluso nella maschera di indirizzi. Le regole 5 e 7 non si applicano alle maschere di indirizzi racchiuse tra virgolette doppie (vedi gli esempi 14 - 18 nella tabella seguente).

10. Il nome utente e la password, la porta di connessione e la distinzione tra caratteri maiuscoli e minuscoli non vengono presi in considerazione durante il confronto con la maschera di indirizzi di una risorsa Web.

Esempi di utilizzo di regole per la creazione di maschere di indirizzi

N.	Maschera di indirizzo	Indirizzo della risorsa Web da verificare	L'indirizzo è incluso nella maschera di indirizzi?	Commento
1	*.example.com	http://www.123example.com	No	Vedere la regola 1.
2	*.example.com	http://www.123.example.com	Sì	Vedere la regola 2.
3	*example.com	http://www.123example.com	Sì	Vedere la regola 1.
4	*example.com	http://www.123.example.com	Sì	Vedere la regola 1.
5	http://www.*.example.com	http://www.123example.com	No	Vedere la regola 1.
6	www.example.com	http://www.example.com	Sì	Vedere le regole 3, 2, 1.
7	www.example.com	https://www.example.com	Sì	Vedere le regole 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Sì	Vedere le regole 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Sì	Vedere le regole 3, 5, 1.
10	example.com	http://www.example.com	Sì	Vedere le regole 3, 1.
11	http://example.com/	http://example.com/abc	Sì	Vedere la regola 6.
12	http://example.com/*	http://example.com	Sì	Vedere la regola 7.
13	http://example.com	https://example.com	No	Vedere la regola 8.
14	"example.com"	http://www.example.com	No	Vedere la regola 9.
15	"http://www.example.com"	http://www.example.com/abc	No	Vedere la regola 9.
16	"*.example.com"	http://www.example.com	Sì	Vedere le regole 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Sì	Vedere le regole 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Sì	Vedere le regole 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	No	Una maschera di indirizzo contiene più informazioni rispetto all'indirizzo di una risorsa Web.

Controllo Web per macchine virtuali

Controllo Web controlla il traffico nel computer e in una macchina virtuale distribuita in locale nel computer. Funziona senza necessità di installare l'applicazione Kaspersky Endpoint Security nella macchina virtuale locale. Questo significa che se l'utente tenta di aprire un sito Web bloccato da una regola di Controllo Web in un browser sulla *macchina virtuale*, l'applicazione installata nel sistema operativo host del *computer* nega l'accesso a tale sito Web.

Controllo Web funziona in modo diverso in diverse macchine virtuali.

Oracle VM VirtualBox

Kaspersky Endpoint Security supporta le regole di Controllo Web nelle macchine virtuali Oracle VM VirtualBox senza limitazioni. L'applicazione può controllare tutto il traffico della macchina virtuale. Se è configurato un filtro per utente nelle regole di Controllo Web, l'applicazione funziona correttamente poiché tutti i processi delle macchine virtuali vengono avviati dall'utente locale.

VMware Workstation

Kaspersky Endpoint Security supporta le regole di Controllo Web nelle macchine virtuali VMware Workstation con limitazioni. L'applicazione non supporta le regole con un filtro per utente configurato. I processi della macchina virtuale sono in esecuzione con l'utente di sistema (SYSTEM). Questo rende impossibile identificare l'utente che sta tentando di aprire il sito Web nella macchina virtuale.

Microsoft Hyper-V

Kaspersky Endpoint Security non supporta le regole di Controllo Web nelle macchine virtuali Microsoft Hyper-V.

Variabili nei modelli di messaggi di Controllo Web

È possibile utilizzare le seguenti variabili nei modelli di messaggi dell'utente o nei modelli di messaggi dell'amministratore:

- **Nome utente** - `%USER_NAME%`.

  Nome dell'account utente corrente nel computer in cui è stato generato il messaggio, nel formato `<device name>\<user alias>` (ad esempio, `DESKTOP-123\John.Smith`).

- **Indirizzo risorsa Web** - `%CANONIC_REQUEST_URL%`.

  Indirizzo della risorsa Web bloccata.

- **Nome regola** - `%RULE%`.

  Nome della regola che ha bloccato la risorsa Web.

- **E-mail per l'invio di un messaggio** - `%COMPLAIN_EMAIL%`.

  Indirizzo e-mail per il feedback sui blocchi di risorse Web. Facendo clic sull'indirizzo e-mail, si apre una finestra in cui l'utente può scrivere un messaggio per l'amministratore.

- **Nome categoria di contenuti** - `%CONTENT_CATEGORY_LIST%`.

  Categoria di siti Web a cui appartiene la risorsa bloccata (ad esempio, *Sistemi di pagamento*).

- **Nome categoria di tipi di dati** - `%TYPE_CATEGORY_LIST%`.

  Categoria di tipo di dati nella risorsa Web bloccata (ad esempio, *Grafica*).

- **Collegamento alla risorsa Web richiesta** - `%CONTINUE_PAGE%`.

  Collegamento alla pagina Web richiesta (ad esempio, `http://www.example.com/pagename.html`).

- **Collegamento al sito Web** - `%CONTINUE_SITE%`.

  Collegamento al sito Web che contiene la pagina Web richiesta (ad esempio, `http://www.example.com/`).

- **Collegamento per l'accesso ai domini** - `%CONTINUE_DOMAIN%`.

  Collegamento su cui è possibile fare clic per ottenere l'accesso a tutte le pagine Web esistenti del nome di dominio. Ad esempio, se l'indirizzo della pagina Web bloccata è `http://www.example.com`, la variabile `%CONTINUE_DOMAIN%` viene sostituita con il collegamento `http://*.example.com`. Facendo clic su questo collegamento, è possibile accedere a tutti gli indirizzi Web del nome di dominio di base `http://www.example.com/` inclusi i sottodomini, ad esempio `http://start.example.com/*` o `http://domain.domain.example.com/*`, dove il carattere `*` rappresenta qualsiasi sequenza di caratteri (inclusa una stringa vuota).

Controllo dispositivi

Controllo dispositivi consente di gestire l'accesso dell'utente ai dispositivi installati nel computer o connessi al computer (ad esempio dischi rigidi, fotocamere o moduli Wi-Fi). In questo modo è possibile proteggere il computer dalle infezioni quando tali dispositivi sono connessi e prevenire perdite o fughe di dati.

Se Controllo dispositivi è abilitato, l'applicazione inoltra le informazioni sui dispositivi connessi a Kaspersky Security Center. È possibile visualizzare l'elenco dei dispositivi connessi in Kaspersky Security Center nella cartella **Avanzate** → **Archivi** → **Hardware**.

Livelli di accesso ai dispositivi

Controllo dispositivi controlla l'accesso ai seguenti livelli:

- **Tipo di dispositivo**. Ad esempio stampanti, unità rimovibili e unità CD/DVD.

  È possibile configurare l'accesso ai dispositivi nel modo seguente:

  - Consenti – .
  - Blocca – .
  - In base alle regole (solo stampanti e dispositivi portatili) – .
  - Dipende dal bus di connessione (eccetto Wi-Fi) – .
  - Blocca con eccezioni (Solo Wi-Fi) – .

- **Bus di connessione**. Un *bus di connessione* è un'interfaccia utilizzata per la connessione dei dispositivi al computer (ad esempio, USB o FireWire). Se la modalità **Dipende dal bus di connessione** è selezionata per il tipo di dispositivo, l'applicazione consente o nega l'accesso al dispositivo a seconda dell'interfaccia di connessione (ad esempio, USB).

È possibile configurare l'accesso ai dispositivi nel modo seguente:

- Consenti – ✓.
- Blocca – ⊘.

- **Dispositivi attendibili**. I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile.

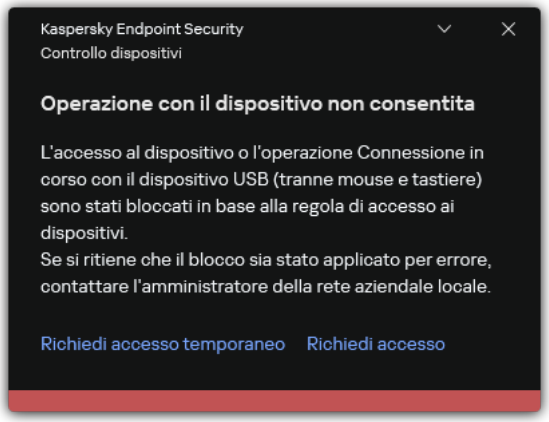
  È possibile aggiungere dispositivi attendibili in base ai seguenti dati:

  - **Dispositivi per ID**. Ogni dispositivo ha un identificatore univoco (Hardware ID o HWID). È possibile visualizzare l'ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. Esempio di ID dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. L'aggiunta di dispositivi in base all'ID è utile se si desidera aggiungere più dispositivi specifici.
  - **Dispositivi per modello**. Ogni dispositivo ha un Vendor ID (VID) e un Product ID (PID). È possibile visualizzare gli ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. Modello per l'immissione di VID e PID: `VID_1234&PID_5678`. L'aggiunta di dispositivi in base al modello è utile se si utilizzano dispositivi di un determinato modello nell'organizzazione. In tal modo è possibile aggiungere tutti i dispositivi di questo modello.
  - **Dispositivi per maschera ID**. Se si utilizzano più dispositivi con ID simili, è possibile aggiungere dispositivi all'elenco dei dispositivi attendibili utilizzando le maschere. Il carattere `*` sostituisce qualsiasi set di caratteri. Kaspersky Endpoint Security non supporta il carattere `?` quando si immette una maschera. Ad esempio, `WDC_C*`.
  - **Dispositivi per maschera del modello**. Se si utilizzano più dispositivi con VID o PID simili, ad esempio dispositivi dello stesso produttore, è possibile aggiungere dispositivi all'elenco dei dispositivi attendibili utilizzando le maschere. Il carattere `*` sostituisce qualsiasi set di caratteri. Kaspersky Endpoint Security non supporta il carattere `?` quando si immette una maschera. Ad esempio, `VID_05AC&PID_*`.

Controllo dispositivi regola l'accesso dell'utente ai dispositivi utilizzando le *regole di accesso*. Controllo dispositivi consente inoltre di salvare gli eventi di connessione/disconnessione dei dispositivi. Per salvare gli eventi, è necessario configurare la registrazione degli eventi in un criterio.

Se l'accesso a un dispositivo dipende dal bus di connessione (stato ◔), Kaspersky Endpoint Security non salva gli eventi di connessione/disconnessione del dispositivo. Per consentire a Kaspersky Endpoint Security di salvare gli eventi di connessione/disconnessione del dispositivo, consentire l'accesso al tipo di dispositivo corrispondente (stato ✓) o aggiungere il dispositivo all'elenco degli oggetti attendibili.

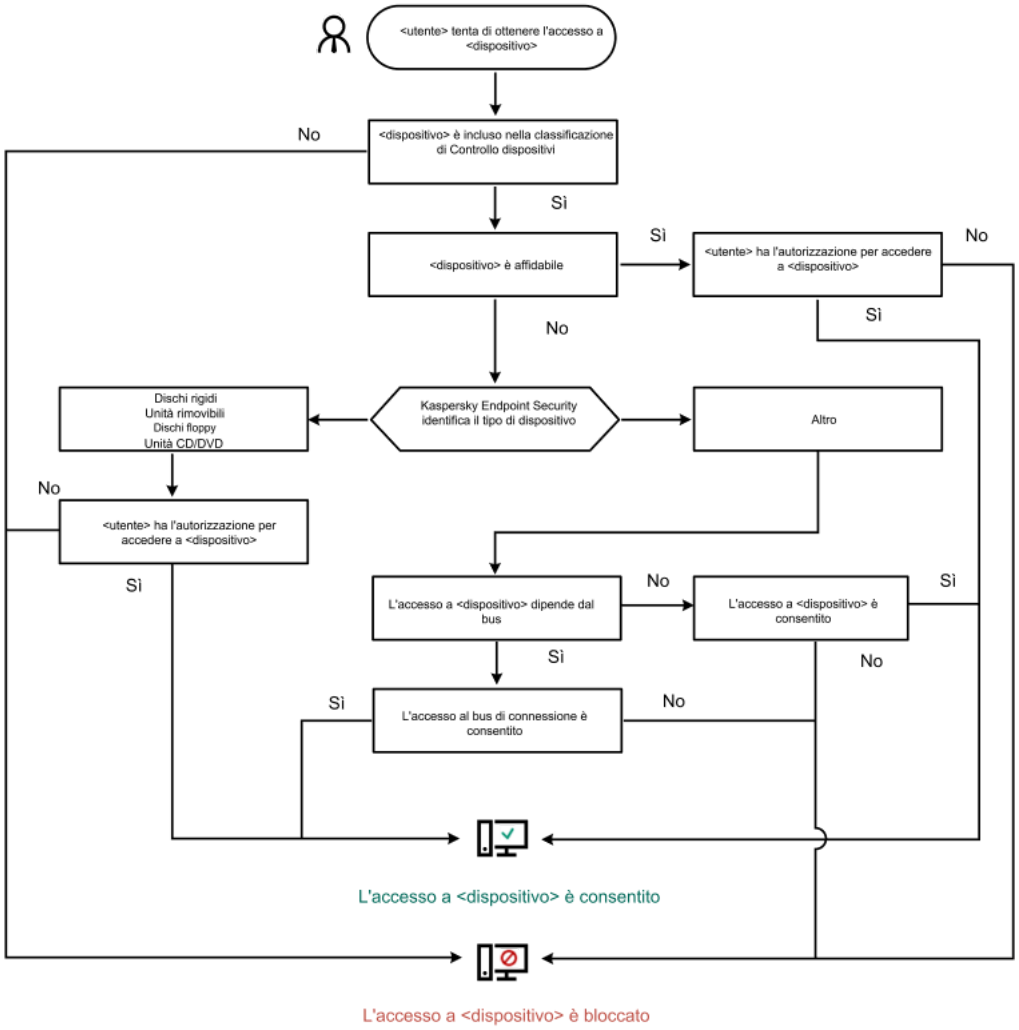
Quando un dispositivo bloccato da Controllo dispositivi viene connesso al computer, Kaspersky Endpoint Security bloccherà l'accesso e mostrerà una notifica (vedere la figura seguente).



Notifica Controllo dispositivi

Algoritmo operativo di Controllo dispositivi

Kaspersky Endpoint Security stabilisce se consentire l'accesso a un dispositivo dopo che l'utente connette il dispositivo al computer (vedere la figura di seguito).



Algoritmo operativo di Controllo dispositivi

Se un dispositivo è connesso e l'accesso è consentito, è possibile modificare la regola di accesso e bloccare l'accesso. In tal caso, la volta successiva che qualcuno tenta di accedere al dispositivo (ad esempio per visualizzare la struttura delle cartelle o eseguire operazioni di lettura o scrittura), Kaspersky Endpoint Security blocca l'accesso. Un dispositivo privo di file system viene bloccato solo alla connessione successiva.

Se un utente del computer in cui è installato Kaspersky Endpoint Security deve richiedere l'accesso a un dispositivo che ritiene sia stato bloccato per errore, inviare all'utente le istruzioni per la richiesta di accesso.

Informazioni sulle regole di accesso

Una *regola di accesso ai dispositivi* consiste in un gruppo di impostazioni che determinano il modo in cui gli utenti possono accedere ai dispositivi installati nel computer o connessi al computer. Queste impostazioni includono l'accesso a un dispositivo specifico, una pianificazione di accesso e le autorizzazioni di lettura o scrittura. Non è possibile aggiungere un dispositivo che non rientra nella classificazione Controllo dispositivi. L'accesso a tali dispositivi è consentito per tutti gli utenti.

Regole di accesso ai dispositivi

Il gruppo di impostazioni per una regola di accesso varia a seconda del tipo di dispositivo (vedere la tabella seguente).

Impostazioni delle regole di accesso

Dispositivi	Controllo dell'accesso	Pianificazione per l'accesso a un dispositivo	Assegnazione di utenti e/o gruppi di utenti	Priorità	Autorizzazione di lettura/scrittura
Dischi rigidi	✓	✓	✓	✓	✓
Unità rimovibili (comprese le unità flash USB)	✓	✓	✓	✓	✓
Dischi floppy	✓	✓	✓	✓	✓
Unità CD/DVD	✓	✓	✓	✓	✓
Dispositivi portatili (MTP)	✓	✓	✓	✓	✓
Stampanti locali	✓	–	✓	✓	–
Stampanti di rete	✓	–	✓	✓	–
Modem	✓	–	–	–	–
Dispositivi a nastro	✓	–	–	–	–
Dispositivi multifunzione	✓	–	–	–	–
Lettori di smart card	✓	–	–	–	–
Dispositivi ActiveSync USB Windows CE	✓	–	–	–	–
Schede di rete esterne	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Fotocamere e scanner	✓	–	–	–	–

Regole di accesso per le reti Wi-Fi

Una regola di accesso per le reti Wi-Fi determina se l'utilizzo delle reti Wi-Fi è consentito (stato) o vietato (stato). È possibile aggiungere una *rete Wi-Fi attendibile* (stato) a una regola. L'utilizzo di una rete Wi-Fi attendibile è consentito senza limitazioni. Per impostazione predefinita, una regola di accesso alle reti Wi-Fi consente l'accesso a qualsiasi rete Wi-Fi.

Regole di accesso ai bus di connessione

Se il valore **Dipende dal bus di connessione** è selezionato per la regola di accesso in base al tipo di dispositivo, l'applicazione consente o nega l'accesso al dispositivo a seconda dell'interfaccia di connessione. Per impostazione predefinita, vengono create regole che consentono l'accesso a tutti i bus di connessione presenti nella classificazione del componente Controllo dispositivi.

Le regole di accesso ai bus di connessione determinano se la connessione dei dispositivi è consentita (stato) o vietata (stato). La priorità delle regole di accesso del tipo di dispositivo è maggiore della priorità delle regole di accesso al bus di connessione.

Non è possibile bloccare tastiera e mouse con Controllo dispositivi. Se si vieta l'accesso al bus di connessione USB, l'utente continuerà a utilizzare una tastiera e un mouse collegati tramite USB. Il componente Prevenzione Attacchi BadUSB è progettato per impedire la connessione al computer di dispositivi USB infetti che imitano tastiere.

Recupero di informazioni sui dispositivi installati

Kaspersky Security Center riceve informazioni sui dispositivi installati dai seguenti provider: Network Agent e Kaspersky Endpoint Security. Le informazioni sui dispositivi installati sono necessarie per la gestione degli accessi e la creazione di un elenco di dispositivi attendibili.

Informazioni sull'hardware del computer

Se Network Agent è installato in un dispositivo Windows, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo:

- RAM
- dispositivi di archiviazione (inclusi i dischi rigidi)
- scheda madre
- CPU
- scheda di rete
- monitor

- GPU
- scheda audio

Network Agent fornisce queste informazioni a ogni sincronizzazione con Kaspersky Security Center. È possibile visualizzare l'hardware di un computer nelle proprietà del computer (**Registro hardware**).

Informazioni sull'hardware

Kaspersky Endpoint Security fornisce informazioni sull'hardware installato: stampanti, unità rimovibili, dispositivi portatili (MTP) e così via. Per ricevere informazioni sull'hardware, è necessario applicare un criterio attivo che abiliti la trasmissione delle informazioni sui dispositivi installati (questa trasmissione è abilitata per impostazione predefinita).

Come abilitare la trasmissione dei dati sui dispositivi installati nella Console di gestione (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Rapporti e archivi**.
5. Nel blocco **Trasferimento dei dati ad Administration Server**, fare clic sul pulsante **Impostazioni**.
6. Selezionare la casella di controllo **Dispositivi installati**.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare la trasmissione dei dati sui dispositivi installati nella Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Integrazione KSC**.
5. Nel blocco **Trasferimento dei dati ad Administration Server**, fare clic sul pulsante **Impostazioni avanzate**.
6. Selezionare la casella di controllo **Informazioni sui dispositivi installati**.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Di conseguenza, è possibile visualizzare l'elenco dei dispositivi installati nella console di Kaspersky Security Center (**Archivi** → **Hardware**).

Gestione dell'accesso ai dispositivi in base al tipo

Controllo dispositivi consente di gestire l'accesso ai dispositivi in base al tipo. Il tipo di dispositivo è determinato dal sistema operativo al momento della connessione. È possibile cercare il tipo di dispositivo utilizzando lo strumento Gestione dispositivi integrato nel sistema operativo. Per gestire l'accesso ai dispositivi, è necessario configurare le regole. Una *regola di accesso ai dispositivi* consiste in un gruppo di impostazioni che determinano il modo in cui gli utenti possono accedere ai dispositivi installati nel computer o connessi al computer. Queste impostazioni includono l'accesso a un dispositivo specifico, una pianificazione di accesso e le autorizzazioni di lettura o scrittura. Non è possibile aggiungere un dispositivo che non rientra nella classificazione Controllo dispositivi. L'accesso a tali dispositivi è consentito per tutti gli utenti.

Per impostazione predefinita, Controllo dispositivi consente l'accesso a tutti i dispositivi per tutti gli utenti.

È possibile configurare l'accesso ai dispositivi come segue:

- **Consenti**.

  Kaspersky Endpoint Security concede a tutti gli utenti l'accesso completo ai dispositivi.

- **Blocca**.

  Kaspersky Endpoint Security blocca le connessioni dei dispositivi. L'applicazione consente solo i dispositivi attendibili per la connessione.

- **Dipende dal bus di connessione**.

  Kaspersky Endpoint Security determina l'interfaccia di connessione dei dispositivi e limita l'accesso ai dispositivi in base allo stato della connessione al bus. L'applicazione consente inoltre la connessione di dispositivi attendibili.

- **In base alle regole**.

  Per alcuni tipi di dispositivi è possibile designare utenti singoli o un gruppo di utenti a cui è consentito utilizzare i dispositivi, impostare una pianificazione per l'accesso ai dispositivi e configurare autorizzazioni di lettura e scrittura. L'applicazione consente inoltre la connessione di dispositivi attendibili.

Prestare attenzione durante la configurazione dell'accesso ai dispositivi del tipo **Dischi rigidi**. Se si blocca l'accesso al disco di sistema, l'applicazione potrebbe causare un arresto anomalo (BSOD) all'avvio del sistema operativo.

Se un dispositivo non rientra nello schema di classificazione di Controllo dispositivi, l'accesso a tale dispositivo non può essere limitato.

Come gestire l'accesso ai dispositivi in base al tipo in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.

5. In **Impostazioni di Controllo dispositivi**, selezionare la scheda **Tipi di dispositivi**.

   La scheda **Tipi di dispositivi** mostra le regole di accesso per tutti i dispositivi inclusi nella classificazione di Controllo dispositivi.

6. Configurare le regole di accesso per i dispositivi:

   a. Selezionare la modalità di accesso: **Consenti**, **Blocca**, **Dipende dal bus di connessione**, **In base alle regole**.

      Per selezionare la modalità di accesso **In base alle regole**, è necessario fare doppio clic per aprire le proprietà della regola di accesso.

   b. Se si seleziona la modalità di accesso **Dipende dal bus di connessione**, è necessario configurare le regole di accesso per le interfacce di connessione nella scheda **Bus di connessione**.

   c. Nel caso dei dispositivi di archiviazione (ad esempio, supporti rimovibili), è possibile configurare le autorizzazioni di accesso per i singoli utenti. È inoltre possibile impostare una pianificazione per l'accesso ai dispositivi e configurare le autorizzazioni di lettura e scrittura.

      È possibile aggiungere i dispositivi all'elenco di attendibilità. I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile.

   d. Se necessario, configurare le regole di stampa.

   e. Se necessario, configurare le regole di accesso ai dispositivi Bluetooth.

   f. Se necessario, configurare le regole di connessione Wi-Fi del computer.

7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come gestire l'accesso ai dispositivi in base al tipo in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza** → **Controllo dispositivi**.

5. In **Regole di accesso ai dispositivi**, selezionare la scheda **Dispositivi e reti Wi-Fi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.

6. Configurare le regole di accesso per i dispositivi:

   a. Selezionare la modalità di accesso: **Consenti**, **Blocca**, **Dipende dal bus**, **Personalizzato**.

      Se la modalità di accesso non è presente nel menu a discesa, aprire le proprietà della regola di accesso facendo doppio clic sul tipo di dispositivo.

   b. Se si seleziona la modalità di accesso **Dipende dal bus**, è necessario configurare le regole di accesso per le interfacce di connessione nella scheda **Bus di connessione**.

c. Nel caso dei dispositivi di archiviazione (ad esempio, supporti rimovibili), è possibile configurare le autorizzazioni di accesso per i singoli utenti. È inoltre possibile impostare una pianificazione per l'accesso ai dispositivi e configurare le autorizzazioni di lettura e scrittura.

È possibile aggiungere i dispositivi all'elenco di attendibilità. I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile.

d. Se necessario, configurare le regole di stampa.

e. Se necessario, configurare le regole di accesso ai dispositivi Bluetooth.

f. Se necessario, configurare le regole di connessione Wi-Fi del computer.

7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come gestire l'accesso ai dispositivi nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nella sezione **Impostazioni di accesso**, fare clic sul collegamento **Dispositivi e reti Wi-Fi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.
4. Configurare le regole di accesso per i dispositivi:

   a. Selezionare la modalità di accesso: **Consenti**, **Blocca**, **Dipende dal bus di connessione**, **In base alle regole**.

   Se la modalità di accesso non è presente nel menu a discesa, aprire le proprietà della regola di accesso facendo doppio clic sul tipo di dispositivo.

   b. Se si seleziona la modalità di accesso **Dipende dal bus di connessione**, è necessario configurare le regole di accesso per le interfacce di connessione nella scheda **Bus di connessione**.

   c. Nel caso dei dispositivi di archiviazione (ad esempio, supporti rimovibili), è possibile configurare le autorizzazioni di accesso per i singoli utenti. È inoltre possibile impostare una pianificazione per l'accesso ai dispositivi e configurare le autorizzazioni di lettura e scrittura.

   È possibile aggiungere i dispositivi all'elenco di attendibilità. I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile.

   d. Se necessario, configurare le regole di stampa.

   e. Se necessario, configurare le regole di accesso ai dispositivi Bluetooth.

   f. Se necessario, configurare le regole di connessione Wi-Fi del computer.
5. Salvare le modifiche.

Di conseguenza, quando un utente tenta di ottenere l'accesso a un dispositivo, l'applicazione blocca l'accesso in base alle regole. Kaspersky Endpoint Security registra anche un evento corrispondente. Se si desidera concedere l'accesso a singoli dispositivi, è possibile aggiungere questi dispositivi all'elenco dei dispositivi attendibili.

Gestione dell'accesso ai dispositivi tramite il bus di connessione

Per modificare una regola di accesso ai bus di connessione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Bus di connessione**.

   La finestra visualizzata mostra le regole di accesso per tutti i bus di connessione inclusi nella classificazione del componente Controllo dispositivi.
4. Selezionare la regola di accesso che si desidera modificare.
5. Nella colonna **Accesso**, selezionare se consentire o meno l'accesso al bus di connessione: **Consenti** o **Blocca**.

   Se è stato modificato l'accesso al bus di connessione **Porta seriale** (COM) o **Porta parallela** (LPT), è necessario riavviare il computer per attivare la regola di accesso.
6. Salvare le modifiche.

Differenziazione dei diritti di accesso degli utenti ai dispositivi

È possibile configurare i diritti di accesso degli utenti in base al tipo di dispositivo o per i dispositivi attendibili.

Differenziazione dei diritti di accesso degli utenti in base al tipo di dispositivo

Controllo dispositivi consente di configurare i diritti di accesso degli utenti ai dati nei *dispositivi di archiviazione*. Per tali dispositivi è possibile configurare le autorizzazioni di scrittura e lettura. Controllo dispositivi supporta i seguenti tipi di *dispositivi di archiviazione*:

- Dischi rigidi
- Unità rimovibili (comprese le unità flash USB)
- Dischi floppy
- Unità CD/DVD
- Dispositivi portatili (MTP) I dispositivi portatili (MTP) includono, ad esempio, dispositivi mobili, macchine fotografiche, lettori multimediali e così via.

In questo modo, è ad esempio possibile consentire l'utilizzo di un supporto rimovibile solo al gruppo di amministratori. Per gli altri tipi di dispositivi, è possibile negare o consentire l'accesso a tutti gli utenti. È anche possibile configurare i diritti di accesso degli utenti per l'utilizzo delle stampanti.

Come configurare i diritti di accesso degli utenti ai dati nei dispositivi di archiviazione in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
5. In **Impostazioni di Controllo dispositivi**, selezionare la scheda **Tipi di dispositivi**.

   La scheda **Tipi di dispositivi** mostra le regole di accesso per tutti i dispositivi inclusi nella classificazione di Controllo dispositivi.
6. Per configurare le regole di accesso ai dispositivi di archiviazione, fare doppio clic per aprire l'elenco delle regole.
7. Configurare la regola di accesso ai dispositivi di archiviazione:

   a. Nel blocco **Regole di accesso**, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata una finestra per l'aggiunta di una nuova regola di accesso ai dispositivi di archiviazione.

   b. Nel campo **Priorità della regola**, impostare la priorità di *scrittura della regola*. Una regola include i seguenti attributi: account utente, pianificazione, autorizzazioni (lettura/scrittura) e priorità.

   Una regola ha una priorità specifica. Se un utente è stato aggiunto a più gruppi, Kaspersky Endpoint Security regola l'accesso al dispositivo in base alla regola con la priorità più elevata. Kaspersky Endpoint Security consente di assegnare la priorità da 0 a 10.000. Più alto è il valore, maggiore sarà la priorità. In altre parole, una voce con il valore 0 ha la priorità più bassa.

   È ad esempio possibile concedere autorizzazioni di sola lettura al gruppo Tutti e concedere autorizzazioni di lettura/scrittura al gruppo degli amministratori. A tale scopo, assegnare la priorità 1 per il gruppo degli amministratori e assegnare la priorità 0 per il gruppo Tutti.

   La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. In altre parole, se un utente è stato aggiunto a più gruppi e la priorità di tutte le regole è la stessa, Kaspersky Endpoint Security regola l'accesso al dispositivo in base a qualsiasi regola di blocco esistente.

   c. In **Regola per utenti e gruppi**, selezionare gli utenti o i gruppi di utenti. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

   d. Fare clic su **OK**.
8. In **Pianificazioni per la regola di accesso selezionata**, configurare una pianificazione di accesso ai dispositivi di archiviazione per gli utenti.

   È ad esempio possibile consentire agli utenti di utilizzare i dispositivi di archiviazione solo durante l'orario di lavoro.
9. Configurare le autorizzazioni di accesso degli utenti ai dispositivi di archiviazione nel programma per la gestione dei file (**Lettura**/**Scrittura**).
10. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare i diritti di accesso degli utenti ai dati nei dispositivi di archiviazione in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo dispositivi**.
5. Nel blocco **Regole di accesso ai dispositivi**, nella tabella delle regole di accesso, aprire le proprietà delle regole di accesso per i dispositivi di archiviazione.
6. Nel blocco **Regole di accesso ai dispositivi**, selezionare **Personalizzato**.
7. Configurare la regola di accesso ai dispositivi di archiviazione:

   a. Nel blocco **Utenti e relativi diritti**, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata una finestra per l'aggiunta di una nuova regola di accesso ai dispositivi di archiviazione.

   b. Nel campo **Priorità**, impostare la priorità di *scrittura della regola*. Una regola include i seguenti attributi: account utente, pianificazione, autorizzazioni (lettura/scrittura) e priorità.

   Una regola ha una priorità specifica. Se un utente è stato aggiunto a più gruppi, Kaspersky Endpoint Security regola l'accesso al dispositivo in base alla regola con la priorità più elevata. Kaspersky Endpoint Security consente di assegnare la priorità da 0 a 10.000. Più alto è il valore, maggiore sarà la priorità. In altre parole, una voce con il valore 0 ha la priorità più bassa.

   È ad esempio possibile concedere autorizzazioni di sola lettura al gruppo Tutti e concedere autorizzazioni di lettura/scrittura al gruppo degli amministratori. A tale scopo, assegnare la priorità 1 per il gruppo degli amministratori e assegnare la priorità 0 per il gruppo Tutti.

   La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. In altre parole, se un utente è stato aggiunto a più gruppi e la priorità di tutte le regole è la stessa, Kaspersky Endpoint Security regola l'accesso al dispositivo in base a qualsiasi regola di blocco esistente.

   c. In **Utente o gruppo**, selezionare gli utenti o i gruppi di utenti. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

   d. In **Pianificazione di accesso**, configurare una pianificazione di accesso ai dispositivi di archiviazione per gli utenti.

   È ad esempio possibile consentire agli utenti di utilizzare i dispositivi di archiviazione solo durante l'orario di lavoro.

   e. Configurare le autorizzazioni di accesso degli utenti ai dispositivi di archiviazione nel programma per la gestione dei file (**Lettura**/**Scrittura**).

   f. Fare clic su **Salva**.
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare i diritti di accesso degli utenti ai dati nei dispositivi di archiviazione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nella sezione **Impostazioni di accesso**, fare clic sul collegamento **Dispositivi e reti Wi-Fi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.
4. Per configurare le regole di accesso ai dispositivi mobili, fare clic con il tasto destro del mouse per aprire l'elenco delle regole.
5. Configurare la regola di accesso ai dispositivi di archiviazione:

   a. Nel blocco **Diritti degli utenti**, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata una finestra per l'aggiunta di una nuova regola di accesso ai dispositivi di archiviazione.

   b. Nel campo **Priorità**, impostare la priorità di *scrittura della regola*. Una regola include i seguenti attributi: account utente, pianificazione, autorizzazioni (lettura/scrittura) e priorità.

   Una regola ha una priorità specifica. Se un utente è stato aggiunto a più gruppi, Kaspersky Endpoint Security regola l'accesso al dispositivo in base alla regola con la priorità più elevata. Kaspersky Endpoint Security consente di assegnare la priorità da 0 a 10.000. Più alto è il valore, maggiore sarà la priorità. In altre parole, una voce con il valore 0 ha la priorità più bassa.

   È ad esempio possibile concedere autorizzazioni di sola lettura al gruppo Tutti e concedere autorizzazioni di lettura/scrittura al gruppo degli amministratori. A tale scopo, assegnare la priorità 1 per il gruppo degli amministratori e assegnare la priorità 0 per il gruppo Tutti.

   La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. In altre parole, se un utente è stato aggiunto a più gruppi e la priorità di tutte le regole è la stessa, Kaspersky Endpoint Security regola l'accesso al dispositivo in base a qualsiasi regola di blocco esistente.

   c. In **Utenti**, selezionare gli utenti o i gruppi di utenti. È possibile selezionare gli utenti in Active Directory o immettere manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

   d. Fare clic su **OK**.
6. In **Pianificazione per l'accesso ai dispositivi**, configurare una pianificazione di accesso ai dispositivi di archiviazione per gli utenti.

   È ad esempio possibile consentire agli utenti di utilizzare i dispositivi di archiviazione solo durante l'orario di lavoro.
7. Configurare le autorizzazioni di accesso degli utenti ai dispositivi di archiviazione nel programma per la gestione dei file (**Lettura**/**Scrittura**).
8. Salvare le modifiche.

Differenziazione dei diritti di accesso degli utenti ai dispositivi attendibili

I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile. Per utilizzare dispositivi attendibili, è possibile concedere l'accesso a un singolo utente, a un gruppo di utenti o a tutti gli utenti dell'organizzazione. È possibile configurare i diritti di accesso degli utenti nelle proprietà del dispositivo attendibile.

Gestione dell'accesso ai dispositivi mobili

Kaspersky Endpoint Security consente di controllare l'accesso ai dati nei dispositivi mobili con Android e iOS. I dispositivi mobili appartengono alla categoria dei dispositivi portatili (MTP). Pertanto, per configurare l'accesso ai dati nei dispositivi mobili, è necessario modificare le impostazioni di accesso per i dispositivi portatili (MTP).

Quando un dispositivo mobile è connesso al computer, il sistema operativo determina il tipo di dispositivo. Se nel computer sono installati Android Debug Bridge (ADB), iTunes o le relative applicazioni equivalenti, il sistema operativo identifica i dispositivi mobili come dispositivi iTunes o ADB. In tutti gli altri casi, il sistema operativo può identificare il tipo di dispositivo mobile come dispositivo portatile (MTP) per il trasferimento di file, un dispositivo PTP (fotocamera) per il trasferimento di immagini o un altro dispositivo. Il tipo di dispositivo dipende dal modello del dispositivo mobile e dalla modalità di connessione USB selezionata. Kaspersky Endpoint Security consente di configurare le autorizzazioni di accesso individuali per i dati nei dispositivi mobili nelle applicazioni ADB, iTunes o il programma per la gestione dei file. In tutti gli altri casi, Controllo dispositivi consente l'accesso ai dispositivi mobili in conformità con le regole di accesso ai dispositivi portatili (MTP).

Accesso ai dispositivi mobili

I dispositivi mobili appartengono alla categoria dei dispositivi portatili (MTP), pertanto le loro impostazioni sono le stesse. È possibile selezionare una delle seguenti modalità di accesso ai dispositivi mobili:

- **Consenti**. Kaspersky Endpoint Security consente l'accesso completo ai dispositivi mobili. È possibile aprire, creare, modificare, copiare o eliminare file nei dispositivi mobili utilizzando il programma per la gestione dei file o le applicazioni ADB e iTunes. È inoltre possibile caricare la batteria del dispositivo collegando il dispositivo mobile a una porta USB del computer.
- **Blocca**. Kaspersky Endpoint Security limita l'accesso ai dispositivi mobili nel programma di gestione dei file e nelle applicazioni ADB e iTunes. L'applicazione consente l'accesso solo ai dispositivi mobili attendibili. È inoltre possibile caricare la batteria del dispositivo collegando il dispositivo mobile a una porta USB del computer.
- **Dipende dal bus di connessione**. Kaspersky Endpoint Security consente il collegamento ai dispositivi mobili in conformità con lo stato della connessione USB (**Consenti** o **Blocca**).
- **In base alle regole**. Kaspersky Endpoint Security limita l'accesso ai dispositivi mobili in conformità con le regole. Nelle regole, è possibile configurare i diritti di accesso (lettura/scrittura), selezionare gli utenti o un gruppo di utenti che possono avere accesso ai dispositivi mobili e configurare una pianificazione per l'accesso ai dispositivi mobili. È inoltre possibile limitare l'accesso ai dati nei dispositivi mobili utilizzando le applicazioni ADB e iTunes.

Configurazione delle regole di accesso ai dispositivi mobili

Le regole di accesso per dispositivi portatili (MTP), dispositivi ADB e dispositivi iTunes sono configurate in modo diverso. Per i dispositivi portatili (MTP) e i dispositivi ADB, è possibile configurare regole per singoli utenti o gruppi di utenti e creare una pianificazione per l'applicazione delle regole. Per i dispositivi iTunes, non è possibile farlo. È possibile consentire o negare l'accesso ai dati solo tramite l'applicazione iTunes per tutti gli utenti.

Come configurare le regole di accesso ai dispositivi mobili in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
4. In **Impostazioni di Controllo dispositivi**, selezionare la scheda **Tipi di dispositivi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.
5. Nel menu di scelta rapida del tipo di dispositivo **Dispositivi portatili (MTP)**, configurare la modalità di accesso ai dispositivi mobili: **Consenti**, **Blocca** o **Dipende dal bus di connessione**.
6. Per configurare le regole di accesso ai dispositivi mobili, fare doppio clic per aprire l'elenco delle regole.
7. Configurare la regola di accesso ai dispositivi mobili:

   a. Nel blocco **Regole di accesso**, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata una finestra per l'aggiunta di una nuova regola di accesso ai dispositivi mobili.

   b. Nel campo **Priorità**, impostare la priorità di scrittura della regola. Una regola include i seguenti attributi: account utente, pianificazione, autorizzazioni (lettura/scrittura/accesso ADB) e priorità.

   Una regola ha una priorità specifica. Se un utente è stato aggiunto a più gruppi, Kaspersky Endpoint Security regola l'accesso al dispositivo in base alla regola con la priorità più elevata. Kaspersky Endpoint Security consente di assegnare la priorità da 0 a 10.000. Più alto è il valore, maggiore sarà la priorità. In altre parole, una voce con il valore 0 ha la priorità più bassa.

   È ad esempio possibile concedere autorizzazioni di sola lettura al gruppo Tutti e concedere autorizzazioni di lettura/scrittura al gruppo degli amministratori. A tale scopo, assegnare la priorità 1 per il gruppo degli amministratori e assegnare la priorità 0 per il gruppo Tutti.

   La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. In altre parole, se un utente è stato aggiunto a più gruppi e la priorità di tutte le regole è la stessa, Kaspersky Endpoint Security regola l'accesso al dispositivo in base a qualsiasi regola di blocco esistente.

   c. In **Regola per utenti e gruppi**, selezionare gli utenti o i gruppi di utenti. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

   d. Fare clic su **OK**.

8. In **Pianificazioni per la regola di accesso selezionata**, configurare una pianificazione di accesso ai dispositivi mobili per gli utenti.

   Non è possibile configurare una pianificazione di accesso separata per i dispositivi ADB. È possibile configurare una pianificazione di accesso comune per i dispositivi ADB e i dispositivi portatili (MTP).

9. Configurare le autorizzazioni di accesso degli utenti ai dispositivi mobili nel programma per la gestione dei file (**Lettura/Scrittura**).

10. Configurare l'accesso ai dati in un dispositivo mobile tramite l'applicazione ADB utilizzando la casella di controllo **Accesso tramite ADB**.

    Se la casella di controllo è deselezionata, quando il dispositivo mobile è connesso, l'applicazione ADB non può rilevare il dispositivo.

11. In **Accesso tramite iTunes**, configurare l'accesso ai dati nel dispositivo mobile tramite l'applicazione iTunes.

    Kaspersky Endpoint Security applica le impostazioni per l'accesso ai dispositivi mobili tramite l'applicazione iTunes per tutti gli utenti. Non è possibile configurare una pianificazione di accesso separata per i dispositivi iTunes.

12. Salvare le modifiche.

Come configurare le regole di accesso ai dispositivi mobili in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza** → **Controllo dispositivi**.

5. Nella sezione **Regole di accesso ai dispositivi**, fare clic sul collegamento **Dispositivi e reti Wi-Fi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.

6. Selezionare il tipo di dispositivo **Dispositivi portatili (MTP)**.

   Vengono visualizzati i diritti di accesso ai dispositivi portatili (MTP).

7. Configurare la modalità di accesso ai dispositivi mobili: **Consenti**, **Blocca**, **Dipende dal bus**, or **Personalizzato**.

8. Utilizzando l'interruttore **Accesso tramite iTunes per tutti gli utenti ABILITATO**, configurare l'accesso ai dati nel dispositivo mobile tramite l'applicazione iTunes.

   Kaspersky Endpoint Security applica le impostazioni per l'accesso ai dispositivi mobili tramite l'applicazione iTunes per tutti gli utenti. Non è possibile configurare una pianificazione di accesso separata per i dispositivi iTunes.

9. Se si seleziona la modalità **Personalizzato**, è necessario aggiungere le regole di accesso ai dispositivi. A tale scopo, in **Utenti e relativi diritti**, facendo clic sul pulsante **Aggiungi** e configurare la regola di accesso ai dispositivi mobili:

    a. Nel campo **Priorità**, impostare la priorità di scrittura della regola. Una regola include i seguenti attributi: account utente, pianificazione, autorizzazioni (lettura/scrittura/accesso ADB) e priorità.

    Una regola ha una priorità specifica. Se un utente è stato aggiunto a più gruppi, Kaspersky Endpoint Security regola l'accesso al dispositivo in base alla regola con la priorità più elevata. Kaspersky Endpoint Security consente di assegnare la priorità da 0 a 10.000. Più alto è il valore, maggiore sarà la priorità. In altre parole, una voce con il valore 0 ha la priorità più bassa.

    È ad esempio possibile concedere autorizzazioni di sola lettura al gruppo Tutti e concedere autorizzazioni di lettura/scrittura al gruppo degli amministratori. A tale scopo, assegnare la priorità 1 per il gruppo degli amministratori e assegnare la priorità 0 per il gruppo Tutti.

    La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. In altre parole, se un utente è stato aggiunto a più gruppi e la priorità di tutte le regole è la stessa, Kaspersky Endpoint Security regola l'accesso al dispositivo in base a qualsiasi regola di blocco esistente.

    b. In **Utente o gruppo**, selezionare gli utenti o i gruppi di utenti che possono accedere ai dispositivi mobili. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

    c. In **Pianificazione di accesso**, configurare una pianificazione di accesso ai dispositivi mobili per gli utenti.

    > Non è possibile configurare una pianificazione di accesso separata per i dispositivi ADB. È possibile configurare una pianificazione di accesso comune per i dispositivi ADB e i dispositivi portatili (MTP).

    d. Configurare le autorizzazioni di accesso degli utenti ai dispositivi mobili nel programma per la gestione dei file (**Lettura**/**Scrittura**).

    e. Configurare l'accesso ai dati in un dispositivo mobile tramite l'applicazione ADB utilizzando la casella di controllo **Accesso tramite ADB**.

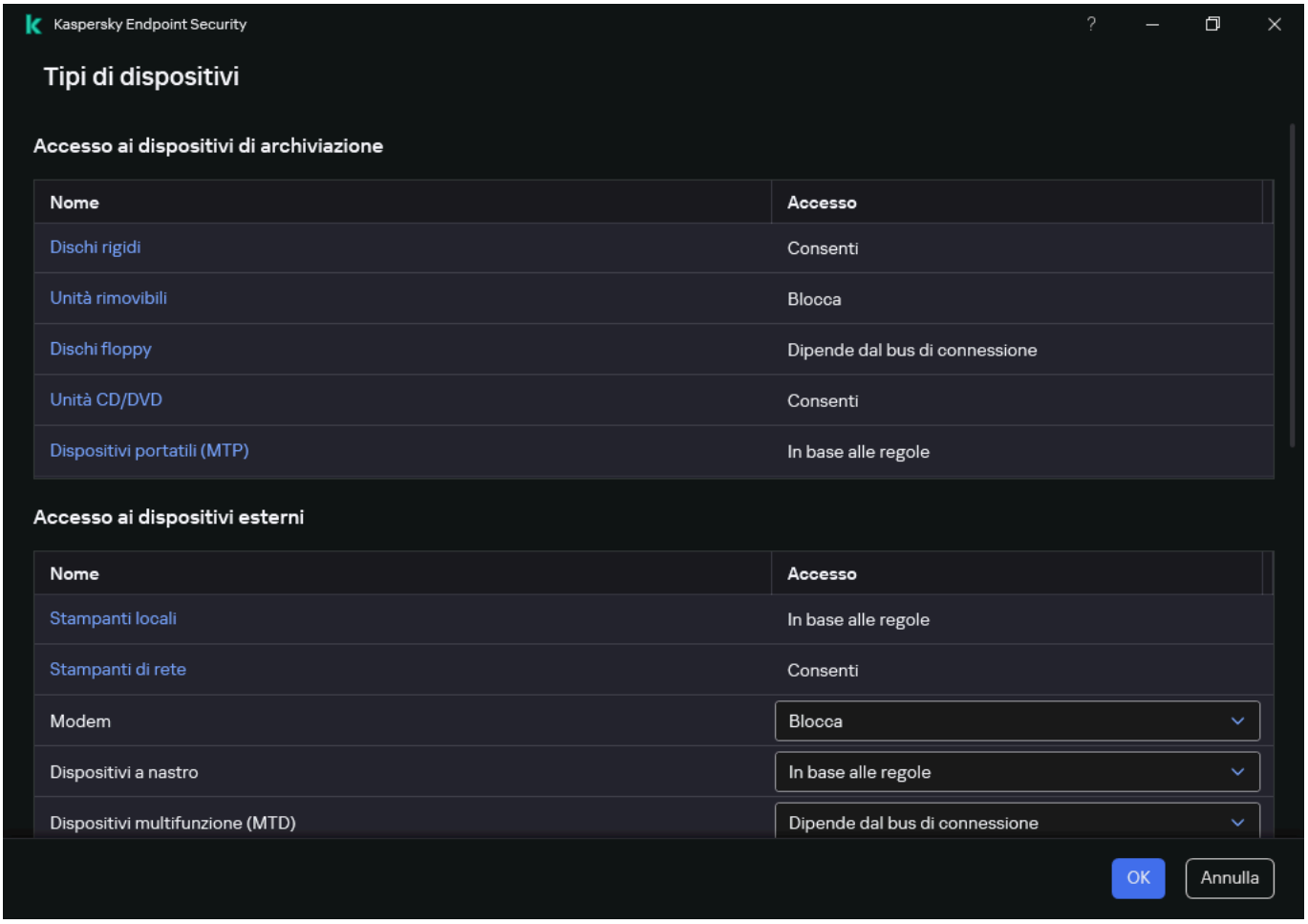
    Se la casella di controllo è deselezionata, quando il dispositivo mobile è connesso, l'applicazione ADB non può rilevare il dispositivo.

10. Salvare le modifiche.

Come configurare le regole di accesso ai dispositivi mobili nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Dispositivi e reti Wi-Fi**.

La finestra visualizzata mostra le regole di accesso per tutti i dispositivi inclusi nella classificazione del componente Controllo dispositivi.



Tipi di dispositivi nel componente Controllo dispositivi

4. Nella sezione **Accesso ai dispositivi di archiviazione**, fare clic sul collegamento **Dispositivi portatili (MTP)**.

   Viene visualizzata una finestra con le regole di accesso ai dispositivi portatili (MTP).

5. In **Accesso**, configurare la modalità di accesso ai dispositivi mobili: **Consenti**, **Blocca**, **Dipende dal bus di connessione** o **In base alle regole**.

6. Se si seleziona la modalità **In base alle regole**, è necessario aggiungere le regole di accesso ai dispositivi:

   a. Nel blocco **Diritti degli utenti**, fare clic sul pulsante **Aggiungi**.

      Verrà visualizzata una finestra per l'aggiunta di una nuova regola di accesso ai dispositivi mobili.

   b. Nel campo **Priorità**, impostare la priorità di scrittura della regola. Una regola include i seguenti attributi: account utente, pianificazione, autorizzazioni (lettura/scrittura/accesso ADB) e priorità.

      Una regola ha una priorità specifica. Se un utente è stato aggiunto a più gruppi, Kaspersky Endpoint Security regola l'accesso al dispositivo in base alla regola con la priorità più elevata. Kaspersky Endpoint Security consente di assegnare la priorità da 0 a 10.000. Più alto è il valore, maggiore sarà la priorità. In altre parole, una voce con il valore 0 ha la priorità più bassa.

      È ad esempio possibile concedere autorizzazioni di sola lettura al gruppo Tutti e concedere autorizzazioni di lettura/scrittura al gruppo degli amministratori. A tale scopo, assegnare la priorità 1 per il gruppo degli amministratori e assegnare la priorità 0 per il gruppo Tutti.

      La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. In altre parole, se un utente è stato aggiunto a più gruppi e la priorità di tutte le regole è la stessa, Kaspersky Endpoint Security regola l'accesso al dispositivo in base a qualsiasi regola di blocco esistente.

c. In **Stato**, attivare la regola di accesso ai dispositivi mobili.

d. In **Regole di accesso**, configurare le autorizzazioni di accesso ai dispositivi mobili per gli utenti.

- Configurare le autorizzazioni di accesso degli utenti ai dispositivi mobili nel programma per la gestione dei file (**Lettura/Scrittura**).
- Configurare l'accesso ai dati in un dispositivo mobile tramite l'applicazione ADB utilizzando la casella di controllo **Accesso tramite ADB**.

  Se la casella di controllo è deselezionata, quando il dispositivo mobile è connesso, l'applicazione ADB non può rilevare il dispositivo.

e. In **Utenti**, selezionare gli utenti o i gruppi di utenti che possono accedere ai dispositivi mobili. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

f. In **Pianificazione per l'accesso ai dispositivi**, configurare una pianificazione di accesso ai dispositivi per gli utenti.

> Non è possibile configurare una pianificazione di accesso separata per i dispositivi ADB. È possibile configurare una pianificazione di accesso comune per i dispositivi ADB e i dispositivi portatili (MTP).

g. In **Accesso tramite iTunes**, configurare l'accesso ai dati nel dispositivo mobile tramite l'applicazione iTunes.

> Kaspersky Endpoint Security applica le impostazioni per l'accesso ai dispositivi mobili tramite l'applicazione iTunes per tutti gli utenti. Non è possibile configurare una pianificazione di accesso separata per i dispositivi iTunes.

7. Salvare le modifiche.

Di conseguenza, l'accesso degli utenti ai dispositivi mobili è limitato in conformità alle regole. Se è stato vietato l'accesso ai dispositivi mobili nelle applicazioni ADB e iTunes, quando si collega un dispositivo mobile, le applicazioni ADB e iTunes non possono rilevare il dispositivo mobile.

Dispositivi mobili attendibili

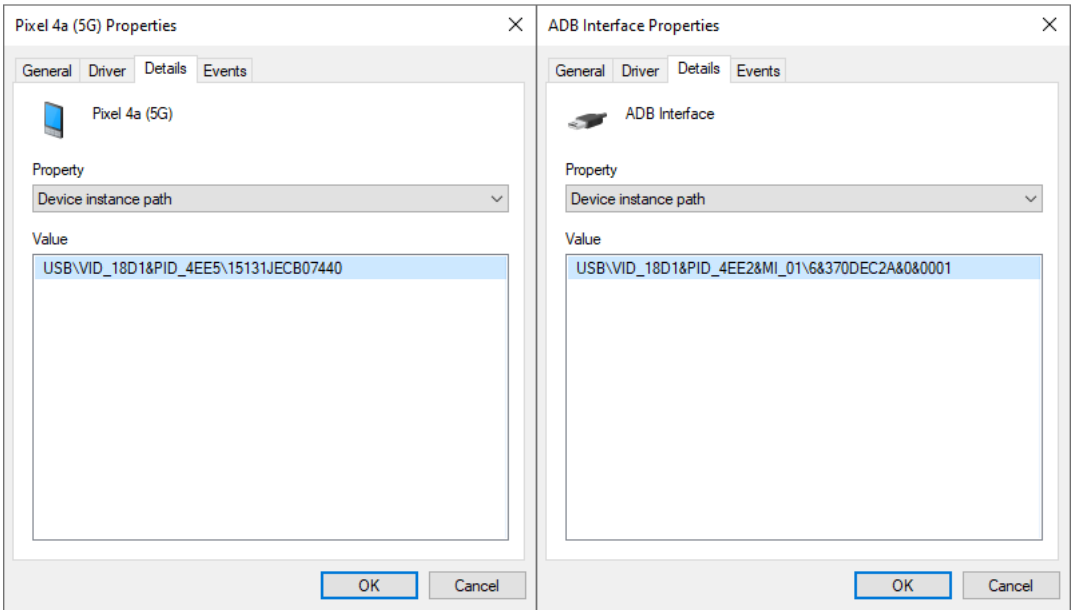
I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile.

La procedura per l'aggiunta di un dispositivo mobile attendibile è esattamente la stessa di altri tipi di dispositivi attendibili. È possibile aggiungere un dispositivo mobile in base all'ID o al modello del dispositivo.

Per aggiungere un dispositivo mobile attendibile in base all'ID, sarà necessario un ID univoco (Hardware ID - HWID). È possibile trovare l'ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo (vedere la figura seguente). Lo strumento Gestione dispositivi consente di farlo. Gli ID dei dispositivi portatili (MTP) e dei dispositivi ADB e iTunes sono diversi anche per lo stesso dispositivo mobile. L'ID di un dispositivo portatile (MTP) può essere simile al seguente: `15131JECB07440`. L'ID di un dispositivo ADB può essere simile al seguente: `6&370DEC2A&0&0001`. L'aggiunta di dispositivi in base all'ID è utile se si desidera aggiungere più dispositivi specifici. È possibile usare anche le maschere.

Se sono state installate le applicazioni ADB o iTunes dopo la connessione di un dispositivo al computer, l'ID univoco del dispositivo può essere reimpostato. Questo significa che Kaspersky Endpoint Security identificherà il dispositivo come un nuovo dispositivo. Se un dispositivo è attendibile, aggiungere nuovamente il dispositivo all'elenco dei dispositivi attendibili.

Per aggiungere un dispositivo mobile attendibile in base al modello del dispositivo, sarà necessario il relativo Vendor ID (VID) e Product ID (PID). È possibile trovare gli ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo (vedere la figura seguente). Modello per l'immissione di VID e PID: `VID_18D1&PID_4EE5`. L'aggiunta di dispositivi in base al modello è utile se si utilizzano dispositivi di un determinato modello nell'organizzazione. In tal modo è possibile aggiungere tutti i dispositivi di questo modello.



ID dispositivo in Gestione dispositivi

Gestione dell'accesso ai dispositivi Bluetooth

Kaspersky Endpoint Security consente di gestire l'accesso ai dispositivi Bluetooth. I dispositivi Bluetooth includono tastiere, mouse, auricolari, stampanti wireless ecc. È inoltre possibile utilizzare il Bluetooth per comunicare, ad esempio, con un dispositivo mobile.

Quando i dispositivi Bluetooth sono connessi o disconnessi, l'applicazione potrebbe creare più eventi sul dispositivo. Il motivo è che il sistema operativo potrebbe rilevare un dispositivo Bluetooth come più dispositivi di tipo diverso. Kaspersky Endpoint Security gestisce anche la scheda Bluetooth tramite il quale il dispositivo è connesso come dispositivo separato. Ecco perché l'applicazione crea un evento per ciascuno dei dispositivi rilevati.

È possibile selezionare una delle seguenti modalità di accesso ai dispositivi Bluetooth:

- **Consenti e non registrare** . Kaspersky Endpoint Security consente la connessione di qualsiasi dispositivo Bluetooth e non salva le informazioni sulla connessione nel registro eventi. È possibile connettere dispositivi di input Bluetooth (tastiere, mouse ecc.), inviare dati tramite Bluetooth, gestire altri dispositivi Bluetooth (auricolari, cuffie ecc.)

- **Consenti** . Kaspersky Endpoint Security consente di connettere qualsiasi dispositivo Bluetooth. È possibile connettere dispositivi di input Bluetooth (tastiere, mouse ecc.), inviare dati tramite Bluetooth, gestire altri dispositivi Bluetooth (auricolari, cuffie ecc.).

- **Blocca** . Kaspersky Endpoint Security limita l'accesso ai dispositivi Bluetooth. È possibile consentire la connessione solo dei dispositivi di input Bluetooth (la classe Human Interface Devices). Questi dispositivi includono tastiere, mouse, joystick ecc.

Non è possibile creare un elenco di dispositivi Bluetooth attendibili. Se si ha accesso limitato ai dispositivi Bluetooth, è possibile connettersi solo con dispositivi di input Bluetooth.

Come configurare le regole di accesso ai dispositivi Bluetooth in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
5. In **Impostazioni di Controllo dispositivi**, selezionare la scheda **Tipi di dispositivi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.
6. Nel menu di scelta rapida del tipo di dispositivo **Bluetooth**, configurare la modalità di accesso ai dispositivi Bluetooth: **Consenti** , **Blocca** o **Consenti e non registrare** .
7. Se si seleziona la modalità **Blocca**, è possibile consentire la connessione solo di dispositivi di input Bluetooth (tastiere, mouse ecc.) A tale scopo, in **Esclusioni**, selezionare la casella di controllo **Dispositivi di input (mouse e tastiere)**.
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare le regole di accesso ai dispositivi Bluetooth in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo dispositivi**.

5. Nella sezione **Regole di accesso ai dispositivi**, fare clic sul collegamento **Dispositivi e reti Wi-Fi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.

6. Selezionare il tipo di dispositivo **Dispositivi Bluetooth**.

   Si aprono le impostazioni di accesso del dispositivo Bluetooth.

7. Configurare la modalità di accesso del dispositivo Bluetooth: **Consenti**, **Blocca**, **Consenti e non registrare**.

8. Se si seleziona la modalità **Blocca**, è possibile consentire la connessione solo di dispositivi di input Bluetooth (tastiere, mouse ecc.) A tale scopo, in **Esclusioni**, selezionare la casella di controllo **Dispositivi di input (mouse e tastiere)**.

9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

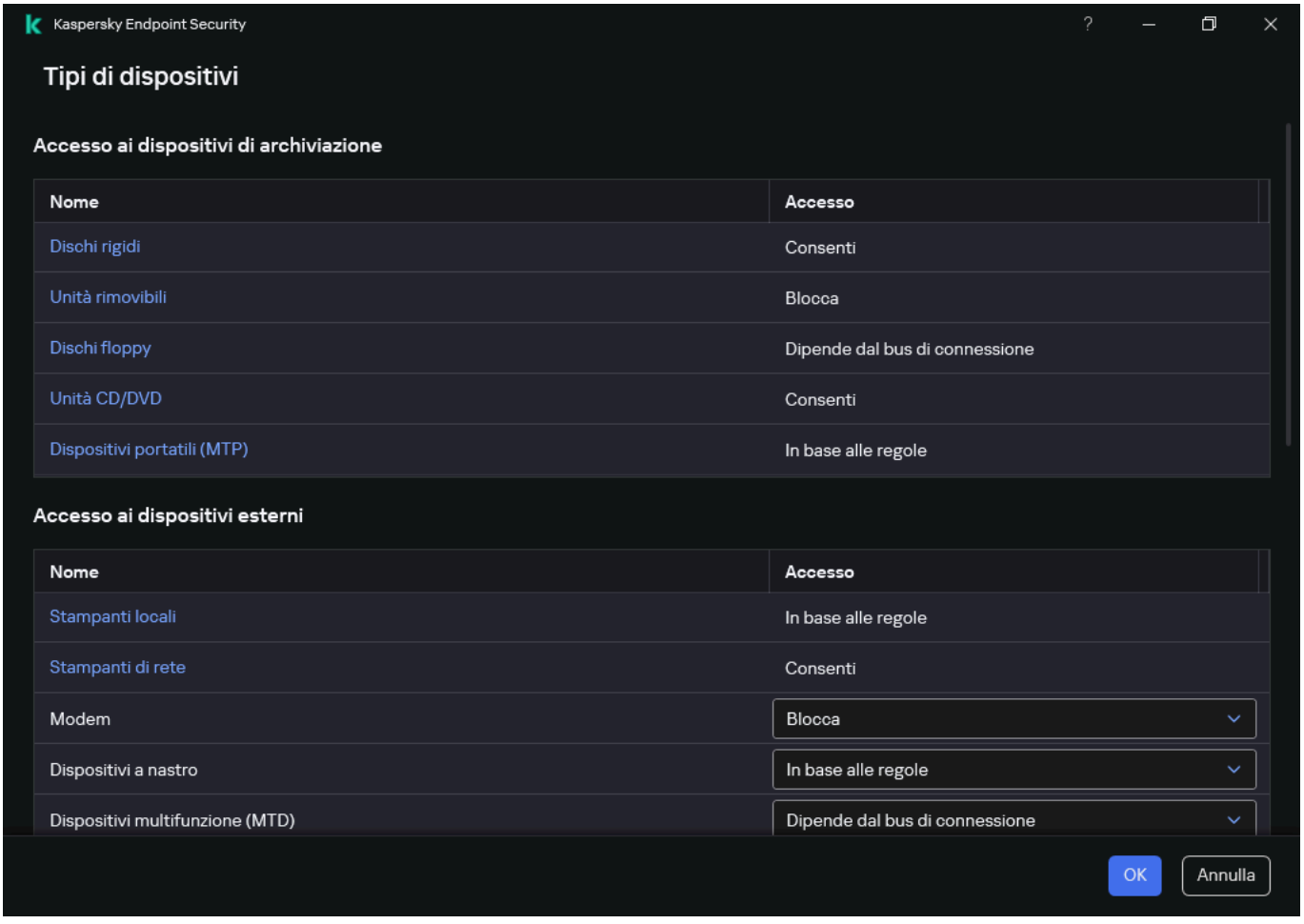
Come configurare le regole di accesso ai dispositivi Bluetooth nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza → Controllo dispositivi**.

3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Dispositivi e reti Wi-Fi**.

   La finestra visualizzata mostra le regole di accesso per tutti i dispositivi inclusi nella classificazione del componente Controllo dispositivi.



Tipi di dispositivi nel componente Controllo dispositivi

4. Nella sezione **Accesso ai dispositivi esterni**, fare clic sul collegamento **Bluetooth**.

   Si aprono le impostazioni di accesso del dispositivo Bluetooth.

5. In **Accesso**, configurare la modalità di accesso del dispositivo Bluetooth: **Consenti**, **Blocca**, **Consenti e non registrare**.

6. Se si seleziona la modalità **Blocca**, è possibile consentire la connessione solo di dispositivi di input Bluetooth (tastiere, mouse ecc.) A tale scopo, in **Esclusioni**, selezionare la casella di controllo **Dispositivi di input (mouse e tastiere)**.

7. Salvare le modifiche.

Controllo della stampa

Il controllo di stampa non è supportato nei computer basati su Arm.

È possibile utilizzare Controllo della stampa per configurare l'accesso degli utenti alle stampanti locali e di rete.

Controllo delle stampanti locali

Kaspersky Endpoint Security consente di configurare l'accesso alle stampanti locali su due livelli: *collegamento* e *stampa*.

Kaspersky Endpoint Security controlla la connessione della stampante locale sui seguenti bus: USB, Porta seriale (COM), Porta parallela (LPT).

Kaspersky Endpoint Security controlla la connessione delle stampanti locali alle porte COM e LPT solo a livello di bus. Pertanto, per impedire le connessioni della stampante tramite le porte COM e LPT, è necessario selezionare la modalità di accesso Dipende dal bus di connessione per le stampanti locali e vietare le connessioni ai bus COM e LPT.

Per le stampanti connesse tramite USB, l'applicazione esercita il controllo su due livelli: tipo di dispositivo (stampanti locali) e bus di connessione (USB).

È possibile selezionare una delle seguenti modalità di accesso alle stampanti locali tramite USB:

- **Consenti** ✓. Kaspersky Endpoint Security concede a tutti gli utenti l'accesso completo alle stampanti locali. Gli utenti possono collegare stampanti e stampare documenti utilizzando i mezzi forniti dal sistema operativo.

- **Blocca** ⊘. Kaspersky Endpoint Security blocca il collegamento delle stampanti locali. L'applicazione consente solo il collegamento di stampanti attendibili.

- **Dipende dal bus di connessione**. Kaspersky Endpoint Security consente la connessione alle stampanti locali in conformità con lo stato della connessione bus USB (**Consenti** o **Blocca**).
- **In base alle regole**. Per controllare la stampa, è necessario aggiungere *regole di stampa*. Nelle regole, è possibile selezionare gli utenti o un gruppo di utenti per i quali si desidera consentire o bloccare l'accesso alla stampa di documenti su stampanti locali.

Controllo delle stampanti di rete

Kaspersky Endpoint Security consente di configurare l'accesso alla stampa sulle stampanti di rete. È possibile selezionare una delle seguenti modalità di accesso alle stampanti di rete:

- **Consenti e non registrare**. Kaspersky Endpoint Security non controlla la stampa sulle stampanti di rete. L'applicazione concede l'accesso alla stampa a tutti gli utenti e non salva le informazioni sulla stampa nel registro eventi.
- **Consenti**. Kaspersky Endpoint Security concede l'accesso alla stampa sulle stampanti di rete a tutti gli utenti.
- **Blocca**. Kaspersky Endpoint Security limita l'accesso alle stampanti di rete per tutti gli utenti. L'applicazione consente l'accesso solo alle stampanti attendibili.
- **In base alle regole**. Kaspersky Endpoint Security concede l'accesso alla stampa in conformità con le regole di stampa. Nelle regole, è possibile selezionare gli utenti o un gruppo di utenti a cui sarà consentito o impedito di stampare documenti sulla stampante di rete.

Aggiunta di regole di stampa per le stampanti

Come aggiungere regole di stampa in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
4. In **Impostazioni di Controllo dispositivi**, selezionare la scheda **Tipi di dispositivi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.
5. Nel menu di scelta rapida dei tipi di dispositivi **Stampanti locali** e **Stampanti di rete**, configurare la modalità di accesso per le stampanti pertinenti: **Consenti**, **Blocca**, **Consenti e non registrare** (solo per le stampanti di rete) o **Dipende dal bus di connessione** (solo per le stampanti locali).
6. Per configurare le regole di stampa su stampanti locali e di rete, fare doppio clic sugli elenchi di regole per aprirli.
7. Selezionare **In base alle regole** come modalità di accesso alla stampante.

8. Selezionare gli utenti o i gruppi di utenti al quale si desidera applicare la regola di stampa.

   a. Fare clic su **Aggiungi**.

      Verrà visualizzata una finestra per l'aggiunta di una nuova regola di stampa.

   b. Assegnare una priorità alla voce di regola. Una voce di regola include i seguenti attributi: account utente, azione (consenti/blocca) e priorità.

      Una regola ha una priorità specifica. Se un utente è stato aggiunto a più gruppi, Kaspersky Endpoint Security regola l'accesso al dispositivo in base alla regola con la priorità più elevata. Kaspersky Endpoint Security consente di assegnare la priorità da 0 a 10.000. Più alto è il valore, maggiore sarà la priorità. In altre parole, una voce con il valore 0 ha la priorità più bassa.

      È ad esempio possibile concedere autorizzazioni di sola lettura al gruppo Tutti e concedere autorizzazioni di lettura/scrittura al gruppo degli amministratori. A tale scopo, assegnare la priorità 1 per il gruppo degli amministratori e assegnare la priorità 0 per il gruppo Tutti.

      La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. In altre parole, se un utente è stato aggiunto a più gruppi e la priorità di tutte le regole è la stessa, Kaspersky Endpoint Security regola l'accesso al dispositivo in base a qualsiasi regola di blocco esistente.

   c. In **Azione**, configurare l'accesso dell'utente alla stampa sulla stampante.

   d. Fare clic su **Utenti e gruppi** e selezionare gli utenti o i gruppi di utenti che possono accedere alla stampa. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

   e. Fare clic su **OK**.

9. Salvare le modifiche.

Come aggiungere regole di stampa in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza** → **Controllo dispositivi**.

5. Nella sezione **Regole di accesso ai dispositivi**, fare clic sul collegamento **Dispositivi e reti Wi-Fi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.

6. Selezionare il tipo di dispositivo **Stampanti locali** o **Stampanti di rete**.

   Vengono visualizzate le regole di accesso alle stampanti.

7. Configurare la modalità di accesso per le stampanti pertinenti: **Consenti**, **Blocca**, **Consenti e non registrare** (solo per le stampanti di rete), **Dipende dal bus** (solo per le stampanti locali), o **Personalizzato**.

8. Se si seleziona la modalità **Personalizzato**, è necessario aggiungere regole di stampa per le stampanti locali o di rete. A tale scopo, fare clic sul pulsante **Aggiungi** nella tabella delle regole di stampa.

   Vengono visualizzate le impostazioni della nuova regola di stampa.

9. Assegnare una priorità alla voce di regola. Una voce di regola include i seguenti attributi: account utente, azione (consenti/blocca) e priorità.

   Una regola ha una priorità specifica. Se un utente è stato aggiunto a più gruppi, Kaspersky Endpoint Security regola l'accesso al dispositivo in base alla regola con la priorità più elevata. Kaspersky Endpoint Security consente di assegnare la priorità da 0 a 10.000. Più alto è il valore, maggiore sarà la priorità. In altre parole, una voce con il valore 0 ha la priorità più bassa.

   È ad esempio possibile concedere autorizzazioni di sola lettura al gruppo Tutti e concedere autorizzazioni di lettura/scrittura al gruppo degli amministratori. A tale scopo, assegnare la priorità 1 per il gruppo degli amministratori e assegnare la priorità 0 per il gruppo Tutti.

   La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. In altre parole, se un utente è stato aggiunto a più gruppi e la priorità di tutte le regole è la stessa, Kaspersky Endpoint Security regola l'accesso al dispositivo in base a qualsiasi regola di blocco esistente.

10. In **Azione**, configurare l'accesso dell'utente alla stampa sulla stampante.

11. In **Utente o gruppo**, selezionare gli utenti o i gruppi di utenti che possono accedere alla stampa. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

12. Salvare le modifiche.

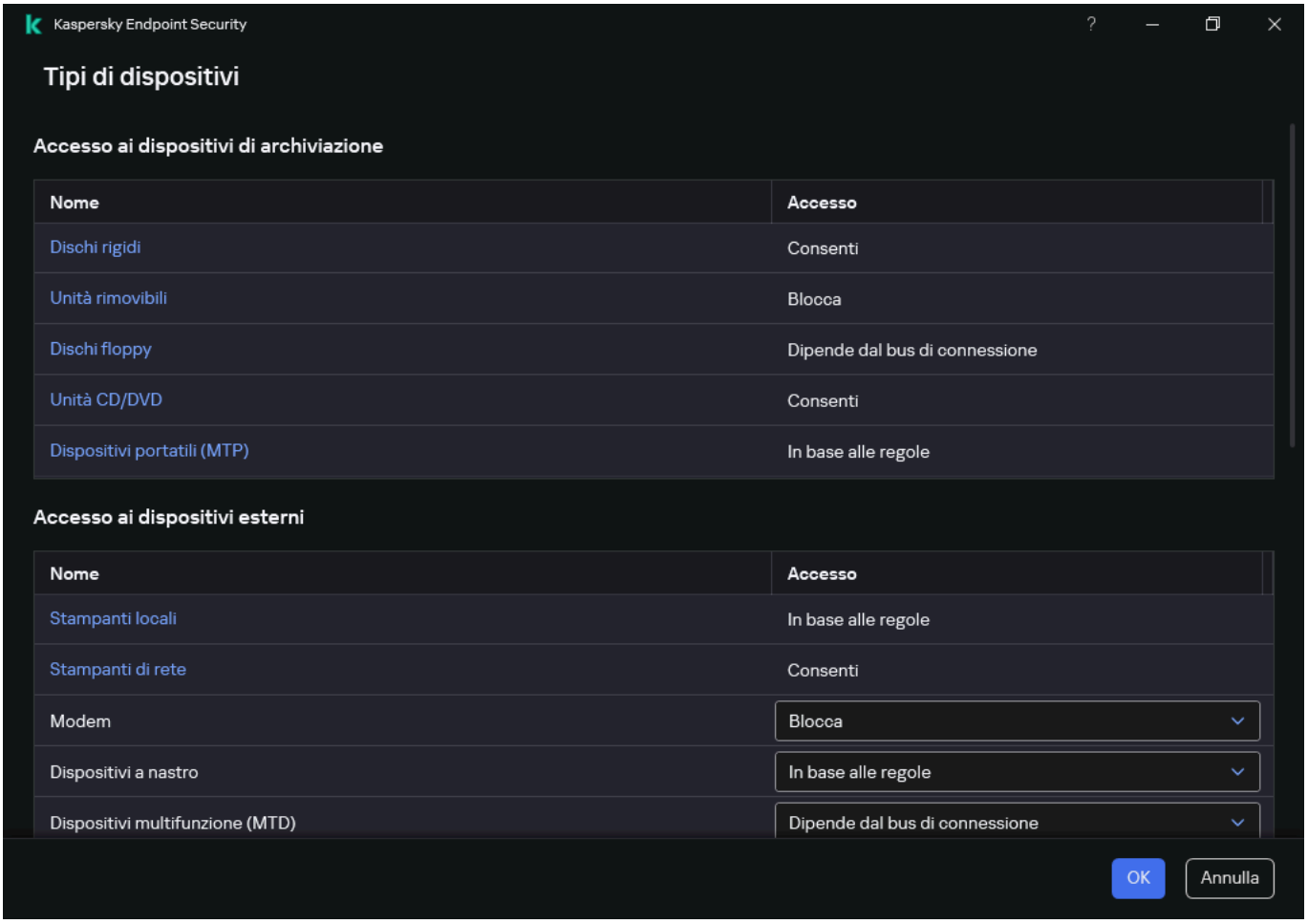
Come aggiungere regole di stampa nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.

3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Dispositivi e reti Wi-Fi**.

La finestra visualizzata mostra le regole di accesso per tutti i dispositivi inclusi nella classificazione del componente Controllo dispositivi.



Tipi di dispositivi nel componente Controllo dispositivi

4. In **Accesso ai dispositivi esterni**, fare clic su **Stampanti locali** o **Stampanti di rete**.

   Viene visualizzata una finestra con le regole di accesso alla stampante.

5. In **Accesso alle stampanti locali** o **Accesso alle stampanti di rete**, configurare la modalità di accesso per le stampanti: **Consenti**, **Blocca**, **Consenti e non registrare** (solo per le stampanti di rete), **Dipende dal bus di connessione** (solo per le stampanti locali) o **In base alle regole**.

6. Se si seleziona la modalità **In base alle regole**, è necessario aggiungere regole di stampa per le stampanti. Selezionare gli utenti o i gruppi di utenti al quale si desidera applicare la regola di stampa.

   a. Fare clic su **Aggiungi**.

      Verrà visualizzata una finestra per l'aggiunta di una nuova regola di stampa.

   b. Assegnare una priorità alla voce di regola. Una voce di regola include i seguenti attributi: account utente, autorizzazioni (consenti/blocca) e priorità.

      Una regola ha una priorità specifica. Se un utente è stato aggiunto a più gruppi, Kaspersky Endpoint Security regola l'accesso al dispositivo in base alla regola con la priorità più elevata. Kaspersky Endpoint Security consente di assegnare la priorità da 0 a 10.000. Più alto è il valore, maggiore sarà la priorità. In altre parole, una voce con il valore 0 ha la priorità più bassa.

      È ad esempio possibile concedere autorizzazioni di sola lettura al gruppo Tutti e concedere autorizzazioni di lettura/scrittura al gruppo degli amministratori. A tale scopo, assegnare la priorità 1 per il gruppo degli amministratori e assegnare la priorità 0 per il gruppo Tutti.

La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. In altre parole, se un utente è stato aggiunto a più gruppi e la priorità di tutte le regole è la stessa, Kaspersky Endpoint Security regola l'accesso al dispositivo in base a qualsiasi regola di blocco esistente.

c. In **Azione**, configurare le autorizzazioni utente per l'accesso alla stampa.

d. In **Utenti e gruppi**, selezionare gli utenti o i gruppi di utenti che possono accedere alla stampa. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

7. Salvare le modifiche.

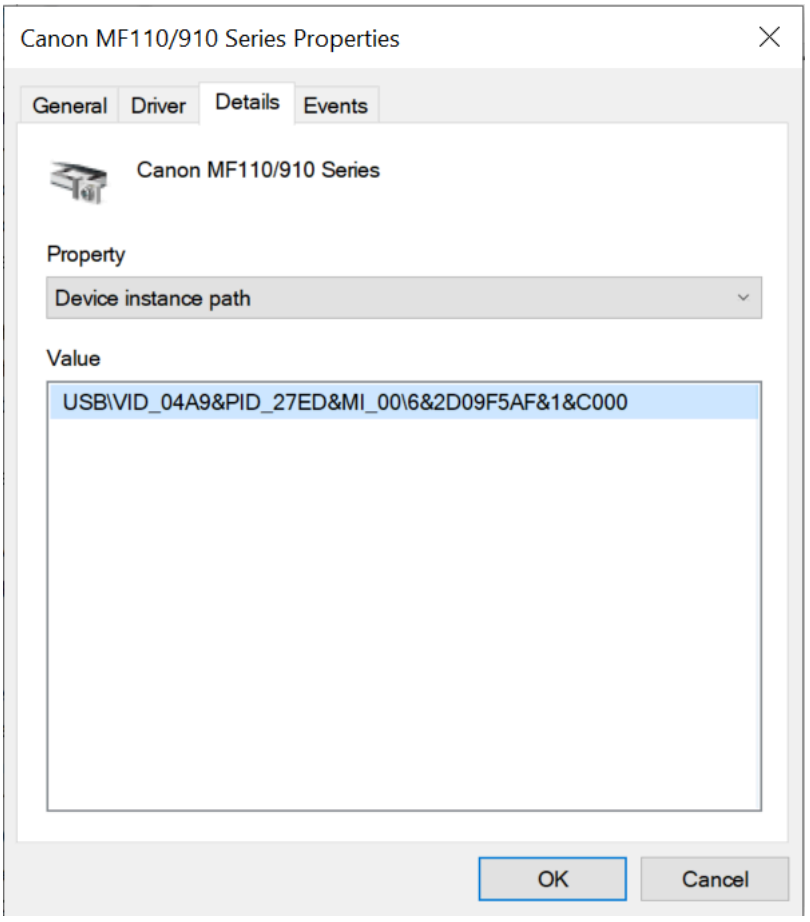
Stampanti attendibili

I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile.

La procedura per l'aggiunta di stampanti attendibili è esattamente la stessa di altri tipi di dispositivi attendibili. È possibile aggiungere stampanti locali in base all'ID o al modello del dispositivo. È possibile aggiungere stampanti di rete solo in base all'ID dispositivo.

Per aggiungere una stampante locale attendibile in base all'ID, sarà necessario un ID univoco (Hardware ID - HWID). È possibile trovare l'ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo (vedere la figura seguente). Lo strumento Device Manager consente di farlo. L'ID di una stampante locale può essere simile al seguente: `6&2D09F5AF&1&C000`. L'aggiunta di dispositivi in base all'ID è utile se si desidera aggiungere più dispositivi specifici. È possibile usare anche le maschere.

Per aggiungere una stampante locale mobile attendibile in base al modello del dispositivo, sarà necessario il relativo Vendor ID (VID) e Product ID (PID). È possibile trovare gli ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo (vedere la figura seguente). Modello per l'immissione di VID e PID: `VID_04A9&PID_27FD`. L'aggiunta di dispositivi in base al modello è utile se si utilizzano dispositivi di un determinato modello nell'organizzazione. In tal modo è possibile aggiungere tutti i dispositivi di questo modello.



ID dispositivo in Gestione dispositivi

Per aggiungere una stampante di rete attendibile, sarà necessario il relativo ID dispositivo. Per le stampanti di rete, l'ID dispositivo può essere il nome di rete della stampante (nome della stampante condivisa), l'indirizzo IP della stampante o l'URL della stampante.

Controllo delle connessioni Wi-Fi

Controllo dispositivi consente di gestire la connessione Wi-Fi del computer (laptop). Le reti Wi-Fi pubbliche potrebbero non essere sicure e l'utilizzo di tali reti può comportare la perdita di dati. Controllo dispositivi consente di impedire a un utente di connettersi alla rete Wi-Fi o di consentire la connessione solo a reti attendibili. Ad esempio, è possibile consentire la connessione solo alla rete Wi-Fi aziendale sufficientemente sicura. Controllo dispositivi bloccherà l'accesso a tutte le reti Wi-Fi tranne quelle specificate nell'elenco delle reti attendibili.

Nei computer in cui viene eseguito Windows 11, è necessario abilitare i servizi di posizione per controllare le connessioni Wi-Fi. A tale scopo, è necessario abilitare l'interruttore **Servizi di posizione** nelle impostazioni del sistema operativo (**Impostazioni** → **Privacy & sicurezza** → **Posizione**). Se i servizi di localizzazione sono disabilitati, Kaspersky Endpoint Security non controlla le connessioni alle reti Wi-Fi.

Come limitare le connessioni Wi-Fi in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
4. In **Impostazioni di Controllo dispositivi**, selezionare la scheda **Tipi di dispositivi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.
5. Nel menu di scelta rapida per il tipo di dispositivo **Wi-Fi**, selezionare l'azione di Controllo dispositivi eseguita durante la connessione alla rete Wi-Fi: **Consenti** ( ), **Blocca** ( ) o **Blocca con eccezioni** ( ).
6. Se è stata selezionata l'opzione **Blocca con eccezioni**, creare un elenco di reti Wi-Fi attendibili:

   a. Fare doppio clic per aprire l'elenco delle reti Wi-Fi attendibili.

   b. Nel blocco **Reti Wi-Fi attendibili**, fare clic sul pulsante **Aggiungi**.

   c. Viene visualizzata una finestra; in questa finestra, configurare la rete Wi-Fi attendibile (vedere la figura riportata di seguito):

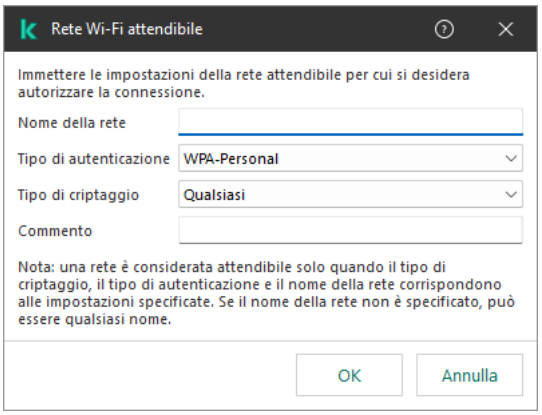
   - **Nome della rete**. Nome o SSID (Service Set Identifier) della rete Wi-Fi.
   - **Tipo di autenticazione**. Tipo di autenticazione utilizzato durante la connessione alla rete Wi-Fi.

     A partire da Kaspersky Endpoint Security for Windows versione 12.0, all'applicazione è stato aggiunto il supporto del protocollo WPA3. Se a un computer viene applicato un criterio di Kaspersky Endpoint Security versione 12.2, il protocollo WPA2 viene selezionato nei computer con Kaspersky Endpoint Security versione 11.11.0 e precedenti; WPA2/WPA3 viene selezionato per le versioni da 12.0 a 12.1; WPA3 viene selezionato per le versioni 12.2 e successive.
   - **Tipo di criptaggio**. Tipo di criptaggio utilizzato per proteggere il traffico Wi-Fi.
   - **Commento**. Ulteriori informazioni sulla rete Wi-Fi aggiunta.

   È possibile visualizzare le impostazioni della rete Wi-Fi attendibile nelle impostazioni del router.

   Una rete Wi-Fi viene considerata attendibile se le relative impostazioni corrispondono a tutte le impostazioni specificate nella regola.

7. Salvare le modifiche.



Impostazioni di rete Wi-Fi attendibile

Come limitare le connessioni Wi-Fi in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo dispositivi**.
5. In **Regole di accesso ai dispositivi**, selezionare la scheda **Dispositivi e reti Wi-Fi**.

   La tabella elenca le regole di accesso per tutti i dispositivi presenti nella classificazione del componente Controllo dispositivi.
6. Nella sezione **Reti Wi-Fi**, fare clic sul collegamento **Wi-Fi**.
7. Nella finestra visualizzata, selezionare l'azione di Controllo dispositivo eseguita durante la connessione alla rete Wi-Fi: **Consenti**, **Blocca** o **Blocco con esclusioni**.
8. Se è stata selezionata l'opzione **Blocco con esclusioni**, creare un elenco di reti Wi-Fi attendibili:

   a. Fare doppio clic per aprire l'elenco delle reti Wi-Fi attendibili.

   b. Nel blocco **Reti Wi-Fi attendibili**, fare clic sul pulsante **Aggiungi**.

   c. Viene visualizzata una finestra; in questa finestra, configurare la rete Wi-Fi attendibile (vedere la figura riportata di seguito):

   - **Nome**. Nome o SSID (Service Set Identifier) della rete Wi-Fi.
   - **Tipo di autenticazione**. Tipo di autenticazione utilizzato durante la connessione alla rete Wi-Fi.

     A partire da Kaspersky Endpoint Security for Windows versione 12.0, all'applicazione è stato aggiunto il supporto del protocollo WPA3. Se a un computer viene applicato un criterio di Kaspersky Endpoint Security versione 12.2, il protocollo WPA2 viene selezionato nei computer con Kaspersky Endpoint Security versione 11.11.0 e precedenti; WPA2/WPA3 viene selezionato per le versioni da 12.0 a 12.1; WPA3 viene selezionato per le versioni 12.2 e successive.

- **Tipo di criptaggio**. Tipo di criptaggio utilizzato per proteggere il traffico Wi-Fi.
- **Commento**. Ulteriori informazioni sulla rete Wi-Fi aggiunta.

È possibile visualizzare le impostazioni della rete Wi-Fi attendibile nelle impostazioni del router.

> Una rete Wi-Fi viene considerata attendibile se le relative impostazioni corrispondono a tutte le impostazioni specificate nella regola.

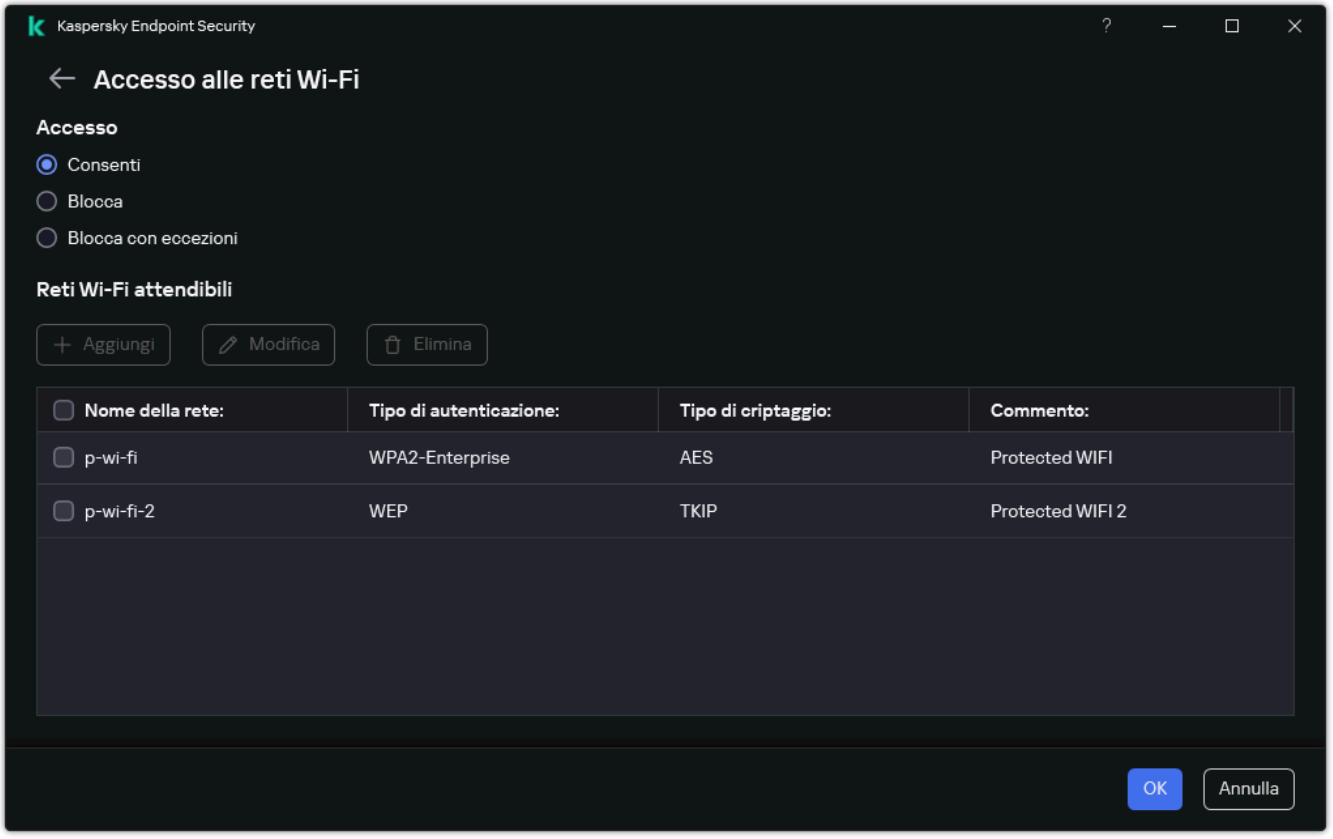
9. Salvare le modifiche.

Come limitare le connessioni Wi-Fi nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Dispositivi e reti Wi-Fi**.

   La finestra visualizzata mostra le regole di accesso per tutti i dispositivi inclusi nella classificazione del componente Controllo dispositivi.
4. Nella sezione **Accesso alle reti Wi-Fi**, fare clic sul collegamento **Wi-Fi**.

   La finestra visualizzata mostra le regole di accesso alla rete Wi-Fi.



Impostazioni di accesso Wi-Fi

5. In **Accesso**, selezionare l'azione di Controllo dispositivo eseguita durante la connessione alla rete Wi-Fi: **Consenti**, **Blocca** o **Blocca con eccezioni**.

6. Se è stata selezionata l'opzione **Blocca con eccezioni**, creare un elenco di reti Wi-Fi attendibili:

   a. Nel blocco **Reti Wi-Fi attendibili**, fare clic sul pulsante **Aggiungi**.

   b. Viene visualizzata una finestra; in questa finestra, configurare la rete Wi-Fi attendibile (vedere la figura riportata di seguito):

   - **Nome della rete**. Nome o SSID (Service Set Identifier) della rete Wi-Fi.
   - **Tipo di autenticazione**. Tipo di autenticazione utilizzato durante la connessione alla rete Wi-Fi.

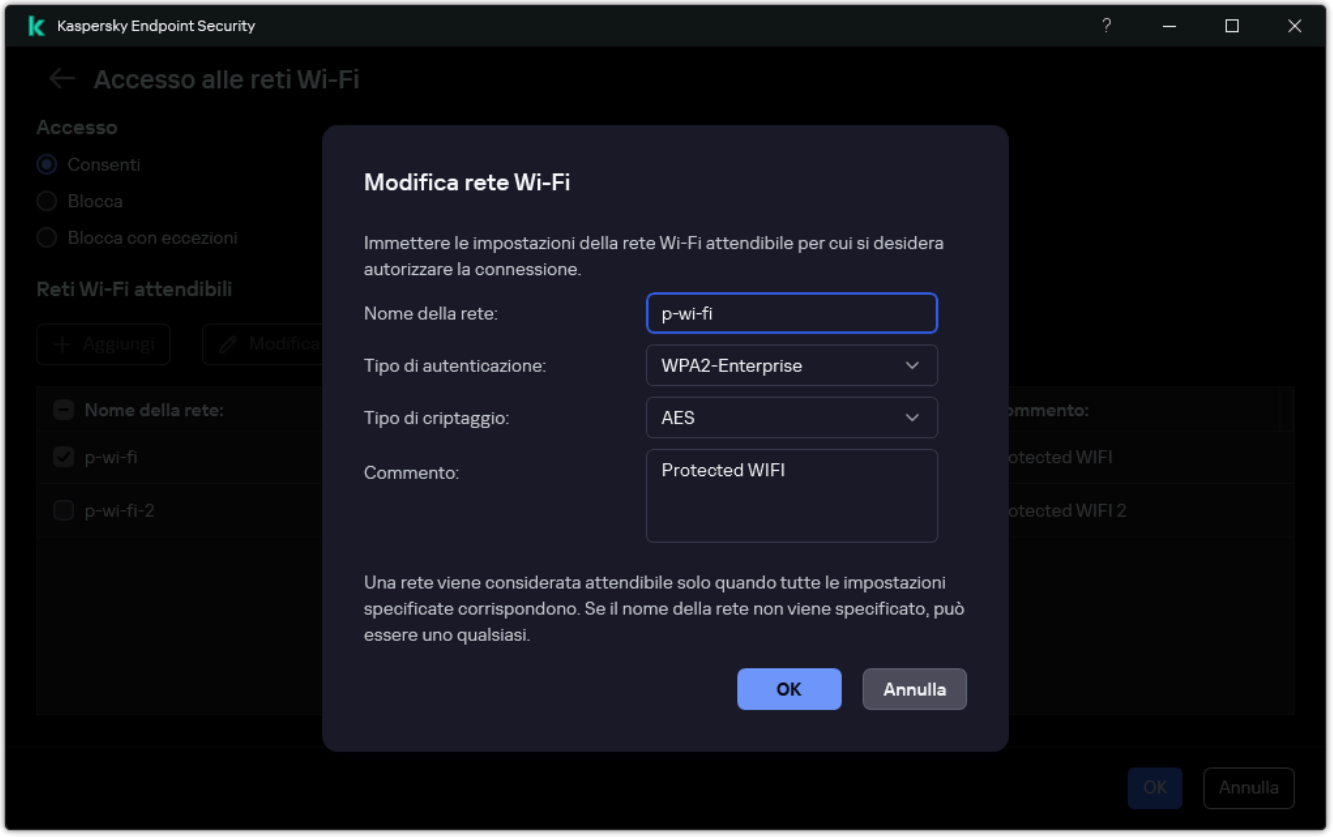
     A partire da Kaspersky Endpoint Security for Windows versione 12.0, all'applicazione è stato aggiunto il supporto del protocollo WPA3. Se a un computer viene applicato un criterio di Kaspersky Endpoint Security versione 12.2, il protocollo WPA2 viene selezionato nei computer con Kaspersky Endpoint Security versione 11.11.0 e precedenti; WPA2/WPA3 viene selezionato per le versioni da 12.0 a 12.1; WPA3 viene selezionato per le versioni 12.2 e successive.

   - **Tipo di criptaggio**. Tipo di criptaggio utilizzato per proteggere il traffico Wi-Fi.
   - **Commento**. Ulteriori informazioni sulla rete Wi-Fi aggiunta.

   È possibile visualizzare le impostazioni della rete Wi-Fi attendibile nelle impostazioni del router.

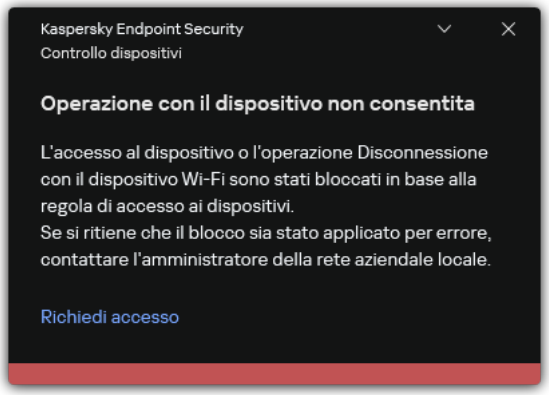
   Una rete Wi-Fi viene considerata attendibile se le relative impostazioni corrispondono a tutte le impostazioni specificate nella regola.

7. Salvare le modifiche.



Impostazioni di rete Wi-Fi attendibile

Di conseguenza, quando un utente tenta di connettersi a una rete Wi-Fi non elencata come attendibile, l'applicazione blocca la connessione e mostra una notifica (vedere la figura riportata di seguito).



Notifica Controllo dispositivi

Monitoraggio dell'utilizzo delle unità rimovibili

Il monitoraggio dell'utilizzo delle unità rimovibili include:

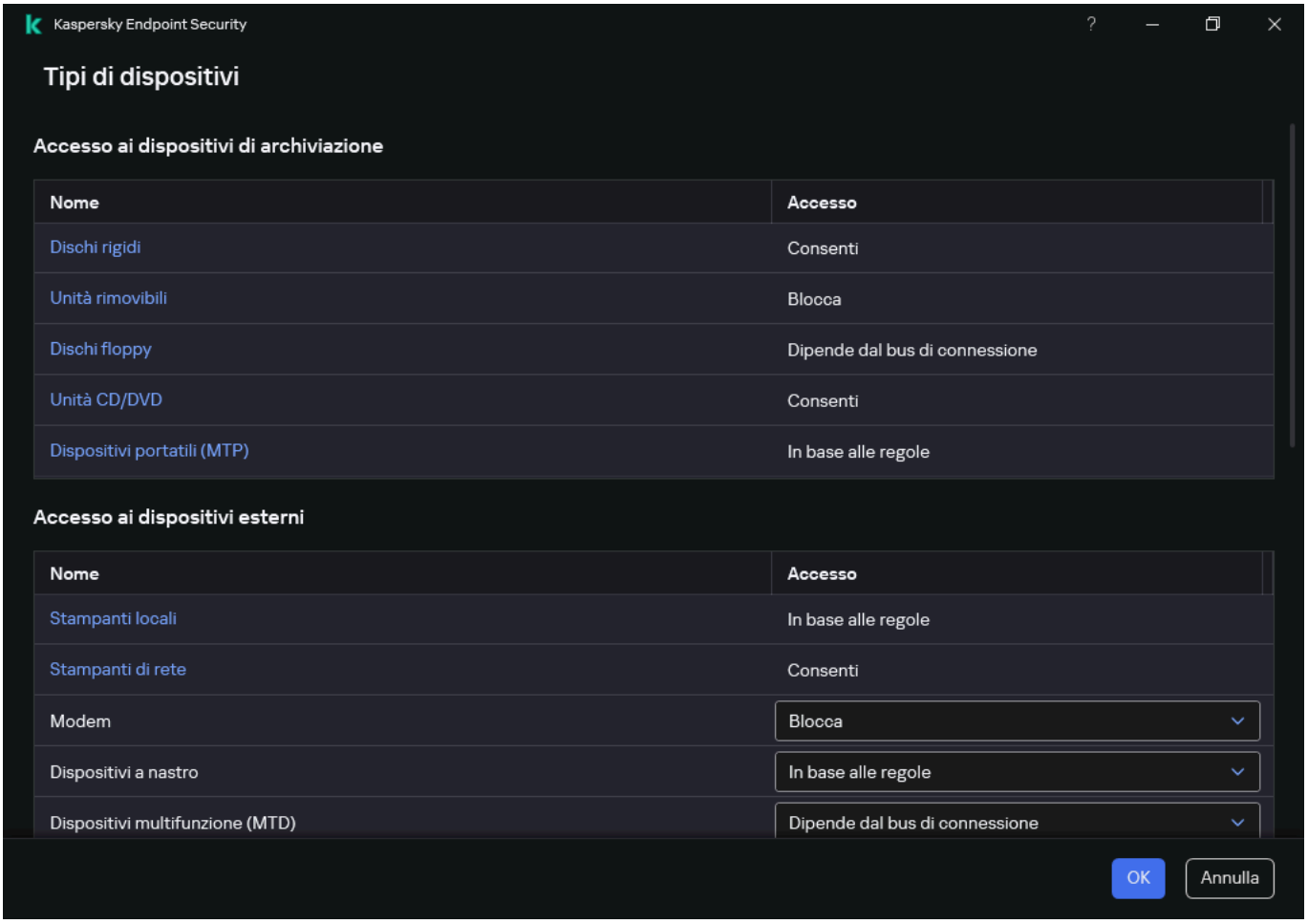
- Il monitoraggio delle operazioni sui file nelle unità rimovibili.
- Il monitoraggio delle connessioni e delle disconnessioni delle unità rimovibili attendibili.

  Kaspersky Endpoint Security consente di monitorare le connessioni e le disconnessioni di tutti i dispositivi attendibili e non solo delle unità rimovibili. È possibile attivare la registrazione degli eventi nelle impostazioni di notifica per il componente Controllo dispositivi. Gli eventi presentano il livello di criticità *Messaggio informativo*.

Per abilitare il monitoraggio dell'utilizzo delle unità rimovibili:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Dispositivi e reti Wi-Fi**.

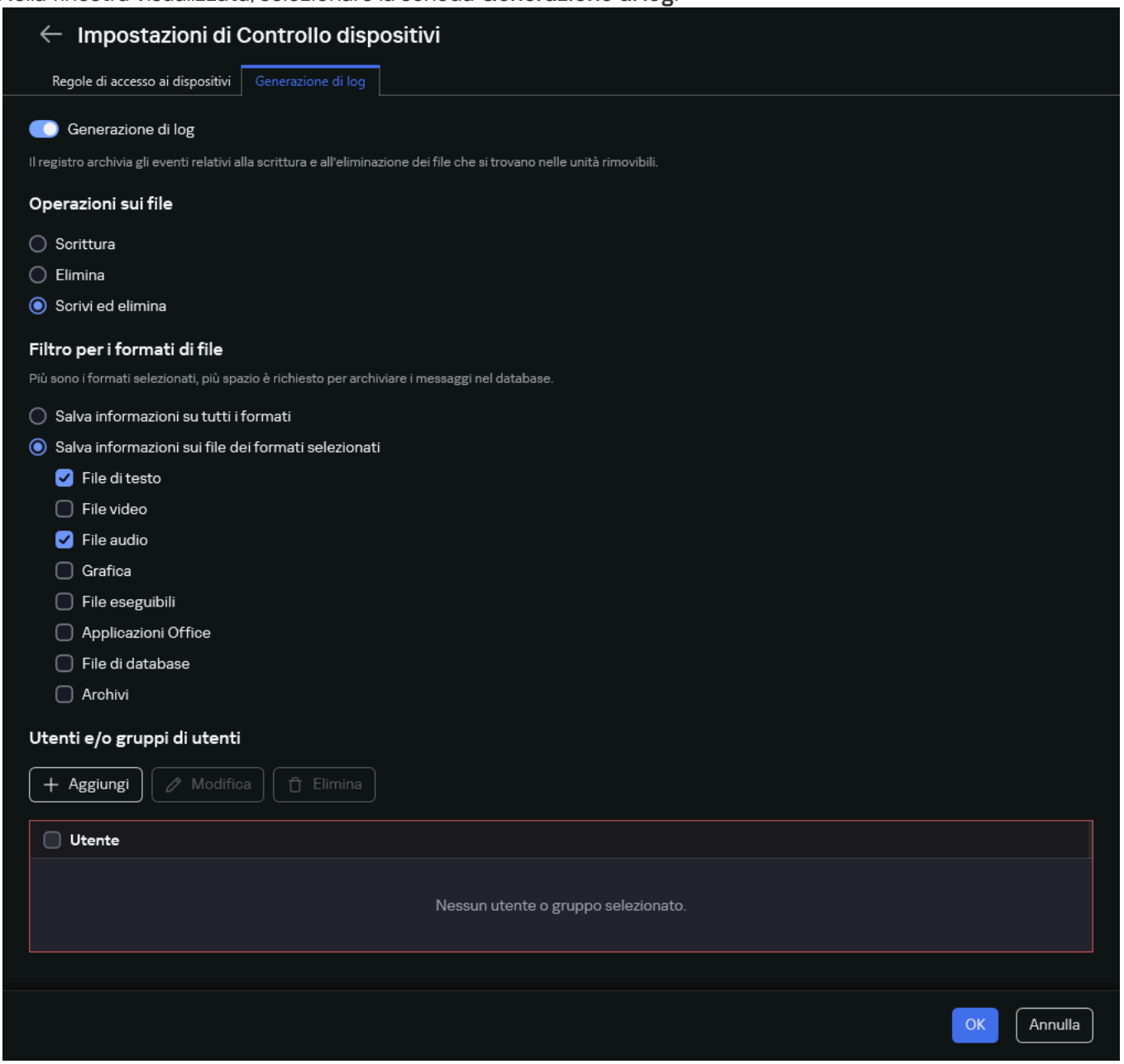
La finestra visualizzata mostra le regole di accesso per tutti i dispositivi inclusi nella classificazione del componente Controllo dispositivi.



Tipi di dispositivi nel componente Controllo dispositivi

4. Nel blocco **Accesso ai dispositivi di archiviazione**, selezionare **Unità rimovibili**.

5. Nella finestra visualizzata, selezionare la scheda **Generazione di log**.



Le impostazioni del monitoraggio dell'utilizzo dell'unità rimovibile

6. Attivare l'interruttore **Generazione di log**.

7. Nel blocco **Operazioni sui file**, selezionare le operazioni che si desidera monitorare: **Scrittura**, **Elimina**.

8. Nella sezione **Filtro per i formati di file** selezionare i formati di file le cui operazioni associate devono essere registrate da Controllo dispositivi.

9. Selezionare gli utenti o il gruppo di utenti di cui si desidera monitorare l'utilizzo delle unità rimovibili.

10. Salvare le modifiche.

Di conseguenza, quando gli utenti eseguono un'operazione di scrittura in file contenuti in unità rimovibili o eliminano file da unità rimovibili, Kaspersky Endpoint Security salva le informazioni su tali operazioni nel registro eventi e invia gli eventi a Kaspersky Security Center. È possibile visualizzare gli eventi associati ai file nelle unità rimovibili in Kaspersky Security Center Administration Console nell'area di lavoro del nodo **Administration Server** nella scheda **Eventi**. Per visualizzare gli eventi nel registro eventi locale di Kaspersky Endpoint Security, è necessario selezionare la casella di controllo **Operazione sul file eseguita** nelle impostazioni delle notifiche per il componente Controllo dispositivi.

Modificare la durata della memorizzazione nella cache

Il componente Controllo dispositivi registra gli eventi relativi ai dispositivi monitorati, come la connessione e la disconnessione di un dispositivo, la lettura di un file da un dispositivo, la scrittura di un file su un dispositivo e altri eventi. Controllo dispositivi quindi consente o blocca l'azione in base alle impostazioni di Kaspersky Endpoint Security.

Controllo dispositivi salva le informazioni sugli eventi per un periodo di tempo specifico chiamato *periodo di memorizzazione nella cache*. Se le informazioni su un evento vengono memorizzate nella cache e questo evento viene ripetuto, non è necessario notificarlo a Kaspersky Endpoint Security o mostrare un'altra richiesta per la concessione dell'accesso all'azione corrispondente, come la connessione di un dispositivo. In questo modo è più comodo utilizzare un dispositivo.

Un evento è considerato un evento duplicato se tutte le seguenti impostazioni dell'evento corrispondono a un record memorizzato nella cache:

- ID dispositivo
- SID dell'account utente che sta tentando di accedere
- Categoria dispositivo
- Azione intrapresa con il dispositivo
- Autorizzazione dell'applicazione per questa azione: consentita o negata
- Percorso del processo utilizzato per eseguire l'azione
- File a cui si accede

Prima di modificare il periodo di memorizzazione nella cache, disabilitare Auto-difesa di Kaspersky Endpoint Security. Dopo aver modificato il periodo di memorizzazione nella cache, abilitare Auto-difesa.

Per modificare il periodo di memorizzazione nella cache:

1. Aprire l'editor del Registro di sistema nel computer.
2. Nell'editor del Registro di sistema passare alla sezione seguente:
   - Per i sistemi operativi a 64 bit:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`
   - Per i sistemi operativi a 32 bit:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`
3. Aprire `DeviceControlEventsCachePeriod` per la modifica.
4. Definire il numero di minuti durante i quali Controllo dispositivi deve salvare le informazioni su un evento prima che queste informazioni vengano eliminate.

Azioni con i dispositivi attendibili

I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile.

Per utilizzare dispositivi attendibili, è possibile concedere l'accesso a un singolo utente, a un gruppo di utenti o a tutti gli utenti dell'organizzazione.

Se ad esempio l'organizzazione non consente l'uso di unità rimovibili ma gli amministratori utilizzano unità rimovibili nelle loro attività, è possibile consentire le unità rimovibili solo per un gruppo di amministratori. A tale scopo, aggiungere unità rimovibili all'elenco delle unità attendibili e configurare le autorizzazioni di accesso dell'utente.

Si sconsiglia di aggiungere più di 5000 dispositivi attendibili, per evitare di causare instabilità di sistema.

Kaspersky Endpoint Security consente di aggiungere un dispositivo all'elenco dei dispositivi attendibili nei seguenti modi:

- Se Kaspersky Security Center non è distribuito nell'organizzazione, è possibile connettere il dispositivo al computer e aggiungerlo all'elenco dei dispositivi attendibili nelle impostazioni dell'applicazione. Per distribuire l'elenco dei dispositivi attendibili in tutti i computer dell'organizzazione, è possibile abilitare l'unione degli elenchi dei dispositivi attendibili in un criterio oppure utilizzare la procedura di esportazione/importazione.

- Se Kaspersky Security Center è distribuito nell'organizzazione, è possibile rilevare tutti i dispositivi connessi in remoto e creare un elenco di dispositivi attendibili nel criterio. L'elenco dei dispositivi attendibili sarà disponibile in tutti i computer a cui viene applicato il criterio.

Kaspersky Endpoint Security consente di controllare l'utilizzo dei dispositivi attendibili (connessione e disconnessione). È possibile attivare la registrazione degli eventi nelle impostazioni di notifica per il componente Controllo dispositivi. Gli eventi presentano il livello di criticità *Messaggi informativi*.

Aggiunta di un dispositivo all'elenco dei dispositivi attendibili

Kaspersky Security Center riceve informazioni sui dispositivi se Kaspersky Endpoint Security è installato nei computer, Controllo dispositivi è abilitato e la trasmissione dei dati del dispositivo è abilitata. Non è possibile aggiungere un dispositivo all'elenco dei dispositivi attendibili a meno che non siano disponibili informazioni sul dispositivo in questione in Kaspersky Security Center.

Per impostazione predefinita, quando si aggiunge un dispositivo all'elenco dei dispositivi attendibili, l'accesso al dispositivo è consentito a tutti gli utenti (il gruppo di utenti Everyone).

È possibile aggiungere un dispositivo all'elenco dei dispositivi attendibili in base ai seguenti dati:

- **Dispositivi per ID**. Ogni dispositivo ha un identificatore univoco (Hardware ID o HWID). È possibile visualizzare l'ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. Esempio di ID dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. L'aggiunta di dispositivi in base all'ID è utile se si desidera aggiungere più dispositivi specifici.

- **Dispositivi per modello**. Ogni dispositivo ha un Vendor ID (VID) e un Product ID (PID). È possibile visualizzare gli ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. Modello per l'immissione di VID e PID: `VID_1234&PID_5678`. L'aggiunta di dispositivi in base al modello è utile se si utilizzano dispositivi di un determinato modello nell'organizzazione. In tal modo è possibile aggiungere tutti i dispositivi di questo modello.

- **Dispositivi per maschera ID**. Se si utilizzano più dispositivi con ID simili, è possibile aggiungere dispositivi all'elenco dei dispositivi attendibili utilizzando le maschere. Il carattere `*` sostituisce qualsiasi set di caratteri. Kaspersky Endpoint Security non supporta il carattere `?` quando si immette una maschera. Ad esempio, `WDC_C*`.

- **Dispositivi per maschera del modello**. Se si utilizzano più dispositivi con VID o PID simili, ad esempio dispositivi dello stesso produttore, è possibile aggiungere dispositivi all'elenco dei dispositivi attendibili utilizzando le maschere. Il carattere `*` sostituisce qualsiasi set di caratteri. Kaspersky Endpoint Security non supporta il carattere `?` quando si immette una maschera. Ad esempio, `VID_05AC&PID_*`.

Come aggiungere un dispositivo all'elenco dei dispositivi attendibili in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
5. Nella parte destra della finestra selezionare la scheda **Dispositivi attendibili**.
6. Selezionare la casella di controllo **Unisci i valori quando vengono ereditati** se si desidera creare un elenco consolidato di dispositivi attendibili per tutti i computer dell'azienda.

   Gli elenchi dei dispositivi attendibili nei criteri padre e figlio verranno uniti. Gli elenchi verranno uniti a condizione che l'unione dei valori durante l'ereditarietà sia abilitata. I dispositivi attendibili del criterio padre vengono visualizzati nei criteri figlio in una visualizzazione di sola lettura. Non è possibile modificare o eliminare i dispositivi attendibili del criterio padre.
7. Fare clic sul pulsante **Aggiungi** e selezionare un metodo per aggiungere un dispositivo all'elenco dei dispositivi attendibili.
8. Per filtrare i dispositivi, selezionare un tipo di dispositivo dall'elenco a discesa **Tipo di dispositivo** (ad esempio **Unità rimovibili**).

   Kaspersky Endpoint Security non supporta l'aggiunta di dispositivi di tipo **Dischi floppy** nell'elenco dei dispositivi attendibili.

9. Nel campo **Nome/Modello** immettere l'ID del dispositivo, il modello (VID e PID) o la maschera, a seconda del metodo di aggiunta selezionato.

   L'aggiunta di dispositivi in base alla maschera del modello (VID e PID) funziona come segue: se si immette una maschera del modello che non corrisponde ad alcun modello, Kaspersky Endpoint Security verifica se l'ID del dispositivo (HWID) corrisponde alla maschera. Kaspersky Endpoint Security controlla solo la parte dell'ID del dispositivo che identifica il produttore e il tipo di dispositivo (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Se la maschera del modello corrisponde a questa parte dell'ID del dispositivo, i dispositivi che corrispondono alla maschera verranno aggiunti all'elenco dei dispositivi attendibili sul computer. Allo stesso tempo, l'elenco dei dispositivi in Kaspersky Security Center rimane vuoto quando si fa clic sul pulsante **Upgrade**. Per visualizzare correttamente l'elenco dei dispositivi, è possibile aggiungere dispositivi tramite la maschera dell'ID del dispositivo.

10. Per filtrare i dispositivi, nel campo **Computer**, immettere il nome del computer o una maschera per il nome del computer a cui è collegato il dispositivo.

    Il carattere `*` sostituisce qualsiasi set di caratteri. Il carattere `?` sostituisce qualsiasi carattere singolo.

11. Fare clic su **Upgrade**.

    La tabella visualizza un elenco dei dispositivi che soddisfano i criteri di filtro definiti.

12. Selezionare le caselle di controllo accanto ai nomi dei dispositivi da aggiungere all'elenco dei dispositivi attendibili.

13. Nel campo **Commento** immettere una descrizione del motivo dell'aggiunta di dispositivi all'elenco dei dispositivi attendibili.

14. Fare clic sul pulsante **Seleziona** a destra del campo **Consenti a utenti e/o gruppi di utenti**.

    È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

    Per impostazione predefinita, l'accesso ai dispositivi attendibili è consentito per il gruppo Tutti.

15. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come aggiungere un dispositivo all'elenco dei dispositivi attendibili in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare alla sezione **Area attendibile**.

5. Nella finestra visualizzata, fare clic sul collegamento **Dispositivi**.

   Verrà visualizzata una finestra contenente un elenco di dispositivi attendibili.

6. Nella parte destra della finestra selezionare la scheda **Dispositivi attendibili**.

7. Selezionare la casella di controllo **Unisci i valori quando vengono ereditati** se si desidera creare un elenco consolidato di dispositivi attendibili per tutti i computer dell'azienda.

   Gli elenchi dei dispositivi attendibili nei criteri padre e figlio verranno uniti. Gli elenchi verranno uniti a condizione che l'unione dei valori durante l'ereditarietà sia abilitata. I dispositivi attendibili del criterio padre vengono visualizzati nei criteri figlio in una visualizzazione di sola lettura. Non è possibile modificare o eliminare i dispositivi attendibili del criterio padre.

8. Fare clic su **Aggiungi**.

   Verrà aperto il modulo per l'aggiunta di un dispositivo attendibile.

9. In **Utente o gruppo**, selezionare gli utenti a cui si desidera consentire l'accesso ai dispositivi attendibili.

   È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

   Per impostazione predefinita, l'accesso ai dispositivi attendibili è consentito per il gruppo Tutti.

10. Per filtrare i dispositivi, selezionare un tipo di dispositivo dall'elenco a discesa **Tipo di dispositivo** (ad esempio **Unità rimovibili**).

    Kaspersky Endpoint Security non supporta l'aggiunta di dispositivi di tipo **Dischi floppy** nell'elenco dei dispositivi attendibili.

11. Se non si conosce l'ID esatto o il modello del dispositivo, selezionare la casella di controllo **Usa maschera**.

12. Selezionare come aggiungere il dispositivo: in base all'ID o al modello del dispositivo (VID e PID).

    L'aggiunta di dispositivi in base alla maschera del modello (VID e PID) funziona come segue: se si immette una maschera del modello che non corrisponde ad alcun modello, Kaspersky Endpoint Security verifica se l'ID del dispositivo (HWID) corrisponde alla maschera. Kaspersky Endpoint Security controlla solo la parte dell'ID del dispositivo che identifica il produttore e il tipo di dispositivo (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Se la maschera del modello corrisponde a questa parte dell'ID del dispositivo, i dispositivi che corrispondono alla maschera verranno aggiunti all'elenco dei dispositivi attendibili sul computer. Contemporaneamente, in Kaspersky Security Center verrà visualizzato l'elenco vuoto dei dispositivi. Per visualizzare correttamente l'elenco dei dispositivi, è possibile aggiungere dispositivi tramite la maschera dell'ID del dispositivo.

13. Per filtrare i dispositivi, nel campo **Cerca dispositivi attendibili**, immettere il nome del computer o una maschera per il nome del computer a cui è collegato il dispositivo.

    Il carattere `*` sostituisce qualsiasi set di caratteri. Il carattere `?` sostituisce qualsiasi carattere singolo.

    La tabella visualizza un elenco dei dispositivi che soddisfano i criteri di filtro definiti.

14. Selezionare le caselle di controllo accanto ai nomi dei dispositivi da aggiungere all'elenco dei dispositivi attendibili.

15. Nel campo **Commento** immettere una descrizione del motivo dell'aggiunta di dispositivi all'elenco dei dispositivi attendibili.

16. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come aggiungere un dispositivo all'elenco dei dispositivi attendibili nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Dispositivi attendibili**.

   Verrà visualizzato l'elenco dei dispositivi attendibili.
4. Fare clic su **Seleziona**.

   Verrà visualizzato l'elenco dei dispositivi connessi. L'elenco dei dispositivi dipende dal valore selezionato nell'elenco a discesa **Visualizza dispositivi connessi**.
5. Nell'elenco dei dispositivi selezionare il dispositivo che si desidera aggiungere all'elenco dei dispositivi attendibili.

   Kaspersky Endpoint Security non supporta l'aggiunta di dispositivi di tipo **Dischi floppy** nell'elenco dei dispositivi attendibili.
6. Nel campo **Commento** è possibile fornire qualsiasi informazione pertinente sul dispositivo attendibile.
7. Selezionare gli utenti o i gruppi di utenti a cui si desidera consentire l'accesso ai dispositivi attendibili.

   È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.
8. Salvare le modifiche.

Quando un dispositivo è collegato, Kaspersky Endpoint Security controlla l'elenco dei dispositivi attendibili per un utente autorizzato. Se il dispositivo è attendibile, Kaspersky Endpoint Security consente l'accesso al dispositivo con tutte le autorizzazioni, anche se viene negato l'accesso al tipo di dispositivo o al bus di connessione. Se il dispositivo non è attendibile e l'accesso è negato, è possibile richiedere l'accesso al dispositivo bloccato.

Esportazione e importazione dell'elenco dei dispositivi attendibili

Per distribuire l'elenco dei dispositivi attendibili a tutti i computer dell'organizzazione, è possibile utilizzare la procedura di esportazione/importazione.

Se è ad esempio necessario distribuire un elenco di unità rimovibili attendibili, procedere come segue:

1. Collegare in sequenza le unità rimovibili al computer.
2. Nelle impostazioni di Kaspersky Endpoint Security aggiungere le unità rimovibili all'elenco delle unità attendibili. Se necessario, configurare le autorizzazioni di accesso dell'utente. Consentire ad esempio solo agli amministratori di accedere alle unità rimovibili.
3. Esportare l'elenco dei dispositivi attendibili nelle impostazioni di Kaspersky Endpoint Security (vedere le istruzioni di seguito).

4. Distribuire il file dell'elenco dei dispositivi attendibili in altri computer dell'organizzazione. Posizionare ad esempio il file in una cartella condivisa.

5. Importare l'elenco dei dispositivi attendibili nelle impostazioni di Kaspersky Endpoint Security negli altri computer dell'organizzazione (vedere le istruzioni di seguito).

Per importare o esportare l'elenco dei dispositivi attendibili:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.

3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Dispositivi attendibili**.

   Verrà visualizzato l'elenco dei dispositivi attendibili.

4. Per esportare l'elenco dei dispositivi attendibili:

   a. Selezionare i dispositivi attendibili che si desidera esportare.

   b. Fare clic su **Esporta**.

   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco dei dispositivi attendibili e selezionare la cartella in cui si desidera salvare il file.

   d. Salvare il file.

      Kaspersky Endpoint Security esporta l'intero elenco dei dispositivi attendibili nel file XML.

5. Per importare l'elenco dei dispositivi attendibili:

   a. Nell'elenco a discesa **Importa**, selezionare l'azione pertinente: **Importa e aggiungi a esistente** o **Importa e sostituisci esistente**.

   b. Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco dei dispositivi attendibili.

   c. Aprire il file.

6. Salvare le modifiche.

Quando un dispositivo è collegato, Kaspersky Endpoint Security controlla l'elenco dei dispositivi attendibili per un utente autorizzato. Se il dispositivo è attendibile, Kaspersky Endpoint Security consente l'accesso al dispositivo con tutte le autorizzazioni, anche se viene negato l'accesso al tipo di dispositivo o al bus di connessione.

Ottenimento dell'accesso a un dispositivo bloccato

Quando si configura Controllo dispositivi, è possibile bloccare per errore l'accesso a un dispositivo necessario.

Se Kaspersky Security Center non è distribuito nell'organizzazione dell'utente, è possibile fornire l'accesso a un dispositivo nelle impostazioni di Kaspersky Endpoint Security. È ad esempio possibile aggiungere il dispositivo all'elenco dei dispositivi attendibili o disabilitare Controllo dispositivi temporaneamente.

Se Kaspersky Security Center è distribuito nell'organizzazione ed è stato applicato un criterio ai computer, è possibile fornire l'accesso a un dispositivo in Administration Console.

Modalità online per la concessione dell'accesso

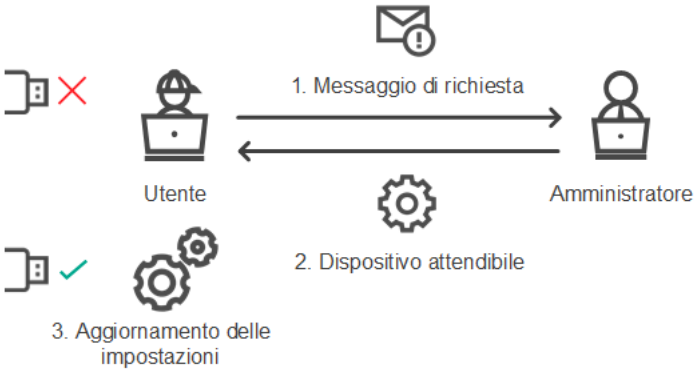
È possibile concedere l'accesso a un dispositivo bloccato in modalità online solo se Kaspersky Security Center è distribuito nell'organizzazione ed è stato applicato un criterio al computer. Il computer deve essere in grado di stabilire una connessione con Administration Server.

La concessione dell'accesso in modalità online prevede i seguenti passaggi:

1. L'utente invia all'amministratore un messaggio contenente una richiesta di accesso.
2. L'amministratore riceve un messaggio con la richiesta nella console di Kaspersky Security Center.

   La console di Kaspersky Security Center dispone di una selezione di eventi preimpostata *Richieste utente* per semplificare il monitoraggio dei messaggi degli utenti.
3. L'amministratore aggiunge il dispositivo all'elenco dei dispositivi attendibili.

   È possibile aggiungere un dispositivo attendibile in un criterio per il gruppo di amministrazione o nelle impostazioni locali dell'applicazione per un singolo computer.
4. L'amministratore aggiorna le impostazioni di Kaspersky Endpoint Security nel computer dell'utente.



Schema per la concessione dell'accesso a un dispositivo in modalità online

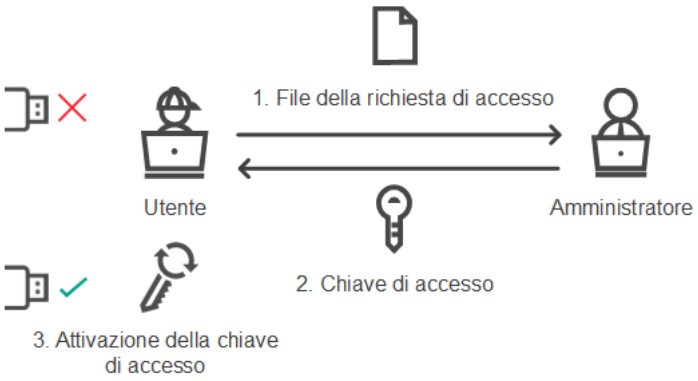
Modalità offline per la concessione dell'accesso

È possibile concedere l'accesso a un dispositivo bloccato in modalità offline solo se Kaspersky Security Center è distribuito nell'organizzazione ed è stato applicato un criterio al computer. Nella sezione **Controllo dispositivi** delle impostazioni dei criteri, la casella di controllo **Consenti richieste di accesso temporaneo** deve essere selezionata.

Se si desidera concedere l'accesso temporaneo a un dispositivo bloccato ma non è possibile aggiungere il dispositivo all'elenco dei dispositivi affidabili, è possibile concedere l'accesso al dispositivo in modalità offline. In questo modo è possibile garantire l'accesso a un dispositivo bloccato anche se il computer non ha accesso alla rete o se il computer si trova all'esterno della rete aziendale.

La concessione dell'accesso in modalità offline prevede i seguenti passaggi:

1. L'utente crea un file della richiesta di accesso e lo invia all'amministratore.
2. L'amministratore crea una chiave di accesso dal file della richiesta di accesso e la invia all'utente.
3. L'utente attiva la chiave di accesso.



Schema per la concessione dell'accesso a un dispositivo in modalità offline

Modalità online per la concessione dell'accesso

È possibile concedere l'accesso a un dispositivo bloccato in modalità online solo se Kaspersky Security Center è distribuito nell'organizzazione ed è stato applicato un criterio al computer. Il computer deve essere in grado di stabilire una connessione con Administration Server.

Un utente richiede l'accesso a un dispositivo bloccato nel seguente modo:

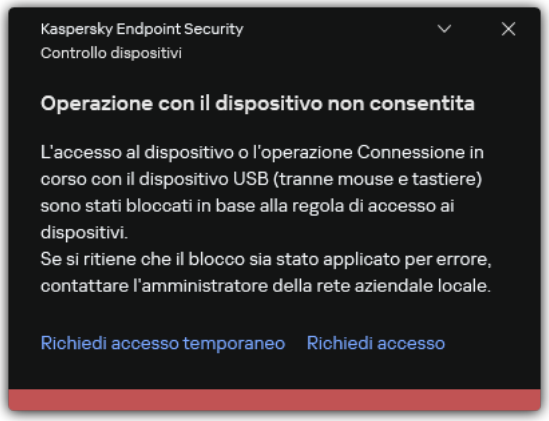
1. Connettere il dispositivo al computer.

   Kaspersky Endpoint Security mostrerà una notifica in cui viene indicato che l'accesso al dispositivo è bloccato (vedere la figura di seguito).

2. Fare clic sul collegamento **Richiedi accesso**.

   Viene visualizzata una finestra con un messaggio per l'amministratore. Questo messaggio contiene le informazioni sul dispositivo bloccato.

3. Fare clic su **Invia**.



Notifica Controllo dispositivi

Successivamente, l'amministratore nella console di Kaspersky Security Center riceve l'evento *Messaggio all'amministratore per il blocco dell'accesso a un dispositivo*. L'evento include il nome utente, il nome del computer, i dettagli del dispositivo a cui l'utente sta tentando di accedere e altre informazioni. È possibile configurare il modo in cui l'amministratore viene informato di tali eventi e, ad esempio, selezionare le notifiche e-mail. La console di Kaspersky Security Center dispone di una selezione di eventi preimpostata *Richieste utente* per semplificare il monitoraggio dei messaggi degli utenti.

Per consentire l'accesso, è necessario aggiungere il dispositivo all'elenco di elementi attendibili. Dopo aver aggiornato le impostazioni di Kaspersky Endpoint Security nel computer, l'utente può accedere al dispositivo.

Modalità offline per la concessione dell'accesso

È possibile concedere l'accesso a un dispositivo bloccato in modalità offline solo se Kaspersky Security Center è distribuito nell'organizzazione ed è stato applicato un criterio al computer. Nella sezione **Controllo dispositivi** delle impostazioni dei criteri, la casella di controllo **Consenti richieste di accesso temporaneo** deve essere selezionata.

Un utente richiede l'accesso a un dispositivo bloccato nel seguente modo:

1. Connettere il dispositivo al computer.

   Kaspersky Endpoint Security mostrerà una notifica in cui viene indicato che l'accesso al dispositivo è bloccato (vedere la figura di seguito).

2. Fare clic sul collegamento **Richiedi accesso temporaneo**.

   Verrà visualizzata una finestra contenente un elenco dei dispositivi connessi.

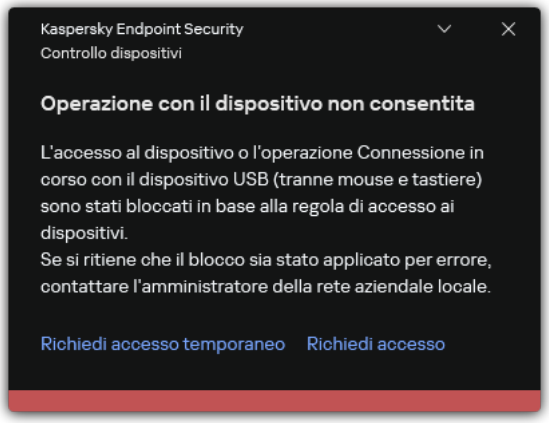
3. Nell'elenco dei dispositivi connessi selezionare il dispositivo per cui si desidera ottenere l'accesso.

4. Fare clic su **Genera file della richiesta di accesso**.

5. Nel campo **Durata accesso** specificare il periodo di tempo per cui si desidera avere accesso al dispositivo.

6. Salvare il file nella memoria del computer.

   Successivamente un file della richiesta di accesso con l'estensione *.akey verrà scaricato nella memoria del computer. Utilizzare uno dei metodi disponibili per inviare il file della richiesta di accesso al dispositivo all'amministratore della LAN aziendale.



Notifica Controllo dispositivi

In che modo l'amministratore può creare una chiave di accesso per il dispositivo bloccato in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, aprire la cartella con il nome del gruppo di amministrazione a cui appartiene il computer client pertinente.
3. Nell'area di lavoro, selezionare la scheda **Dispositivi**.
4. Nell'elenco dei computer client, selezionare il computer relativo all'utente a cui è necessario concedere l'accesso temporaneo al dispositivo bloccato.
5. Nel menu di scelta rapida del computer, selezionare la voce **Concedi l'accesso in modalità offline**.
6. Viene visualizzata una finestra, che consente di selezionare la scheda **Controllo dispositivi**.
7. Fare clic sul pulsante **Sfoglia** e scaricare il file della richiesta di accesso ricevuto dall'utente.

   Verranno visualizzate le informazioni sul dispositivo bloccato al quale l'utente ha richiesto l'accesso.
8. Se necessario, modificare il valore dell'impostazione **Durata accesso**.

   Per impostazione predefinita, l'impostazione **Durata accesso** assume il valore indicato dall'utente durante la creazione del file della richiesta di accesso.
9. Specificare il valore dell'impostazione **Attiva tramite**.

   Questa impostazione definisce il periodo di tempo per cui l'utente può attivare l'accesso al dispositivo bloccato con la chiave di accesso fornita.
10. Salvare il file della chiave di accesso nella memoria del computer.

In che modo l'amministratore può creare una chiave di accesso per il dispositivo bloccato in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Nell'elenco dei computer client, selezionare il computer relativo all'utente a cui è necessario concedere l'accesso temporaneo al dispositivo bloccato.
3. Fare clic sul pulsante con i puntini di sospensione (...) sopra l'elenco dei computer, quindi fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.
4. Nella finestra visualizzata, selezionare la sezione **Controllo dispositivi**.
5. Fare clic sul pulsante **Panoramica** e scaricare il file della richiesta di accesso ricevuto dall'utente.

   Verranno visualizzate le informazioni sul dispositivo bloccato al quale l'utente ha richiesto l'accesso.
6. Se necessario, modificare il valore dell'impostazione **Durata accesso (ore)**.

   Per impostazione predefinita, l'impostazione **Durata accesso (ore)** assume il valore indicato dall'utente durante la creazione del file della richiesta di accesso.

7. Specificare il periodo di tempo durante il quale la chiave di accesso può essere attivata sul dispositivo.

   Questa impostazione definisce il periodo di tempo per cui l'utente può attivare l'accesso al dispositivo bloccato con la chiave di accesso fornita.

8. Salvare il file della chiave di accesso nella memoria del computer.

Di conseguenza, la chiave di accesso al dispositivo bloccato verrà scaricata nella memoria del computer. Il file di una chiave di accesso ha l'estensione *.acode. Utilizzare uno dei metodi disponibili per inviare la chiave di accesso al dispositivo bloccato all'utente.

L'utente attiva la chiave di accesso nel seguente modo:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nel blocco **Richiesta di accesso**, fare clic sul pulsante **Richiedi accesso al dispositivo**.
4. Nella finestra visualizzata, fare clic sul pulsante **Attiva chiave di accesso**.
5. Nella finestra visualizzata, selezionare il file con la chiave di accesso al dispositivo ricevuta dall'amministratore della LAN aziendale.

   Viene aperta una finestra contenente le informazioni sulla concessione dell'accesso.

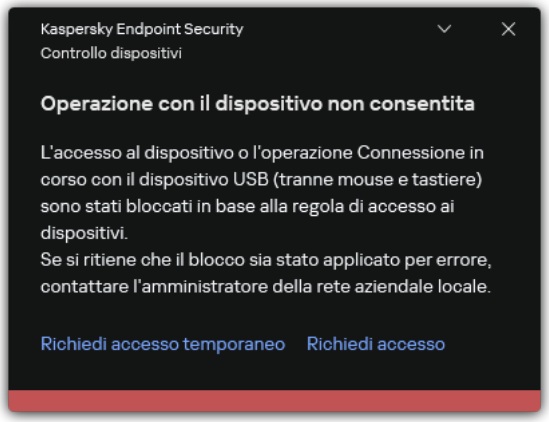
6. Fare clic su **OK**.

Successivamente l'utente riceve l'accesso al dispositivo per il periodo di tempo impostato dall'amministratore. L'utente riceve il set completo di diritti per l'accesso al dispositivo (lettura e scrittura). Allo scadere della chiave, l'accesso al dispositivo verrà bloccato. Se l'utente richiede l'accesso permanente al dispositivo, aggiungere il dispositivo all'elenco dei dispositivi attendibili.

Modifica dei modelli dei messaggi di Controllo dispositivi

Quando l'utente tenta di accedere a un dispositivo bloccato, Kaspersky Endpoint Security visualizza un messaggio segnalando che l'accesso al dispositivo è bloccato o che un'operazione con il contenuto del dispositivo è vietata. Gli esperti di Kaspersky forniscono un modello di messaggio per l'utente in cui vengono descritti i motivi per cui è stato bloccato l'accesso al dispositivo (vedere la figura seguente).

Sono disponibili variabili speciali per la gestione del modello di messaggio (ad esempio `%USER_NAME%`). Le variabili consentono di utilizzare un unico modello di messaggio per computer diversi. Quando si genera un messaggio, Kaspersky Endpoint Security recupera il valore della variabile dalle impostazioni del sistema operativo e lo inserisce nel messaggio corrispondente al computer, all'utente e all'evento specifici.



Notifica Controllo dispositivi

Se l'utente ritiene che l'accesso al dispositivo sia stato bloccato (o che un'operazione con il contenuto del dispositivo sia stata vietata) per errore, può inviare un messaggio all'amministratore della rete aziendale locale facendo clic sul collegamento nel messaggio sull'azione bloccata visualizzato. A tale scopo, l'utente deve fare clic sui pulsanti **Richiedi accesso** o **Richiedi accesso temporaneo** e inviare un messaggio all'amministratore descrivendo la situazione. È inoltre possibile preparare un modello per il messaggio per l'amministratore, aggiungendovi dati che potrebbero aiutare a decidere se consentire o bloccare l'accesso al dispositivo. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'accesso a un dispositivo**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato.

Come modificare i modelli di messaggio di Controllo dispositivi in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
4. Nel blocco **Impostazioni dei modelli di messaggio**, fare clic sul pulsante **Modelli**.
5. Viene visualizzata una finestra; in tale finestra, configurare i modelli di Controllo applicazioni:

   - **Messaggio relativo al blocco**. Modello del messaggio visualizzato quando un utente tenta di accedere a un dispositivo bloccato. Questo messaggio viene visualizzato anche quando un utente tenta di eseguire un'operazione sui contenuti del dispositivo bloccata per questo utente.
   - **Messaggio all'amministratore**. Un modello del messaggio inviato all'amministratore della rete LAN quando l'utente ritiene che l'accesso al dispositivo sia stato bloccato o che un'operazione relativa ai contenuti del dispositivo sia stata vietata per errore.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

È anche possibile ripristinare il testo del modello predefinito.

6. Salvare le modifiche.

Come modificare i modelli di messaggio di Controllo dispositivi in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo dispositivi**.
5. Nel blocco **Modelli di messaggi**, configurare i modelli per i messaggi di Controllo applicazioni:

   - **Messaggio all'utente**. Modello del messaggio visualizzato quando un utente tenta di accedere a un dispositivo bloccato. Questo messaggio viene visualizzato anche quando un utente tenta di eseguire un'operazione sui contenuti del dispositivo bloccata per questo utente.
   - **Messaggio all'amministratore**. Un modello del messaggio inviato all'amministratore della rete LAN quando l'utente ritiene che l'accesso al dispositivo sia stato bloccato o che un'operazione relativa ai contenuti del dispositivo sia stata vietata per errore.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Aggiungi variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

   È anche possibile ripristinare il testo del modello predefinito.
6. Salvare le modifiche.

Come modificare i modelli di messaggio di Controllo dispositivi nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
3. Nel blocco **Modelli di messaggi**, configurare i modelli per i messaggi di Controllo applicazioni:

   - **Messaggio relativo al blocco**. Modello del messaggio visualizzato quando un utente tenta di accedere a un dispositivo bloccato. Questo messaggio viene visualizzato anche quando un utente tenta di eseguire un'operazione sui contenuti del dispositivo bloccata per questo utente.
   - **Messaggio all'amministratore**. Un modello del messaggio inviato all'amministratore della rete LAN quando l'utente ritiene che l'accesso al dispositivo sia stato bloccato o che un'operazione relativa ai contenuti del dispositivo sia stata vietata per errore.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Aggiungi variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

   È anche possibile ripristinare il testo del modello predefinito.
4. Salvare le modifiche.

Anti-Bridging

Anti-Bridging inibisce la creazione di bridge di rete impedendo la creazione simultanea di più connessioni di rete per un computer. Questo consente di proteggere una rete aziendale dagli attacchi su reti non protette e non autorizzate.

Anti-Bridging regola la creazione di connessioni di rete mediante *regole di connessione*.

Le regole di connessione vengono create per i seguenti tipi di dispositivi predefiniti:

- Schede di rete;
- Schede di rete Wi-Fi;
- Modem.

Se viene abilitata una regola di connessione, Kaspersky Endpoint Security:

- Blocca la connessione attiva quando viene stabilita una nuova connessione, se il tipo di dispositivo specificato nella regola è utilizzato per entrambe le connessioni;
- Blocca le connessioni stabilite tramite i tipi di dispositivi per cui vengono utilizzate le regole con priorità inferiore.

Abilitazione di Anti-Bridging

Anti-Bridging è disabilitato per impostazione predefinita.

Per abilitare Anti-Bridging:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Anti-Bridging**.
4. Utilizzare l'interruttore **Abilita Anti-Bridging** per abilitare o disabilitare questa funzionalità.
5. Salvare le modifiche.

In seguito all'abilitazione di Anti-Bridging, Kaspersky Endpoint Security blocca le connessioni già stabilite in base alle regole di connessione.

Modifica dello stato di una regola di connessione

Per modificare lo stato di una regola di connessione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.

3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Anti-Bridging**.
4. Nella sezione **Regole per i dispositivi** selezionare la regola di cui si desidera modificare lo stato.
5. Utilizzare gli interruttori nella colonna **Controllo** per abilitare o disabilitare la regola.
6. Salvare le modifiche.

Modificare la priorità di una regola di connessione

Per modificare la priorità di una regola di connessione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
3. Nel blocco **Impostazioni di accesso**, fare clic sul pulsante **Anti-Bridging**.
4. Nella sezione **Regole per i dispositivi** selezionare la regola di cui desideri modificare la priorità.
5. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di connessione.

   Più alta è la posizione di una regola nella tabella delle regole, maggiore è la sua priorità. Anti-Bridging blocca tutte le connessioni ad eccezione di una connessione stabilita utilizzando il tipo di dispositivo per cui viene utilizzata la regola con la priorità più elevata.
6. Salvare le modifiche.

Controllo adattivo delle anomalie

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server.

Il componente Controllo adattivo delle anomalie monitora e blocca le azioni non tipiche dei computer in una rete aziendale. Controllo adattivo delle anomalie utilizza un set di regole per monitorare i comportamenti non tipici (ad esempio, la regola *Avvio di Microsoft PowerShell dall'applicazione Office*). Le regole vengono create dagli esperti di Kaspersky in base agli scenari tipici delle attività dannose. È possibile configurare la modalità di gestione di ogni regola da parte di Controllo adattivo delle anomalie e, ad esempio, consentire l'esecuzione degli script PowerShell per l'automazione di determinate attività del flusso di lavoro. Kaspersky Endpoint Security aggiorna il set di regole insieme ai database dell'applicazione. Gli aggiornamenti dei set di regole devono essere confermati manualmente.

Impostazioni di Controllo adattivo delle anomalie

La configurazione di Controllo adattivo delle anomalie prevede i seguenti passaggi:

1. Addestramento di Controllo adattivo delle anomalie.

In seguito all'attivazione di Controllo adattivo delle anomalie, le relative regole vengono eseguite in *modalità addestramento*. Durante l'addestramento, Controllo adattivo delle anomalie monitora l'attivazione delle regole e invia gli eventi di attivazione a Kaspersky Security Center. Ogni regola ha una durata specifica per la modalità di addestramento. La durata della modalità di addestramento è impostata dagli esperti di Kaspersky. In genere, la modalità di addestramento è attiva per due settimane.

Se una regola non è attivata durante l'addestramento, Controllo adattivo delle anomalie considererà non tipiche le azioni associate a tale regola. Kaspersky Endpoint Security bloccherà tutte le azioni associate alla regola.

Se è stata attivata una regola durante l'addestramento, Kaspersky Endpoint Security registra gli eventi nel rapporto sull'attivazione delle regole e nell'archivio **Attivazioni di regole nello stato Smart Training**.

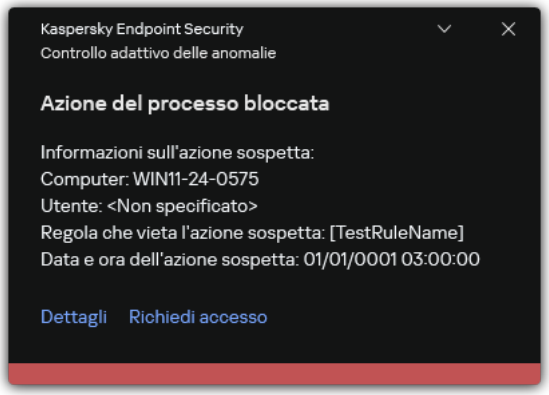
2. Analisi del rapporto sull'attivazione delle regole.

   L'amministratore analizza il rapporto sull'attivazione delle regole o i contenuti dell'archivio **Attivazioni di regole nello stato Smart Training**. L'amministratore può quindi selezionare il comportamento di Controllo adattivo delle anomalie quando viene attivata la regola, scegliendo se bloccarla o consentirla. L'amministratore può inoltre continuare a monitorare la modalità di esecuzione della regola e prolungare la durata della modalità addestramento. Se l'amministratore non esegue alcuna azione, anche l'applicazione continuerà a funzionare in modalità addestramento. Il periodo della modalità addestramento viene riavviato.

Controllo adattivo delle anomalie viene configurato in tempo reale tramite i seguenti canali:

- Controllo adattivo delle anomalie inizia automaticamente a bloccare le azioni associate alle regole che non sono mai state attivate in modalità addestramento.
- Kaspersky Endpoint Security aggiunge nuove regole oppure rimuove quelle obsolete.
- L'amministratore configura l'esecuzione di Controllo adattivo delle anomalie dopo l'analisi del rapporto sull'attivazione delle regole e dei contenuti dell'archivio **Attivazioni di regole nello stato Smart Training**. È consigliabile controllare il rapporto sull'attivazione delle regole e i contenuti dell'archivio **Attivazioni di regole nello stato Smart Training**.

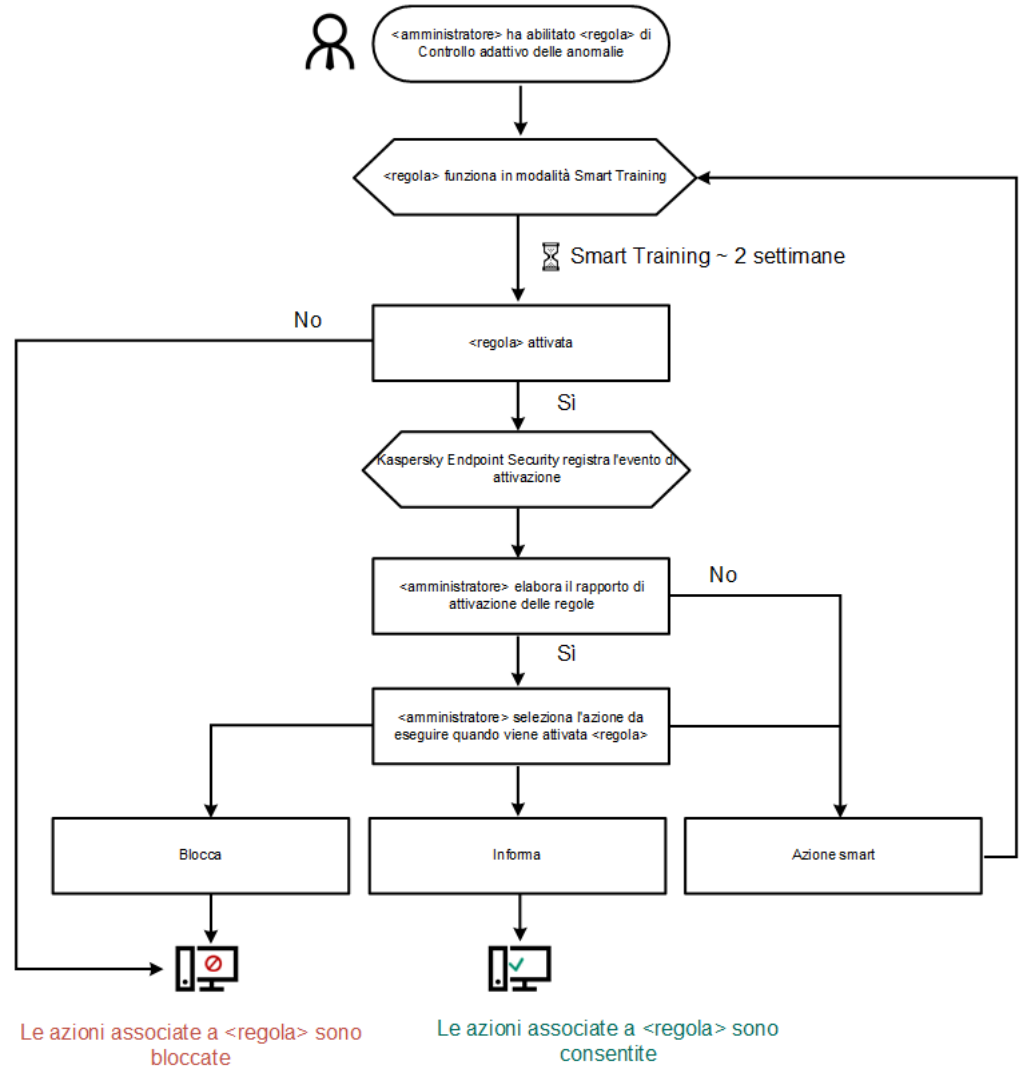
Quando un'applicazione dannosa tenta di eseguire un'azione, Kaspersky Endpoint Security blocca l'azione e visualizza una notifica (vedere la figura seguente).



Notifica di Controllo adattivo delle anomalie

Algoritmo operativo di Controllo adattivo delle anomalie

Kaspersky Endpoint Security decide se consentire o bloccare un'azione associata a una regola in base al seguente algoritmo (vedere la figura seguente).



Algoritmo operativo di Controllo adattivo delle anomalie

Addestramento di Controllo adattivo delle anomalie

Controllo adattivo delle anomalie include un set di regole (modelli di comportamento). In seguito all'attivazione di Controllo adattivo delle anomalie, le relative regole vengono eseguite in *modalità addestramento*. Durante l'addestramento, Controllo adattivo delle anomalie monitora l'attivazione delle regole e invia gli eventi di attivazione a Kaspersky Security Center. Controllo adattivo delle anomalie non blocca le attività delle applicazioni nel computer, ma informa solo l'amministratore. È inoltre possibile selezionare manualmente l'azione eseguita quando viene attivata una regola di Controllo adattivo delle anomalie.

Come visualizzare l'elenco di regole di Controllo adattivo delle anomalie in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.

3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

4. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.

5. Selezionare la casella di controllo **Controllo adattivo delle anomalie**.

6. Sotto **Impostazioni delle regole di Controllo adattivo delle anomalie**, esaminare l'elenco delle regole.

   Per impostazione predefinita, tutte le regole funzionano nella modalità **Azione smart**.

7. Se necessario, confermare l'aggiornamento della regola Controllo adattivo delle anomalie.

8. Se necessario, selezionare un'azione quando viene attivata una regola di Controllo adattivo delle anomalie:

   - **Blocca**. Se si seleziona questa azione, quando viene attivata una regola di Controllo adattivo delle anomalie Kaspersky Endpoint Security blocca l'attività a cui si applica la regola e registra una voce contenente le informazioni sull'attività.

   - **Informa**. Se si seleziona questa azione, quando viene attivata una regola di Controllo adattivo delle anomalie Kaspersky Endpoint Security consente l'attività a cui si applica la regola e registra una voce contenente le informazioni sull'attività.

9. Se necessario, disabilitare le regole che non si desidera utilizzare.

10. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come visualizzare le regole di Controllo adattivo delle anomalie in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.

5. Attivare l'interruttore **Controllo adattivo delle anomalie ABILITATO**.

6. Sotto **Regole**, esaminare l'elenco delle regole.

   Per impostazione predefinita, tutte le regole funzionano nella modalità **Azione smart**.

7. Se necessario, confermare l'aggiornamento della regola Controllo adattivo delle anomalie.

8. Se necessario, selezionare un'azione quando viene attivata una regola di Controllo adattivo delle anomalie:

   - **Blocca**. Se si seleziona questa azione, quando viene attivata una regola di Controllo adattivo delle anomalie Kaspersky Endpoint Security blocca l'attività a cui si applica la regola e registra una voce contenente le informazioni sull'attività.

   - **Informa**. Se si seleziona questa azione, quando viene attivata una regola di Controllo adattivo delle anomalie Kaspersky Endpoint Security consente l'attività a cui si applica la regola e registra una voce contenente le informazioni sull'attività.

9. Se necessario, disabilitare le regole che non si desidera utilizzare.

10. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come visualizzare l'elenco di regole di Controllo adattivo delle anomalie nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.

3. Attivare l'interruttore **Controllo adattivo delle anomalie**.

4. Nella sezione **Regole**, fare clic sul collegamento **Modifica regole**.

   Verrà visualizzato l'elenco delle regole di Controllo adattivo delle anomalie. Per impostazione predefinita, tutte le regole funzionano nella modalità **Azione smart**.

5. Se necessario, confermare l'aggiornamento della regola Controllo adattivo delle anomalie.

6. Se necessario, selezionare un'azione quando viene attivata una regola di Controllo adattivo delle anomalie:

   - **Blocca**. Se si seleziona questa azione, quando viene attivata una regola di Controllo adattivo delle anomalie Kaspersky Endpoint Security blocca l'attività a cui si applica la regola e registra una voce contenente le informazioni sull'attività.

   - **Informa**. Se si seleziona questa azione, quando viene attivata una regola di Controllo adattivo delle anomalie Kaspersky Endpoint Security consente l'attività a cui si applica la regola e registra una voce contenente le informazioni sull'attività.

7. Se necessario, disabilitare le regole che non si desidera utilizzare.

8. Salvare le modifiche.

Ogni regola ha una durata specifica per la modalità di addestramento. La durata della modalità di addestramento è impostata dagli esperti di Kaspersky. In genere, la modalità di addestramento è attiva per due settimane.

Se, durante l'addestramento, una regola non viene mai attivata, Controllo adattivo delle anomalie considera tale comportamento atipico e modifica lo stato della regola in **Blocco intelligente**. Successivamente, l'applicazione blocca qualsiasi attività che corrisponde a questa regola.

Se una regola viene attivata durante l'addestramento, è necessario configurare manualmente l'azione che viene applicata dall'applicazione all'attività rilevata che corrisponde a questa regola. Se non si seleziona l'azione quando la regola viene attivata, Controllo adattivo delle anomalie continua in modalità di addestramento.

Abilitazione e disabilitazione di una regola di Controllo adattivo delle anomalie

Per abilitare o disabilitare una regola di Controllo adattivo delle anomalie:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.

3. Nel blocco **Regole**, fare clic sul pulsante **Modifica regole**.

   Verrà visualizzato l'elenco delle regole di Controllo adattivo delle anomalie.

4. Nella tabella selezionare un set di regole (ad esempio *Attività delle applicazioni Office*) ed espandere il set.

5. Selezionare una regola (ad esempio, *Avvio di Microsoft PowerShell dall'applicazione Office*).

6. Utilizzare l'interruttore nella colonna **Stato** per abilitare o disabilitare la regola di Controllo adattivo delle anomalie.

7. Salvare le modifiche.

Modifica dell'azione eseguita quando viene attivata una regola di Controllo adattivo delle anomalie

Per modificare l'azione eseguita quando viene attivata una regola di Controllo adattivo delle anomalie:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.

3. Nel blocco **Regole**, fare clic sul pulsante **Modifica regole**.

   Verrà visualizzato l'elenco delle regole di Controllo adattivo delle anomalie.

4. Selezionare una regola nella tabella.

5. Fare clic su **Modifica**.

   Verrà visualizzata la finestra delle proprietà delle regole di Controllo adattivo delle anomalie.

6. Nella sezione **Azione** selezionare una delle seguenti opzioni:

   - **Azione smart**. Se questa opzione è selezionata, la regola di Controllo adattivo delle anomalie opera con lo stato Smart Training per un periodo di tempo definito dagli esperti di Kaspersky. In questa modalità, quando viene attivata una regola di Controllo adattivo delle anomalie, Kaspersky Endpoint Security consente l'attività a cui si applica la regola e registra una voce nell'archivio **Attivazioni di regole nello stato Smart Training** di Kaspersky Security Center Administration Server. Al termine del periodo di tempo impostato per l'utilizzo dello stato Smart Training, Kaspersky Endpoint Security blocca l'attività a cui si applica la regola di Controllo adattivo delle anomalie e registra una voce contenente le informazioni sulle attività.

   - **Blocca**. Se si seleziona questa azione, quando viene attivata una regola di Controllo adattivo delle anomalie Kaspersky Endpoint Security blocca l'attività a cui si applica la regola e registra una voce contenente le informazioni sull'attività.

   - **Informa**. Se si seleziona questa azione, quando viene attivata una regola di Controllo adattivo delle anomalie Kaspersky Endpoint Security consente l'attività a cui si applica la regola e registra una voce contenente le informazioni sull'attività.

7. Salvare le modifiche.

Creazione di un'esclusione per una regola di Controllo adattivo delle anomalie

Non è possibile creare più di 1.000 esclusioni per le regole di Controllo adattivo delle anomalie. Non è consigliabile creare più di 200 esclusioni. Per ridurre il numero di esclusioni utilizzate, è consigliabile utilizzare le maschere nelle impostazioni delle esclusioni.

Un'esclusione per una regola di Controllo adattivo delle anomalie include una descrizione degli oggetti di origine e di destinazione. L'*oggetto di origine* è l'oggetto che esegue le azioni. L'*oggetto di destinazione* è l'oggetto in cui vengono eseguite le azioni. È stato ad esempio aperto un file denominato `file.xlsx`. In seguito a questa operazione, viene caricato nella memoria del computer un file della libreria con estensione DLL. Questa libreria è utilizzata da un browser (file eseguibile denominato `browser.exe`). In questo esempio `file.xlsx` è l'oggetto di origine, Excel è il processo di origine, `browser.exe` è l'oggetto di destinazione e Browser è il processo di destinazione.

Per creare un'esclusione per una regola di Controllo adattivo delle anomalie:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.
3. Nel blocco **Regole**, fare clic sul pulsante **Modifica regole**.

   Verrà visualizzato l'elenco delle regole di Controllo adattivo delle anomalie.
4. Selezionare una regola nella tabella.
5. Fare clic su **Modifica**.

   Verrà visualizzata la finestra delle proprietà delle regole di Controllo adattivo delle anomalie.
6. Nel blocco **Esclusioni**, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra delle proprietà delle esclusioni.
7. Selezionare l'utente per cui si desidera configurare un'esclusione.

   È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

   Controllo adattivo delle anomalie non supporta le esclusioni per i gruppi di utenti. Se si seleziona un gruppo di utenti, Kaspersky Endpoint Security non applica l'esclusione.
8. Nel campo **Descrizione** immettere una descrizione dell'esclusione.

9. Definire le impostazioni dell'oggetto di origine o del processo di origine avviato dall'oggetto:

   - **Processo di origine**. Percorso o maschera del percorso del file o della cartella contenente i file (ad esempio, `C:\Dir\File.exe` o `Dir\*.exe`).
   - **Hash processo origine**. Hash SHA256 del file.
   - **Oggetto di origine**. Percorso o maschera del percorso del file o della cartella contenente i file (ad esempio, `C:\Dir\File.exe` o `Dir\*.exe`). Ad esempio il percorso del file `document.docm`, che utilizza uno script o una macro per avviare i processi di destinazione.

     È inoltre possibile specificare altri oggetti da escludere, ad esempio un indirizzo Web, una macro, un comando nella riga di comando, un percorso del registro di sistema o altri elementi. Specificare l'oggetto in base al seguente modello: `object://<object>` dove `<object>` si riferisce al nome dell'oggetto, ad esempio `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. È inoltre possibile utilizzare le maschere, ad esempio `object://*C:\Windows\temp\*`.
   - **Hash oggetto origine**. Hash SHA256 del file.

   La regola di Controllo adattivo delle anomalie non viene applicata alle azioni eseguite dall'oggetto o ai processi avviati dall'oggetto.

10. Specificare le impostazioni dell'oggetto di destinazione o dei processi di destinazione avviati nell'oggetto.

    - **Processo di destinazione**. Percorso o maschera del percorso del file o della cartella contenente i file (ad esempio, `C:\Dir\File.exe` o `Dir\*.exe`).
    - **Hash processo destinazione**. Hash SHA256 del file.
    - **Oggetto di destinazione**. Il comando per avviare il processo di destinazione. Specificare il comando utilizzando il modello seguente `object://<command>`, ad esempio `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. È inoltre possibile utilizzare le maschere, ad esempio `object://*C:\Windows\temp\*`.
    - **Hash oggetto destinazione**. Hash SHA256 del file.

    La regola di Controllo adattivo delle anomalie non viene applicata alle azioni eseguite sull'oggetto o ai processi avviati sull'oggetto.

11. Salvare le modifiche.

Esportazione e importazione delle esclusioni per le regole di Controllo adattivo delle anomalie

Per esportare o importare l'elenco delle esclusioni per le regole selezionate:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.

3. Nel blocco **Regole**, fare clic sul pulsante **Modifica regole**.

   Verrà visualizzato l'elenco delle regole di Controllo adattivo delle anomalie.

4. Per esportare l'elenco delle regole:

   a. Selezionare le regole di cui si desidera esportare le eccezioni.

   b. Fare clic su **Esporta**.

   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle esclusioni e selezionare la cartella in cui si desidera salvare il file.

   d. Confermare di voler esportare solo le esclusioni selezionate o esportare l'intero elenco di esclusioni.

   e. Salvare il file.

5. Per importare l'elenco delle esclusioni:

   a. Fare clic su **Importa**.

   b. Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle esclusioni.

   c. Aprire il file.

      Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

6. Salvare le modifiche.

Applicazione degli aggiornamenti per le regole di Controllo adattivo delle anomalie

È possibile aggiungere nuove regole di Controllo adattivo delle anomalie alla tabella delle regole e le regole di Controllo adattivo delle anomalie esistenti possono essere eliminate dalla tabella delle regole durante l'aggiornamento dei database anti-virus. Kaspersky Endpoint Security distingue le regole di Controllo adattivo delle anomalie che devono essere eliminate o aggiunte alla tabella se non è stato applicato un aggiornamento per queste regole.

Finché non viene applicato l'aggiornamento, Kaspersky Endpoint Security visualizza le regole di Controllo adattivo delle anomalie che verranno eliminate dall'aggiornamento nella tabella delle regole e assegna a tali regole lo stato *Disabilitato*. Non è possibile modificare le impostazioni di queste regole.

Per applicare gli aggiornamenti per le regole di Controllo adattivo delle anomalie:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.

3. Nel blocco **Regole**, fare clic sul pulsante **Modifica regole**.

   Verrà visualizzato l'elenco delle regole di Controllo adattivo delle anomalie.

4. Nella finestra visualizzata, fare clic sul pulsante **Approva aggiornamenti**.

   Il pulsante **Approva aggiornamenti** è disponibile se è disponibile un aggiornamento per le regole di Controllo adattivo delle anomalie.

5. Salvare le modifiche.

Modifica dei modelli dei messaggi di Controllo adattivo delle anomalie

Quando un utente tenta di eseguire un'azione bloccata dalle regole di Controllo adattivo delle anomalie, Kaspersky Endpoint Security visualizza un messaggio per indicare che le azioni potenzialmente dannose sono bloccate. Se l'utente ritiene che un'azione sia stata bloccata per errore, può utilizzare il collegamento nel testo del messaggio per inviare un messaggio all'amministratore della rete aziendale locale.

Sono disponibili modelli speciali per i messaggi all'amministratore in merito al blocco di azioni potenzialmente dannose. Sono disponibili variabili speciali per la gestione del modello di messaggio (ad esempio `%USER_NAME%`). Le variabili consentono di utilizzare un unico modello di messaggio per computer diversi. Quando si genera un messaggio, Kaspersky Endpoint Security recupera il valore della variabile dalle impostazioni del sistema operativo e lo inserisce nel messaggio corrispondente al computer, all'utente e all'evento specifici.

Per modificare un modello di messaggio:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.

3. Nella sezione **Modelli** configurare i modelli per i messaggi di Controllo adattivo delle anomalie:

   - **Messaggio relativo al blocco**. Modello del messaggio visualizzato a un utente quando viene attivata una regola di Controllo adattivo delle anomalie che blocca un'azione non tipica.

   - **Messaggio all'amministratore**. Modello del messaggio che un utente può inviare all'amministratore della rete aziendale locale se l'utente ritiene che il blocco sia un errore. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'attività di un'applicazione**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Aggiungi variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

   È anche possibile ripristinare il testo predefinito del modello utilizzando il pulsante **Reimposta**.

4. Salvare le modifiche.

Monitoraggio delle operazioni di Controllo adattivo delle anomalie

Controllo adattivo delle anomalie include diversi strumenti di monitoraggio. Lo scopo principale del monitoraggio di Controllo adattivo delle anomalie è configurare il componente durante l'addestramento.

Rapporti di Controllo adattivo delle anomalie

Controllo adattivo delle anomalie utilizza i seguenti rapporti:

- **Rapporto sullo stato delle regole di Controllo adattivo delle anomalie**. Il rapporto contiene informazioni sullo stato delle regole di Controllo adattivo delle anomalie (*Disattivato*, *Smart Training*, *Smart Block*, *Notifica*, *Blocca*). Questo rapporto consente di analizzare il livello di addestramento di Controllo adattivo delle anomalie e valutare il numero di regole che sono passate dalla modalità *Smart Training* alla modalità operativa normale (ad esempio *Smart Block*).

- **Rapporto sulle regole attivate di Controllo adattivo delle anomalie**. Il rapporto contiene informazioni sui trigger di regole. Il rapporto mostra anche la modalità di attivazione della regola: *Blocca* (compreso *Smart Block*) o *Notifica*. Questo rapporto consente di valutare l'attività di Controllo adattivo delle anomalie nei computer degli utenti.

Come visualizzare i rapporti di Controllo adattivo delle anomalie in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.
4. Eseguire una delle seguenti operazioni:
   - Se si desidera visualizzare il rapporto sullo stato delle regole di Controllo adattivo delle anomalie, fare clic sul collegamento **Rapporto sullo stato delle regole di Controllo adattivo delle anomalie**.
   - Se si desidera visualizzare il rapporto sulle regole di Controllo adattivo delle anomalie attivate, fare clic sul collegamento **Rapporto sulle regole attivate di Controllo adattivo delle anomalie**.
5. Verrà avviato il processo di generazione del rapporto.

Il rapporto viene visualizzato in una nuova finestra.

Come visualizzare i rapporti di Controllo adattivo delle anomalie in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.

5. Nel blocco **Regole**, eseguire una delle seguenti operazioni:

   - Se si desidera visualizzare il rapporto sullo stato delle regole di Controllo adattivo delle anomalie, selezionare **Visualizza rapporto → Stato regole**.

   - Se si desidera visualizzare il rapporto sulle regole di Controllo adattivo delle anomalie attivate, fare clic su **Visualizza rapporto → Rilevamenti**.

6. Verrà avviato il processo di generazione del rapporto.

   Il rapporto viene visualizzato in una nuova finestra.

Per generare rapporti nella console di Kaspersky Security Center, è necessario abilitare il trasferimento dei dati ad Administration Server. Il trasferimento dei dati è abilitato per impostazione predefinita.

Come abilitare il trasferimento dei dati per Controllo adattivo delle anomalie in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Impostazioni generali → Rapporti e archivi**.

4. Nel blocco **Trasferimento dei dati ad Administration Server**, fare clic sul pulsante **Impostazioni**.

5. Selezionare le seguenti caselle:

   - **Rapporto sullo stato delle regole di Controllo adattivo delle anomalie**.

   - **Rapporto sulle regole attivate di Controllo adattivo delle anomalie**.

6. Salvare le modifiche.

Come abilitare il trasferimento dei dati per Controllo adattivo delle anomalie in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali → Integrazione KSC**.

5. In **Trasferimento dei dati ad Administration Server**, selezionare le seguenti caselle di controllo:

   - **Rapporto sullo stato delle regole di Controllo adattivo delle anomalie**.

   - **Rapporto sulle regole attivate di Controllo adattivo delle anomalie**.

6. Salvare le modifiche.

Archivio Attivazioni di regole nello stato Smart Training

In modalità di addestramento, Controllo adattivo delle anomalie invia le informazioni sulle regole attivate a un archivio separato, **Attivazioni di regole nello stato Smart Training**. Le informazioni sulle regole attivate sono rappresentate nell'archivio come un elenco di eventi. Per ottimizzare Controllo adattivo delle anomalie, è possibile confermare il comportamento atipico nel computer oppure aggiungere un'esclusione dalla regola.

Eventi di Controllo adattivo delle anomalie

Controllo adattivo delle anomalie registra gli eventi di attivazione della regola nelle modalità *Blocca* (incluso *Smart Block*) e *Notifica*. A tale scopo sono forniti i seguenti eventi:

Azione del processo bloccata

Azione del processo ignorata

Gli eventi contengono informazioni sull'attività sospetta, inclusi i checksum dei file, gli utenti coinvolti, l'ora di attivazione della regola e il nome del computer. Dopo aver analizzato l'evento, è possibile aggiungere immediatamente esclusioni dalla regola se l'attività è legittima.

Controllo applicazioni

Controllo applicazioni gestisce l'avvio delle applicazioni nei computer degli utenti. Ciò consente di implementare un criterio di sicurezza aziendale quando si utilizzano le applicazioni. Controllo applicazioni riduce anche il rischio di infezione del computer limitando l'accesso alle applicazioni.

La configurazione di Controllo applicazioni prevede i seguenti passaggi:

1. Creazione delle categorie di applicazioni.

   L'amministratore crea categorie di applicazioni che l'amministratore desidera gestire. Le categorie di applicazioni sono destinate a tutti i computer della rete aziendale, indipendentemente dai gruppi di amministrazione. Per creare una categoria, è possibile utilizzare i seguenti criteri: Categoria KL (ad esempio, *Browser* o un'altra categoria), hash del file, fornitore dell'applicazione e altri criteri.

2. Creazione delle regole di Controllo applicazioni.

   L'amministratore crea le regole di Controllo applicazioni nel criterio per il gruppo di amministrazione. La regola include le categorie di applicazioni e lo stato di avvio delle applicazioni di queste categorie: bloccate o consentite. L'amministratore può creare molte regole. Una sola applicazione può soddisfare i criteri di più regole. La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. Kaspersky Endpoint Security controlla se un'applicazione soddisfa una regola ogni volta che viene avviata. Kaspersky Endpoint Security abbina in sequenza l'applicazione a tutte le regole di Controllo applicazioni.

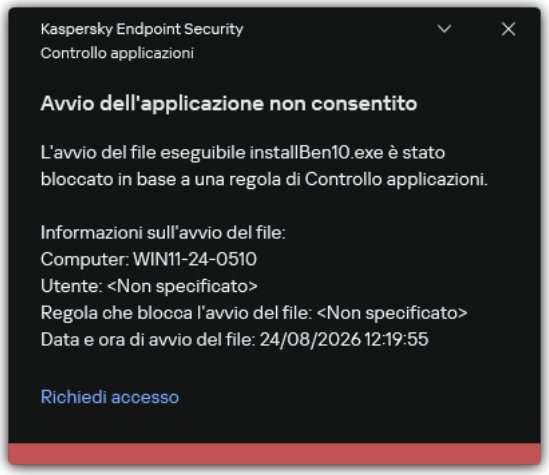
3. Selezione della modalità di Controllo applicazioni.

   L'amministratore sceglie la modalità per l'utilizzo delle applicazioni che non sono incluse in nessuna delle regole: (lista vietati e lista consentiti delle applicazioni).

Quando un utente tenta di avviare un'applicazione vietata, Kaspersky Endpoint Security blocca l'avvio dell'applicazione e visualizza una notifica (vedere la figura seguente).

È disponibile una *modalità test* per verificare la configurazione di Controllo applicazioni. In questa modalità, Kaspersky Endpoint Security procede come segue:

- Consente l'avvio delle applicazioni, comprese quelle vietate.
- Mostra una notifica sull'avvio di un'applicazione vietata e aggiunge informazioni al rapporto sul computer dell'utente.
- Invia i dati sull'avvio delle applicazioni vietate a Kaspersky Security Center.



Notifica di Controllo applicazioni

Modalità di esecuzione di Controllo applicazioni

Il componente Controllo applicazioni funziona in due modalità:

- **Lista vietati**. In questa modalità, Controllo applicazioni consente agli utenti di avviare tutte le applicazioni ad eccezione di quelle vietate nelle regole di Controllo applicazioni.

  Questa modalità di Controllo applicazioni è abilitata per impostazione predefinita.

- **Lista consentiti**. In questa modalità, Controllo applicazioni impedisce agli utenti di avviare qualsiasi applicazione ad eccezione di quelle consentite e non vietate nelle regole di Controllo applicazioni.

  Se le regole di permesso di Controllo applicazioni sono completamente configurate, il componente blocca l'avvio di tutte le nuove applicazioni che non sono state verificate dall'amministratore della LAN, consentendo al contempo il funzionamento del sistema operativo e delle applicazioni attendibili alle quali gli utenti si affidano per le proprie attività.

  Sono disponibili suggerimenti sulla configurazione delle regole di Controllo applicazioni nella modalità Lista consentiti.

Controllo Applicazioni può essere configurato per il funzionamento in queste modalità sia utilizzando l'interfaccia locale di Kaspersky Endpoint Security che utilizzando Kaspersky Security Center.

Tuttavia, Kaspersky Security Center offre strumenti che non sono disponibili nell'interfaccia locale di Kaspersky Endpoint Security, come gli strumenti necessari per le seguenti attività:

- Creazione delle categorie di applicazioni.

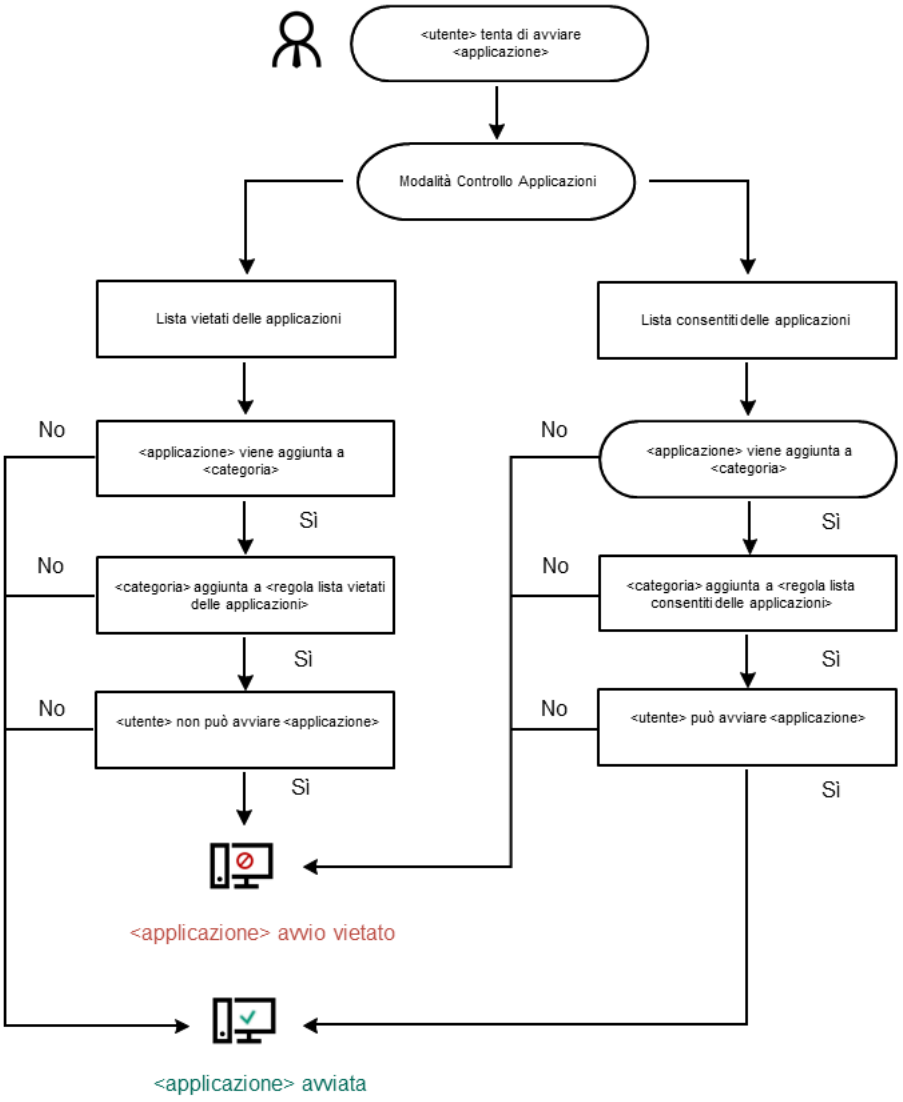
  Le regole di Controllo applicazioni create in Kaspersky Security Center Administration Console si basano sulle categorie di applicazioni personalizzate e non sulle condizioni di inclusione ed esclusione, come nel caso dell'interfaccia locale di Kaspersky Endpoint Security.

- Ricezione delle informazioni sulle applicazioni installate nei computer della LAN aziendale.

Questo è il motivo per cui si consiglia di utilizzare Kaspersky Security Center per configurare il funzionamento del componente Controllo applicazioni.

Algoritmo operativo di Controllo applicazioni

Kaspersky Endpoint Security utilizza un algoritmo per prendere una decisione in merito all'avvio di un'applicazione (vedere la figura seguente).



Algoritmo operativo di Controllo applicazioni

Limitazioni delle funzionalità di Controllo applicazioni

L'esecuzione del componente Controllo applicazioni è limitata nei seguenti casi:

- Quando si esegue l'upgrade della versione dell'applicazione, l'importazione delle impostazioni del componente Controllo applicazioni non è supportata.
- Se la connessione con i server KSN non è disponibile, Kaspersky Endpoint Security ottiene le informazioni sulla reputazione delle applicazioni e dei relativi moduli solo dai database locali.

  L'elenco delle applicazioni che Kaspersky Endpoint Security designa come categoria KL **Altro software\Applicazioni attendibili in base alla reputazione in KSN** può variare a seconda che sia disponibile o meno una connessione ai server di KSN.

- Nel database di Kaspersky Security Center possono essere archiviate informazioni su 150.000 file elaborati. Una volta raggiunto questo numero di record, non saranno elaborati nuovi file. Per riprendere le operazioni di inventario, è necessario eliminare i file di cui è stato precedentemente creato l'inventario nel database di Kaspersky Security Center dal computer in cui è installato Kaspersky Endpoint Security.
- Il componente non controlla l'avvio degli script, a meno che lo script non sia inviato all'interprete tramite la riga di comando.

  Se l'avvio di un interprete è consentito dalle regole di Controllo applicazioni, il componente non bloccherà uno script avviato da questo interprete.

  Se almeno uno degli script specificati nella riga di comando dell'interprete non può essere avviato dalle regole di Controllo applicazioni, il componente blocca tutti gli script specificati nella riga di comando dell'interprete.

- Il componente non controlla l'avvio di script da interpreti che non sono supportati da Kaspersky Endpoint Security.

  Kaspersky Endpoint Security supporta i seguenti interpreti:

  - Java
  - PowerShell

  Sono supportati i seguenti tipi di interpreti:

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe
  - %SystemRoot%\system32\cscript.exe

- %SystemRoot%\system32\wscript.exe
- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

Ottenimento di informazioni sulle applicazioni installate

Per creare regole di Controllo applicazioni ottimali, è prima consigliabile raccogliere informazioni sulle applicazioni utilizzate nei computer della rete LAN aziendale. A tale scopo, è possibile ottenere le seguenti informazioni:

- Produttori, versioni e localizzazioni delle applicazioni utilizzate nella rete LAN aziendale.
- Frequenza degli aggiornamenti delle applicazioni.
- Criteri di utilizzo delle applicazioni adottati nell'azienda (può trattarsi di criteri di sicurezza o di criteri amministrativi).
- Percorso di archiviazione dei pacchetti di distribuzione delle applicazioni.

Visualizzazione delle informazioni sulle applicazioni

Le informazioni sulle applicazioni installate sono fornite da Kaspersky Security Center Network Agent. Le informazioni sulle applicazioni installate sono disponibili nella console di Kaspersky Security Center nella cartella **Registro delle applicazioni**. Network Agent aggiorna le informazioni a ogni sincronizzazione con Kaspersky Security Center. Per ulteriori dettagli sulle informazioni inviate da Network Agent, consultare la Guida di Kaspersky Security Center.

Per aprire la finestra delle proprietà delle applicazioni nella cartella Registro delle applicazioni:

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura di Administration Console, selezionare **Avanzate** → **Gestione applicazioni** → **Registro delle applicazioni**.
3. Selezionare un'applicazione.
4. Dal menu di scelta rapida dell'applicazione selezionare **Proprietà**.

Visualizzazione delle informazioni sui file eseguibili

È possibile ridurre il carico sul database durante la query di informazioni sui file eseguibili. A tale scopo, è consigliabile eseguire l'attività *Inventario* in diversi computer di riferimento in cui è installato il set standard di software.

Le informazioni sui file eseguibili sono fornite da Kaspersky Endpoint Security. Per ricevere informazioni sull'hardware, è necessario applicare un criterio attivo che abiliti la trasmissione delle informazioni sulle applicazioni installate (tale trasmissione è abilitata per impostazione predefinita).

Come abilitare l'invio delle informazioni sull'applicazione nella Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Rapporti e archivi**.
4. Nel blocco **Trasferimento dei dati ad Administration Server**, fare clic sul pulsante **Impostazioni**.
5. Selezionare la casella di controllo **Applicazioni avviate**.
6. Salvare le modifiche.

Come abilitare l'invio delle informazioni sulle applicazioni in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Integrazione KSC**.
5. Nel blocco **Trasferimento dei dati ad Administration Server**, fare clic sul pulsante **Impostazioni avanzate**.
6. Nella finestra visualizzata, selezionare la casella di controllo **Informazioni sulle applicazioni avviate**.
7. Salvare le modifiche.

È possibile ottenere un elenco di file eseguibili utilizzando l'attività *Inventario* di Kaspersky Endpoint Security. È possibile visualizzare l'elenco dei file eseguibili nella console di Kaspersky Security Center, nella cartella **File eseguibili**.

Prima di eseguire l'attività *Inventario*, assicurarsi che il database soddisfi i suggerimenti di Kaspersky Security Center. Per ulteriori dettagli sulla limitazioni del database, consultare la Guida di Kaspersky Security Center.

Come eseguire l'attività Inventario in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Inventario**.

Passaggio 2. Ambito dell'inventario

Creare un elenco di cartelle in cui si desidera che Kaspersky Endpoint Security cerchi i file eseguibili. Configurare le impostazioni dell'inventario (vedere la tabella seguente).

Passaggio 3. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 4. Selezione dell'account per eseguire l'attività

Selezione dell'account per eseguire l'attività *Inventario*. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale. Se l'ambito dell'inventario include unità di rete o altri oggetti con accesso limitato, selezionare un account utente con diritti di accesso sufficienti.

Passaggio 5. Configurazione di una pianificazione di avvio dell'attività

Ad esempio, configurare manualmente la pianificazione dell'attività.

Passaggio 6. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Inventario di base*.

Passaggio 7. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività. In seguito a questa operazione, viene eseguita una ricerca dei file eseguibili nei computer degli utenti in base alla pianificazione configurata.

Come eseguire un'attività Inventario in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Inventory**.

   c. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Inventario di base*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Selezione dell'account per eseguire l'attività. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.

6. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Per configurare l'attività, passare alle proprietà dell'attività (vedere la tabella di seguito).

8. Selezionare la casella di controllo accanto all'attività.

9. Fare clic su **Avvia**.

   È possibile monitorare lo stato dell'attività e il numero di dispositivi in cui l'attività è stata completata o è stata completata con un errore. Di conseguenza, i file eseguibili verranno ricercati nei computer degli utenti secondo la pianificazione specificata.

Per aprire la finestra delle proprietà di un file eseguibile nella cartella File eseguibili:

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura di Administration Console, selezionare **Avanzate** → **Gestione applicazioni** → **File eseguibili**.
3. Selezionare un file eseguibile.
4. Dal menu di scelta rapida del file eseguibile selezionare **Proprietà**.

Per visualizzare informazioni generali su un'applicazione e sui relativi file eseguibili, e l'elenco dei computer in cui è installata un'applicazione, aprire la finestra delle proprietà di un'applicazione selezionata nella cartella **Registro delle applicazioni** o **File eseguibili**.

Aggiornamento delle informazioni sulle applicazioni installate e sui file eseguibili

Il funzionamento del componente Controllo Applicazioni con il database dei file eseguibili è stato ottimizzato in Kaspersky Endpoint Security. Kaspersky Endpoint Security aggiorna automaticamente il database dopo l'eliminazione del file dal computer. Ciò consente di mantenere aggiornato il database e di risparmiare le risorse di Kaspersky Security Center. Per mantenere aggiornato il database delle applicazioni installate, è necessario abilitare l'invio delle informazioni dell'applicazione ad Administration Server (abilitato per impostazione predefinita).

Impostazioni dell'inventario

Parametro	Descrizione
Ambiti inventario	Elenco di oggetti che formeranno l'ambito di inventario.
Inventario dei moduli DLL	Kaspersky Endpoint Security cerca i moduli DLL nell'ambito dell'inventario e invia le informazioni a Kaspersky Security Center. L'abilitazione dell'inventario dei moduli DLL aumenta notevolmente il tempo necessario per il completamento dell'attività Inventario e le dimensioni del database.
Inventario dei file di script	Kaspersky Endpoint Security cerca gli script nell'ambito dell'inventario e invia le informazioni a Kaspersky Security Center. L'abilitazione dei file script di inventario aumenta notevolmente il tempo necessario per il completamento dell'attività Inventario e le dimensioni del database.
Esegui solo quando il computer è inattivo	Avvio posticipato dell'attività quando le risorse del computer sono occupate. Kaspersky Endpoint Security avvia l'attività di scansione se il computer è bloccato o se lo screensaver è attivo. Se l'esecuzione dell'attività è stata interrotta, ad esempio sbloccando il computer, Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui era stata interrotta. Questa opzione di pianificazione consente di conservare le risorse del computer durante l'utilizzo del computer.
Esamina solo i file nuovi e modificati	Esamina solo i nuovi file e i file che sono stati modificati dopo l'ultima scansione. Questo consente di ridurre la durata di una scansione. Questa modalità si applica sia ai file semplici che compositi.
Ignora file scansionato per più di (sec) N sec	Limitazione della durata di esecuzione dell'attività. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. L'attività non è contrassegnata come completata. La prossima volta che Kaspersky Endpoint Security esegue l'attività, questa verrà eseguita dall'inizio e in base alla pianificazione.

Parametro	Descrizione
Esamina gli archivi	Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio).
Esamina i pacchetti di distribuzione	Scansione dei pacchetti di distribuzione delle applicazioni di terze parti.
Non decomprimere i file compositi di grandi dimensioni	Se la casella di controllo è selezionata, l'applicazione non esegue la scansione dei file compositi se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, l'applicazione esamina i file compositi di qualsiasi dimensione. L'applicazione esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.

Come abilitare la modalità Applicazioni bloccate

Applicazioni bloccate è la modalità con cui Controllo applicazioni consente agli utenti di avviare tutte le applicazioni ad eccezione di quelle vietate nelle regole di Controllo applicazioni. In altre parole, se non esiste una regola di rifiuto, Controllo applicazioni consente di avviare l'applicazione. Questa modalità di Controllo applicazioni è abilitata per impostazione predefinita.

Prima di abilitare la modalità *Applicazioni bloccate*, è consigliabile testare le regole di Controllo applicazioni. A tale scopo, è possibile abilitare la modalità di test.

Come selezionare la modalità Applicazioni bloccate in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
5. Selezionare la casella di controllo **Controllo applicazioni**.
6. Nel blocco **Impostazioni di Controllo applicazioni**, utilizzare l'elenco a discesa **Modalità controllo** e selezionare **Lista vietati**.
7. Nell'elenco a discesa **Azione**, selezionare l'azione per Controllo applicazioni.
   - **Testa regole**. Controllo applicazioni non blocca le applicazioni la cui esecuzione è impedita dalle regole, ma genera eventi sull'esecuzione delle applicazioni che altrimenti sarebbero bloccati.
   - **Applica regole**. Controllo applicazioni blocca le applicazioni bloccate e genera gli eventi corrispondenti.

8. Selezionare lo stato delle regole di Controllo applicazioni:

   - **Attivato**. Questo stato indica che la regola viene utilizzata durante l'esecuzione del componente Controllo applicazioni.
   - **Disattivato**. Questo stato indica che la regola viene ignorata durante l'esecuzione del componente Controllo applicazioni.
   - **Verifica**. Questo stato indica che Kaspersky Endpoint Security consente sempre l'avvio delle applicazioni a cui si applica la regola ma registra le informazioni relative all'avvio di tali applicazioni nel rapporto.

   Se necessario, aggiungere nuove regole di Controllo applicazioni.

9. Configurare le impostazioni avanzate di Controllo applicazioni:

   - **Monitora il caricamento dei moduli DLL (aumenta notevolmente il carico sul sistema)**. Se la casella di controllo è selezionata, Kaspersky Endpoint Security controlla il caricamento dei moduli DLL quando gli utenti tentano di avviare le applicazioni. Le informazioni sul modulo DLL e sull'applicazione che lo ha caricato vengono registrate nel rapporto.

     Quando si abilita il controllo del caricamento dei moduli DLL e dei driver, verificare che nelle impostazioni di Controllo applicazioni sia abilitata una delle seguenti regole: la regola **Immagine gold** predefinita o un'altra regola che contiene la categoria KL "**Immagine gold\Certificati attendibili**" e garantisce che i moduli DLL e i driver attendibili siano caricati prima dell'avvio di Kaspersky Endpoint Security. Abilitare il controllo del caricamento dei moduli DLL e dei driver quando la regola **Immagine gold** è disabilitata può generare instabilità nel sistema operativo.

     Kaspersky Endpoint Security monitora solo i moduli DLL e i driver caricati dal momento che è stata selezionata la casella di controllo. Dopo aver selezionato la casella di controllo, è consigliabile riavviare il computer per assicurarsi che l'applicazione monitori tutti i moduli DLL e i driver, inclusi quelli caricati prima dell'avvio di Kaspersky Endpoint Security.

   - **Usa una rigorosa verifica della firma digitale**. È possibile selezionare un certificato come condizione di attivazione per una regola di Controllo applicazioni. Se questa casella di controllo è selezionata, Kaspersky Endpoint Security applica le regole alle applicazioni firmate con i certificati solo dall'archivio dei certificati di sistema attendibili. Le applicazioni firmate con tale certificato sono considerate attendibili anche dai componenti della protezione, ad esempio l'attività *Scansione malware*. Tuttavia, se si specifica un certificato da un archivio diverso in una regola di Controllo applicazioni, Kaspersky Endpoint Security non applica tale regola.

     Se la casella di controllo è deselezionata, Kaspersky Endpoint Security applica le regole alle applicazioni firmate da un certificato di Windows Trusted Root Certificate Store. Tali applicazioni non fanno parte dell'area attendibile. I componenti della protezione monitorano le attività di tali applicazioni.

   - **Messaggio relativo al blocco**. Modello del messaggio visualizzato quando viene attivata una regola di Controllo applicazioni che blocca l'avvio di un'applicazione.
   - **Messaggio all'amministratore**. Modello del messaggio che un utente può inviare all'amministratore della LAN aziendale se l'utente ritiene che un'applicazione sia stata bloccata per errore.

10. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare la modalità Applicazioni bloccate in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo app**.
5. Attivare l'interruttore **Controllo applicazioni ABILITATO**.
6. Nel blocco **Modalità operativa**, selezionare **Blocca tutto tranne l'elenco di regole**.
7. Nel blocco **Azione**, selezionare l'azione per Controllo applicazioni.
   - **Informa**. Controllo applicazioni non blocca le applicazioni la cui esecuzione è impedita dalle regole, ma genera eventi sull'esecuzione delle applicazioni che altrimenti sarebbero bloccati.
   - **Applica regole**. Controllo applicazioni blocca le applicazioni bloccate e genera gli eventi corrispondenti.
8. Selezionare lo stato delle regole di Controllo applicazioni:
   - **Abilitato**. Questo stato indica che la regola viene utilizzata durante l'esecuzione del componente Controllo applicazioni.
   - **Disabilitato**. Questo stato indica che la regola viene ignorata durante l'esecuzione del componente Controllo applicazioni.
   - **Modalità di test**. Questo stato indica che Kaspersky Endpoint Security consente sempre l'avvio delle applicazioni a cui si applica la regola ma registra le informazioni relative all'avvio di tali applicazioni nel rapporto.

   Se necessario, aggiungere nuove regole di Controllo applicazioni.
9. Configurare le impostazioni avanzate di Controllo applicazioni:
   - **Monitora il caricamento dei moduli DLL**. Se la casella di controllo è selezionata, Kaspersky Endpoint Security controlla il caricamento dei moduli DLL quando gli utenti tentano di avviare le applicazioni. Le informazioni sul modulo DLL e sull'applicazione che lo ha caricato vengono registrate nel rapporto.

     Quando si abilita il controllo del caricamento dei moduli DLL e dei driver, verificare che nelle impostazioni di Controllo applicazioni sia abilitata una delle seguenti regole: la regola **Immagine gold** predefinita o un'altra regola che contiene la categoria KL "**Immagine gold\Certificati attendibili**" e garantisce che i moduli DLL e i driver attendibili siano caricati prima dell'avvio di Kaspersky Endpoint Security. Abilitare il controllo del caricamento dei moduli DLL e dei driver quando la regola **Immagine gold** è disabilitata può generare instabilità nel sistema operativo.

     Kaspersky Endpoint Security monitora solo i moduli DLL e i driver caricati dal momento che è stata selezionata la casella di controllo. Dopo aver selezionato la casella di controllo, è consigliabile riavviare il computer per assicurarsi che l'applicazione monitori tutti i moduli DLL e i driver, inclusi quelli caricati prima dell'avvio di Kaspersky Endpoint Security.

- **Usa una rigorosa verifica della firma digitale**. È possibile selezionare un certificato come condizione di attivazione per una regola di Controllo applicazioni. Se questa casella di controllo è selezionata, Kaspersky Endpoint Security applica le regole alle applicazioni firmate con i certificati solo dall'archivio dei certificati di sistema attendibili. Le applicazioni firmate con tale certificato sono considerate attendibili anche dai componenti della protezione, ad esempio l'attività *Scansione malware*. Tuttavia, se si specifica un certificato da un archivio diverso in una regola di Controllo applicazioni, Kaspersky Endpoint Security non applica tale regola.

  Se la casella di controllo è deselezionata, Kaspersky Endpoint Security applica le regole alle applicazioni firmate da un certificato di Windows Trusted Root Certificate Store. Tali applicazioni non fanno parte dell'area attendibile. I componenti della protezione monitorano le attività di tali applicazioni.

- **Messaggio all'utente**. Modello del messaggio visualizzato quando viene attivata una regola di Controllo applicazioni che blocca l'avvio di un'applicazione.

- **Messaggio all'amministratore**. Modello del messaggio che un utente può inviare all'amministratore della LAN aziendale se l'utente ritiene che un'applicazione sia stata bloccata per errore.

10. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare la modalità Applicazioni bloccate nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
3. Attivare l'interruttore **Controllo applicazioni**.
4. Nel blocco **Modalità Controllo avvio applicazioni**, selezionare **Lista vietati. Sono consentite tutte le applicazioni tranne quelle presenti nell'elenco delle regole**.
5. Nel blocco **Azione all'avvio delle applicazioni bloccate dalle regole**, selezionare l'azione per Controllo applicazioni.

   - **Informa (modalità di test) e registra eventi in rapporto**. Controllo applicazioni non blocca le applicazioni la cui esecuzione è impedita dalle regole, ma genera eventi sull'esecuzione delle applicazioni che altrimenti sarebbero bloccati.

   - **Blocca**. Controllo applicazioni blocca le applicazioni bloccate e genera gli eventi corrispondenti.

6. Selezionare lo stato delle regole di Controllo applicazioni:

   - **Abilitato**. Questo stato indica che la regola viene utilizzata durante l'esecuzione del componente Controllo applicazioni.

   - **Disabilitato**. Questo stato indica che la regola viene ignorata durante l'esecuzione del componente Controllo applicazioni.

   - **Modalità di test**. Questo stato indica che Kaspersky Endpoint Security consente sempre l'avvio delle applicazioni a cui si applica la regola ma registra le informazioni relative all'avvio di tali applicazioni nel rapporto.

   Se necessario, aggiungere nuove regole di Controllo applicazioni.

7. Configurare le impostazioni avanzate di Controllo applicazioni:

- **Monitora caricamento dei moduli DLL**. Se la casella di controllo è selezionata, Kaspersky Endpoint Security controlla il caricamento dei moduli DLL quando gli utenti tentano di avviare le applicazioni. Le informazioni sul modulo DLL e sull'applicazione che lo ha caricato vengono registrate nel rapporto.

  Quando si abilita il controllo del caricamento dei moduli DLL e dei driver, verificare che nelle impostazioni di Controllo applicazioni sia abilitata una delle seguenti regole: la regola **Immagine gold** predefinita o un'altra regola che contiene la categoria KL "**Immagine gold\Certificati attendibili**" e garantisce che i moduli DLL e i driver attendibili siano caricati prima dell'avvio di Kaspersky Endpoint Security. Abilitare il controllo del caricamento dei moduli DLL e dei driver quando la regola **Immagine gold** è disabilitata può generare instabilità nel sistema operativo.

  Kaspersky Endpoint Security monitora solo i moduli DLL e i driver caricati dal momento che è stata selezionata la casella di controllo. Dopo aver selezionato la casella di controllo, è consigliabile riavviare il computer per assicurarsi che l'applicazione monitori tutti i moduli DLL e i driver, inclusi quelli caricati prima dell'avvio di Kaspersky Endpoint Security.

- **Usa una rigorosa verifica della firma digitale**. È possibile selezionare un certificato come condizione di attivazione per una regola di Controllo applicazioni. Se questa casella di controllo è selezionata, Kaspersky Endpoint Security applica le regole alle applicazioni firmate con i certificati solo dall'archivio dei certificati di sistema attendibili. Le applicazioni firmate con tale certificato sono considerate attendibili anche dai componenti della protezione, ad esempio l'attività *Scansione malware*. Tuttavia, se si specifica un certificato da un archivio diverso in una regola di Controllo applicazioni, Kaspersky Endpoint Security non applica tale regola.

  Se la casella di controllo è deselezionata, Kaspersky Endpoint Security applica le regole alle applicazioni firmate da un certificato di Windows Trusted Root Certificate Store. Tali applicazioni non fanno parte dell'area attendibile. I componenti della protezione monitorano le attività di tali applicazioni.

- **Modelli di messaggi sul blocco delle applicazioni**. Modello del messaggio visualizzato quando viene attivata una regola di Controllo applicazioni che blocca l'avvio di un'applicazione.

- **Modello di messaggio visualizzato quando viene bloccato l'avvio di un'applicazione**. Modello del messaggio che un utente può inviare all'amministratore della LAN aziendale se l'utente ritiene che un'applicazione sia stata bloccata per errore.

8. Salvare le modifiche.

Di conseguenza, Controllo applicazioni blocca le applicazioni bloccate. Kaspersky Endpoint Security genera anche gli eventi *Avvio dell'applicazione non consentito*. È possibile utilizzare questi eventi per generare il rapporto *Rapporto sulle applicazioni proibite* nella console di Kaspersky Security Center. Nel riepilogo del rapporto è possibile visualizzare l'elenco delle applicazioni e dei computer in cui è stata attivata la regola di Controllo applicazioni.

Controllo applicazioni basato su un computer di base

È possibile utilizzare un computer di base per creare un'immagine con il set di applicazioni desiderato. È quindi possibile utilizzare questa immagine per distribuire il sistema operativo e le applicazioni in altri computer. Non è sempre possibile mantenere aggiornata l'immagine. Controllo applicazioni consente di gestire un elenco delle applicazioni consentite in base a un computer di base. Controllo applicazioni determina automaticamente quali applicazioni sono installate nel computer di base e aggiorna la categoria. In questo modo i computer ottengono un elenco aggiornato delle applicazioni consentite.

La configurazione di Controllo applicazioni in base a un computer di base prevede i passaggi seguenti:

1. Creazione di una categoria ad aggiornamento automatico. Durante la creazione della nuova categoria, selezionare la categoria **Categoria che include i file eseguibili da una cartella specifica** e selezionare il computer di base.

   Come creare una categoria aggiornata automaticamente in Administration Console (MMC)

   1. Aprire Kaspersky Security Center Administration Console.
   2. Nella struttura di Administration Console, selezionare **Avanzate** → **Gestione applicazioni** → **Categorie di applicazioni**.
   3. Fare clic sul pulsante **Nuova categoria** nell'area di lavoro.

      Verrà avviata la creazione guidata della categoria di applicazioni.
   4. Seguire le istruzioni della procedura guidata di creazione delle categorie di applicazioni.

Passaggio 1. Selezione del tipo di categoria

Selezionare **Categoria che include i file eseguibili dai dispositivi selezionati** come tipo di categoria.

Passaggio 2. Immissione del nome di una categoria utente

In questo passaggio specificare un nome per la categoria di applicazioni.

Passaggio 3. Impostazioni

> Questo passaggio è disponibile se è stato selezionato il tipo di categoria **Categoria che include i file eseguibili dei dispositivi selezionati**.

In questo passaggio fare clic sul pulsante **Aggiungi** e specificare i computer i cui file eseguibili verranno aggiunti alla categoria di applicazioni da parte di Kaspersky Security Center. Tutti i file eseguibili dei computer specificati presentati nella cartella **File eseguibili** verranno aggiunti alla categoria di applicazioni da parte di Kaspersky Security Center.

In questo passaggio è anche possibile configurare le seguenti impostazioni:

- Algoritmo per il calcolo della funzione hash. Per selezionare un algoritmo, è necessario selezionare almeno una delle seguenti caselle di controllo:
  - **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)**.
  - **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- La casella di controllo **Sincronizza i dati con l'archivio dell'Administration Server**. Selezionare questa casella di controllo se si desidera che Kaspersky Security Center cancelli periodicamente la categoria di applicazioni e vi inserisca tutti i file eseguibili dei computer specificati presenti nella cartella **File eseguibili**.

  Se la casella di controllo **Sincronizza i dati con l'archivio dell'Administration Server** è deselezionata, Kaspersky Security Center non apporterà modifiche a una categoria di applicazioni dopo la relativa creazione.

Passaggio 4. Filtraggio

In questo passaggio, configurare un filtro per i file.

È possibile specificare il tipo di file che si desidera utilizzare per creare la categoria di applicazioni.

- **Tutti i file**. La categoria corrisponderà a tutti i file. Questa opzione è selezionata per impostazione predefinita.
- **Solo i file esterni alle categorie di applicazioni**. La categoria corrisponderà solo ai file al di fuori delle categorie di applicazioni.

È possibile specificare le cartelle dei computer selezionati che contengono i file da utilizzare per creare la categoria di applicazioni.

- **Tutte le cartelle**. La categoria corrisponderà a tutte le cartelle. Questa opzione è selezionata per impostazione predefinita.
- **Cartella specificata**. La categoria corrisponderà solo alla cartella specificata. Se si seleziona questa opzione, è necessario specificare il percorso di una cartella.

Passaggio 5. Creazione di una categoria personalizzata

Terminare la procedura guidata.

Come creare una categoria con contenuti aggiunti automaticamente in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Operazioni → Applicazioni di terze parti → Categorie di applicazioni**.

   Verrà visualizzato l'elenco delle categorie di applicazioni.

2. Fare clic su **Aggiungi**.

   Verrà avviata la creazione guidata della categoria di applicazioni.

3. Configurare le impostazioni generali della categoria di applicazioni:

   - Nome della categoria.
   - Metodo di creazione della categoria. Selezionare **Categoria che include i file eseguibili dai dispositivi selezionati** come tipo di categoria.

   Procedere con il passaggio successivo.

4. Configurare le impostazioni avanzate della categoria di applicazioni:

   - Specificare i computer da cui Kaspersky Security Center aggiungerà i file eseguibili alla categoria di applicazioni. Tutti i file eseguibili dei computer specificati presentati nella cartella **File eseguibili** verranno aggiunti alla categoria di applicazioni da parte di Kaspersky Security Center.
   - Selezionare un algoritmo per il calcolo della funzione hash.
   - Configurare un intervallo per la sincronizzazione dei dati con l'archivio di Administration Server.
   - Configurare un filtro per i file.

5. Terminare la procedura guidata.

Quando si crea una categoria aggiornata automaticamente, può essere utile suddividere i file in più categorie. Ad esempio, i file del sistema operativo e i file nella cartella Program Files. A tale scopo, è possibile utilizzare un filtro nelle impostazioni della categoria e selezionare singole cartelle.

2. Selezione della modalità di Controllo applicazioni. È necessario impedire l'esecuzione di tutte le applicazioni che non sono consentite esplicitamente. A tale scopo, selezionare la modalità *Applicazioni bloccate*.

3. Creazione di una regola di Controllo applicazioni. Nelle impostazioni delle regole, selezionare la categoria a cui appartengono i file eseguibili dal computer di base.

   Come configurare Controllo applicazioni basato su un computer di base in Administration Console (MMC)

   1. Aprire Kaspersky Security Center Administration Console.
   2. Nella struttura della console, selezionare **Criteri**.
   3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
   4. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
   5. Selezionare la casella di controllo **Controllo applicazioni**.
   6. Nel blocco **Impostazioni di Controllo applicazioni**, utilizzare l'elenco a discesa **Modalità controllo** e selezionare **Lista vietati**.
   7. Nell'elenco a discesa **Azione**, selezionare l'azione per Controllo applicazioni.

      - **Testa regole**. Controllo applicazioni non blocca le applicazioni la cui esecuzione è impedita dalle regole, ma genera eventi sull'esecuzione delle applicazioni che altrimenti sarebbero bloccati.
      - **Applica regole**. Controllo applicazioni blocca le applicazioni bloccate e genera gli eventi corrispondenti.

   8. Nell'elenco delle regole di Controllo applicazioni, fare clic sul pulsante **Aggiungi**.

      Verrà avviata la procedura guidata per l'aggiunta di una regola di Controllo applicazioni.

   9. Nell'elenco a discesa **Categoria**, selezionare una categoria aggiornata automaticamente in base al computer di base.
   10. Selezionare gli utenti o i gruppi di utenti al quale si desidera applicare la regola di Controllo applicazioni.

11. Configurare le impostazioni avanzate della regola di Controllo Applicazioni:

    - **Nega per gli altri utenti**. L'applicazione impedisce l'avvio delle applicazioni appartenenti alla categoria selezionata per tutti gli utenti che non sono presenti nell'elenco.

    - **Programmi di aggiornamento attendibili**. Kaspersky Endpoint Security considera le applicazioni incluse nella categoria selezionata come programmi di aggiornamento attendibili a cui è consentito creare altri file eseguibili che potranno essere eseguiti successivamente.

12. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare Controllo applicazioni basato su un computer di base in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza** → **Controllo app**.

5. Attivare l'interruttore **Controllo applicazioni ABILITATO**.

6. Nel blocco **Modalità operativa**, selezionare **Blocca tutto tranne l'elenco di regole**.

7. Nel blocco **Azione**, selezionare l'azione per Controllo applicazioni.

    - **Informa**. Controllo applicazioni non blocca le applicazioni la cui esecuzione è impedita dalle regole, ma genera eventi sull'esecuzione delle applicazioni che altrimenti sarebbero bloccati.

    - **Applica regole**. Controllo applicazioni blocca le applicazioni bloccate e genera gli eventi corrispondenti.

8. Nell'elenco delle regole di Controllo applicazioni, fare clic sul pulsante **Aggiungi**.

   Verrà avviata la procedura guidata per l'aggiunta di una regola di Controllo applicazioni.

9. Sotto **Categorie/applicazioni**, selezionare una categoria aggiornata automaticamente in base al computer di base.

10. Selezionare gli utenti o i gruppi di utenti al quale si desidera applicare la regola di Controllo applicazioni.

11. Configurare le impostazioni avanzate della regola di Controllo Applicazioni:

    - **Utenti**. L'applicazione impedisce l'avvio delle applicazioni appartenenti alla categoria selezionata per tutti gli utenti che non sono presenti nell'elenco.

    - **Programmi di aggiornamento attendibili**. Kaspersky Endpoint Security considera le applicazioni incluse nella categoria selezionata come programmi di aggiornamento attendibili a cui è consentito creare altri file eseguibili che potranno essere eseguiti successivamente.

12. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare Controllo applicazioni basato su un computer di base nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza → Controllo applicazioni**.
3. Attivare l'interruttore **Controllo applicazioni**.
4. Nel blocco **Modalità Controllo avvio applicazioni**, selezionare **Lista vietati. Sono consentite tutte le applicazioni tranne quelle presenti nell'elenco delle regole**.
5. Nel blocco **Azione all'avvio delle applicazioni bloccate dalle regole**, selezionare l'azione per Controllo applicazioni.
   - **Informa (modalità di test) e registra eventi in rapporto**. Controllo applicazioni non blocca le applicazioni la cui esecuzione è impedita dalle regole, ma genera eventi sull'esecuzione delle applicazioni che altrimenti sarebbero bloccati.
   - **Blocca**. Controllo applicazioni blocca le applicazioni bloccate e genera gli eventi corrispondenti.
6. Nell'elenco delle regole di Controllo applicazioni, fare clic sul pulsante **Aggiungi**.

   Verrà avviata la procedura guidata per l'aggiunta di una regola di Controllo applicazioni.
7. Sotto **Categoria**, selezionare una categoria aggiornata automaticamente in base al computer di base.
8. Selezionare gli utenti o i gruppi di utenti al quale si desidera applicare la regola di Controllo applicazioni.
9. Configurare le impostazioni avanzate della regola di Controllo Applicazioni:
   - **Nega per gli altri utenti**. L'applicazione impedisce l'avvio delle applicazioni appartenenti alla categoria selezionata per tutti gli utenti che non sono presenti nell'elenco.
   - **Programmi di aggiornamento attendibili**. Kaspersky Endpoint Security considera le applicazioni incluse nella categoria selezionata come programmi di aggiornamento attendibili a cui è consentito creare altri file eseguibili che potranno essere eseguiti successivamente.
10. Salvare le modifiche.

Gestione delle regole di Controllo applicazioni

Kaspersky Endpoint Security controlla l'avvio delle applicazioni da parte degli utenti tramite regole. Una regola di Controllo applicazioni specifica le condizioni di attivazione e le azioni eseguite da Controllo applicazioni quando viene attivata la regola (autorizzazione o blocco dell'avvio delle applicazioni da parte degli utenti).

Condizioni di attivazione della regola

Una condizione che attiva una regola ha la seguente correlazione: "tipo di condizione - criterio della condizione - valore della condizione". In base alle condizioni di attivazione della regola, Kaspersky Endpoint Security applica (o non applica) una regola a un'applicazione.

Nelle regole vengono utilizzati i seguenti tipi di condizioni:

- *Condizioni di inclusione*. Kaspersky Endpoint Security applica la regola all'applicazione se l'applicazione corrisponde ad almeno una delle condizioni di inclusione.
- *Condizioni di esclusione*. Kaspersky Endpoint Security non applica la regola all'applicazione se l'applicazione corrisponde ad almeno una delle condizioni di esclusione e non corrisponde a nessuna delle condizioni di inclusione.

Le condizioni di attivazione della regola vengono create utilizzando i criteri. Per creare regole in Kaspersky Endpoint Security vengono utilizzati i seguenti criteri:

- Percorso della cartella che contiene il file eseguibile dell'applicazione o percorso del file eseguibile dell'applicazione.
- Metadati: nome del file eseguibile dell'applicazione, versione del file eseguibile dell'applicazione, nome dell'applicazione, versione dell'applicazione, produttore dell'applicazione.
- Hash del file eseguibile dell'applicazione.
- Certificato: autorità di emissione, oggetto e identificazione personale.
- Inclusione dell'applicazione in una categoria KL.
- Percorso del file eseguibile dell'applicazione in un'unità rimovibile.

Il valore del criterio deve essere specificato per ogni criterio utilizzato nella condizione. Se i parametri dell'applicazione avviata corrispondono ai valori dei criteri specificati nella condizione di inclusione, la regola viene attivata. In questo caso, Controllo applicazioni esegue l'azione specificata nella regola. Se i parametri dell'applicazione corrispondono ai valori dei criteri specificati nella condizione di esclusione, Controllo applicazioni non controlla l'avvio dell'applicazione.

Se è stato selezionato un certificato come condizione di attivazione della regola, è necessario assicurarsi che tale certificato venga aggiunto alla memoria di sistema attendibile nel computer e controllare le impostazioni di utilizzo della memoria di sistema attendibile nell'applicazione.

Decisioni prese dal componente Controllo applicazioni all'attivazione di una regola

Quando viene attivata una regola, Controllo applicazioni consente agli utenti (o ai gruppi di utenti) di avviare le applicazioni o di bloccare l'avvio in base alla regola. È possibile selezionare singoli utenti o gruppi di utenti a cui è consentito o non consentito avviare le applicazioni che determinano l'attivazione di una regola.

Se una regola non specifica gli utenti per cui è consentito l'avvio delle applicazioni che corrispondono alla regola, viene denominata regola di *blocco*.

Se una regola non specifica alcun utente per cui non è consentito l'avvio delle applicazioni che corrispondono alla regola, viene denominata regola di *autorizzazione*.

La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. Ad esempio, se sono state assegnate una regola di permesso di Controllo applicazioni per un gruppo di utenti e una regola di blocco di Controllo applicazioni per uno degli utenti del gruppo, l'avvio dell'applicazione non sarà consentito per tale utente.

Stato operativo di una regola

Le regole di Controllo applicazioni possono avere uno dei seguenti stati operativi:

- **Abilitato**. Questo stato indica che la regola viene utilizzata durante l'esecuzione del componente Controllo applicazioni.
- **Disabilitato**. Questo stato indica che la regola viene ignorata durante l'esecuzione del componente Controllo applicazioni.
- **Modalità di test**. Questo stato indica che Kaspersky Endpoint Security consente l'avvio delle applicazioni a cui si applicano le regole ma registra le informazioni relative all'avvio di tali applicazioni nel rapporto.

Aggiunta di una condizione di attivazione per la regola di Controllo applicazioni

Per semplificare la creazione delle regole di Controllo applicazioni, è possibile creare categorie di applicazioni.

È consigliabile creare una categoria "Applicazioni di lavoro" in cui è incluso il set di applicazioni standard utilizzate nell'azienda. Se diversi gruppi di utenti utilizzano differenti set di applicazioni per il proprio lavoro, è possibile creare una categoria distinta per ogni gruppo di utenti.

Per creare una categoria di applicazioni in Administration Console:

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura di Administration Console, selezionare **Avanzate** → **Gestione applicazioni** → **Categorie di applicazioni**.
3. Fare clic sul pulsante **Nuova categoria** nell'area di lavoro.

   Viene avviata la procedura guidata di creazione delle categorie utente.
4. Seguire le istruzioni della procedura guidata di creazione della nuova categoria.

Passaggio 1. Selezione del tipo di categoria

In questo passaggio selezionare uno dei seguenti tipi di categorie di applicazioni:

- Categoria con contenuto aggiunto manualmente. I dati dei file eseguibili vengono aggiunti alla categoria in modo manuale Se è stato selezionato questo tipo di categoria, durante il passaggio *Configurazione delle condizioni per l'inclusione delle applicazioni nelle categorie* e durante il passaggio *Configurazione delle condizioni per l'esclusione delle applicazioni dalle categorie*, sarà possibile definire i criteri in base ai quali i file eseguibili verranno inclusi nella categoria.

- Categoria che include i file eseguibili dei dispositivi selezionati. Tali file eseguibili sono elaborati automaticamente e le relative metriche vengono aggiunte alla categoria Se si seleziona questo tipo di categoria, durante il passaggio *Impostazioni* sarà possibile specificare un computer i cui file eseguibili verranno inclusi automaticamente nella categoria.

- Categoria che include file eseguibili di una cartella specifica. I file eseguibili delle applicazioni copiati nella cartella specificata sono elaborati automaticamente e le relative metriche vengono aggiunte alla categoria Se si seleziona questo tipo di categoria, durante il passaggio *Cartella archivio* sarà possibile specificare una cartella da cui i file eseguibili verranno inclusi automaticamente nella categoria.

Quando si crea una categoria con contenuto aggiunto automaticamente, Kaspersky Security Center esegue l'inventario dei file con i seguenti formati: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX e SCR.

Passaggio 2. Immissione del nome di una categoria utente

In questo passaggio specificare un nome per la categoria di applicazioni.

Passaggio 3. Configurazione delle condizioni per l'inclusione di applicazioni in una categoria

Quando si aggiunge un numero elevato di condizioni alle regole di Controllo applicazioni (ad esempio, hash di file), aumenta il consumo delle risorse del computer. Quando il numero totale di condizioni raggiunge 50.000, possono verificarsi problemi di prestazioni. Per ottimizzare le prestazioni, è consigliabile rivedere e ridurre il numero di condizioni.

Questo passaggio è disponibile se è stato selezionato il tipo di categoria **Categoria con contenuto aggiunto manualmente**.

In questo passaggio, nell'elenco a discesa **Aggiungi** selezionare le condizioni per l'inclusione delle applicazioni nella categoria:

- **Dall'elenco di file e&seguibili**. Aggiungere applicazioni dall'elenco dei file eseguibili nel dispositivo client alla categoria personalizzata.
- **Dalle proprietà dei file**. Specificare i dati dettagliati dei file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Metadati dai file nella cartella**. Selezionare una cartella nel dispositivo client contenente i file eseguibili. Kaspersky Security Center indicherà i metadati di questi file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Checksum dei file nella cartella**. Selezionare una cartella nel dispositivo client contenente i file eseguibili. Kaspersky Security Center indicherà gli hash di questi file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Certificati per i file della cartella**. Selezionare una cartella nel dispositivo client contenente i file eseguibili firmati con i certificati. Kaspersky Security Center indicherà i certificati di questi file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.

  Non è consigliabile utilizzare condizioni le cui proprietà non hanno il parametro **Impronta digitale del certificato** specificato.

- **Metadati dei file del programma di installazione MSI**. Selezionare il pacchetto MSI. Kaspersky Security Center indicherà i metadati dei file eseguibili compressi in questo pacchetto MSI come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Checksum dei &file dal programma di installazione MSI dell'applicazione**. Selezionare il pacchetto MSI. Kaspersky Security Center indicherà gli hash dei file eseguibili compressi in questo pacchetto MSI come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Da categoria KL**. Specificare una categoria KL come condizione per l'aggiunta delle applicazioni alla categoria personalizzata. Una *categoria KL* è un elenco di applicazioni che dispongono di attributi condivisi. L'elenco è gestito dagli esperti di Kaspersky. Ad esempio, la categoria KL nota come *Applicazioni Office* include le applicazioni della suite Microsoft Office, Adobe Acrobat e altre ancora.

  È possibile selezionare tutte le categorie KL per generare un elenco esteso di applicazioni attendibili.

- **Specificare il percorso dell'a&pplicazione (maschere supportate)**. Selezionare una cartella nel dispositivo client. Kaspersky Security Center aggiungerà i file eseguibili di questa cartella alla categoria personalizzata.
- **Seleziona certi&ficato dall'archivio**. Selezionare i certificati che sono stati utilizzati per firmare i file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.

  Non è consigliabile utilizzare condizioni le cui proprietà non hanno il parametro **Impronta digitale del certificato** specificato.

È possibile scegliere l'archivio dei certificati. Per impostazione predefinita, Controllo applicazioni applica le regole solo per le applicazioni firmate con un certificato dell'archivio dei certificati di sistema attendibile. Ciò è abilitato dalla casella di controllo **Usa una rigorosa verifica della firma digitale**.

- **Tipo di unità**. Specificare il tipo di dispositivo di archiviazione (tutti i dischi rigidi e le unità rimovibili o solo le unità rimovibili) come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.

Passaggio 4. Configurazione delle condizioni per l'esclusione di applicazioni da una categoria

Questo passaggio è disponibile se è stato selezionato il tipo di categoria **Categoria con contenuto aggiunto manualmente**.

Le applicazioni specificate in questo passaggio vengono escluse dalla categoria anche se queste applicazioni sono state specificate durante il passaggio "Configurazione delle condizioni per l'inclusione di applicazioni in una categoria".

In questo passaggio, nell'elenco a discesa **Aggiungi** selezionare le condizioni per l'esclusione delle applicazioni dalla categoria:

- **Dall'elenco di file e&seguibili**. Aggiungere applicazioni dall'elenco dei file eseguibili nel dispositivo client alla categoria personalizzata.
- **Dalle proprietà dei file**. Specificare i dati dettagliati dei file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Metadati dai file nella cartella**. Selezionare una cartella nel dispositivo client contenente i file eseguibili. Kaspersky Security Center indicherà i metadati di questi file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Checksum dei file nella cartella**. Selezionare una cartella nel dispositivo client contenente i file eseguibili. Kaspersky Security Center indicherà gli hash di questi file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Certificati per i file della cartella**. Selezionare una cartella nel dispositivo client contenente i file eseguibili firmati con i certificati. Kaspersky Security Center indicherà i certificati di questi file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Metadati dei file del programma di installazione MSI**. Selezionare il pacchetto MSI. Kaspersky Security Center indicherà i metadati dei file eseguibili compressi in questo pacchetto MSI come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.
- **Checksum dei &file dal programma di installazione MSI dell'applicazione**. Selezionare il pacchetto MSI. Kaspersky Security Center indicherà gli hash dei file eseguibili compressi in questo pacchetto MSI come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.

- **Da categoria KL**. Specificare una categoria KL come condizione per l'aggiunta delle applicazioni alla categoria personalizzata. Una *categoria KL* è un elenco di applicazioni che dispongono di attributi condivisi. L'elenco è gestito dagli esperti di Kaspersky. Ad esempio, la categoria KL nota come *Applicazioni Office* include le applicazioni della suite Microsoft Office, Adobe Acrobat e altre ancora.

  È possibile selezionare tutte le categorie KL per generare un elenco esteso di applicazioni attendibili.

- **Specificare il percorso dell'a&pplicazione (maschere supportate)**. Selezionare una cartella nel dispositivo client. Kaspersky Security Center aggiungerà i file eseguibili di questa cartella alla categoria personalizzata.

- **Seleziona certi&ficato dall'archivio**. Selezionare i certificati che sono stati utilizzati per firmare i file eseguibili come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.

- **Tipo di unità**. Specificare il tipo di dispositivo di archiviazione (tutti i dischi rigidi e le unità rimovibili o solo le unità rimovibili) come condizione per l'aggiunta delle applicazioni alla categoria personalizzata.

Passaggio 5. Impostazioni

Questo passaggio è disponibile se è stato selezionato il tipo di categoria **Categoria che include i file eseguibili dei dispositivi selezionati**.

In questo passaggio fare clic sul pulsante **Aggiungi** e specificare i computer i cui file eseguibili verranno aggiunti alla categoria di applicazioni da parte di Kaspersky Security Center. Tutti i file eseguibili dei computer specificati presentati nella cartella **File eseguibili** verranno aggiunti alla categoria di applicazioni da parte di Kaspersky Security Center.

In questo passaggio è anche possibile configurare le seguenti impostazioni:

- Algoritmo per il calcolo della funzione hash. Per selezionare un algoritmo, è necessario selezionare almeno una delle seguenti caselle di controllo:

  - **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)**.

  - **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- La casella di controllo **Sincronizza i dati con l'archivio dell'Administration Server**. Selezionare questa casella di controllo se si desidera che Kaspersky Security Center cancelli periodicamente la categoria di applicazioni e vi inserisca tutti i file eseguibili dei computer specificati presenti nella cartella **File eseguibili**.

  Se la casella di controllo **Sincronizza i dati con l'archivio dell'Administration Server** è deselezionata, Kaspersky Security Center non apporterà modifiche a una categoria di applicazioni dopo la relativa creazione.

Passaggio 6. Cartella del repository

Questo passaggio è disponibile se è stato selezionato il tipo di categoria **Categoria che include file eseguibili di una cartella specifica**.

In questo passaggio, specificare la cartella in cui Kaspersky Security Center eseguirà la ricerca dei file eseguibili per aggiungere automaticamente le applicazioni alla categoria di applicazioni.

In questo passaggio è anche possibile configurare le seguenti impostazioni:

- La casella di controllo **Includi librerie di collegamento dinamico (DLL) in questa categoria**. Selezionare questa casella di controllo se si desidera includere le librerie di collegamento dinamico (file DLL) nella categoria di applicazioni.

  L'inclusione dei file DLL nella categoria di applicazioni possono ridurre le prestazioni di Kaspersky Security Center.

- La casella di controllo **Includi i dati degli script in questa categoria**. Selezionare questa casella di controllo se si desidera includere gli script nella categoria di applicazioni.

  L'inclusione degli script nella categoria di applicazioni può ridurre le prestazioni di Kaspersky Security Center.

- Algoritmo per il calcolo della funzione hash. Per selezionare un algoritmo, è necessario selezionare almeno una delle seguenti caselle di controllo:

  - **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)**.
  - **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- La casella di controllo **Forza scansione delle modifiche nella cartella**. Selezionare questa casella di controllo se si desidera che Kaspersky Security Center esegua periodicamente la ricerca dei file eseguibili nella cartella utilizzata per l'aggiunta automatica alla categoria di applicazioni.

  Se la casella di controllo **Forza scansione delle modifiche nella cartella** è deselezionata, Kaspersky Security Center cerca i file eseguibili nella cartella utilizzata per l'aggiunta automatica alla categoria di applicazioni solo se sono state apportate modifiche nella cartella, sono stati aggiunti file nella cartella o sono stati eliminati file dalla cartella.

- Il campo **Intervallo di scansione (1-168 ore)**. In questo campo è possibile specificare l'intervallo di tempo (in ore) dopo il quale Kaspersky Security Center esegue la ricerca dei file eseguibili nella cartella utilizzata per l'aggiunta automatica alla categoria di applicazioni.

  Il campo è disponibile se la casella di controllo **Forza scansione delle modifiche nella cartella** è selezionata.

Passaggio 7. Creazione di una categoria personalizzata

Terminare la procedura guidata.

Per aggiungere una nuova condizione di attivazione per una regola di Controllo applicazioni nell'interfaccia dell'applicazione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.

3. Fare clic sul pulsante **Applicazioni bloccate** o **Applicazioni consentite**.

   Verrà visualizzato l'elenco delle regole di Controllo applicazioni.

4. Selezionare la regola per cui si desidera configurare una condizione di attivazione.

   Verrà visualizzata la finestra delle proprietà della regola di Controllo applicazioni.

5. Selezionare la scheda **Condizioni: N** o la scheda **Esclusioni: N** e fare clic sul pulsante **Aggiungi**.

6. Selezionare le condizioni di attivazione per una regola di Controllo applicazioni:

   - **Condizioni delle proprietà delle applicazioni avviate**. Nell'elenco delle applicazioni in esecuzione è possibile selezionare le applicazioni a cui verrà applicata la regola di Controllo applicazioni. Kaspersky Endpoint Security elenca anche le applicazioni precedentemente in esecuzione nel computer. È necessario selezionare il criterio che si desidera utilizzare per creare una o più condizioni di attivazione della regola: **Hash file**, **Certificato**, **Categoria KL**, **Metadati** or **Percorso del file o della cartella**.

   - **Condizioni "Categoria KL"**. Una *categoria KL* è un elenco di applicazioni che dispongono di attributi condivisi. L'elenco è gestito dagli esperti di Kaspersky. Ad esempio, la categoria KL nota come "Applicazioni Office" include le applicazioni della suite Microsoft Office, Adobe® Acrobat® e altre ancora.

   - **Condizione personalizzata**. È possibile selezionare il file dell'applicazione e una delle condizioni di attivazione della regola: **Hash file**, **Certificato**, **Metadati** or **Percorso del file o della cartella**.

   - **Condizione in base all'unità file (unità rimovibile)**. La regola di Controllo applicazioni viene applicata solo ai file eseguiti in un'unità rimovibile.

   - **Condizioni delle proprietà dei file nella cartella specificata**. La regola di Controllo applicazioni viene applicata solo ai file nella cartella specificata. È inoltre possibile includere o escludere file dalle sottocartelle. È necessario selezionare il criterio che si desidera utilizzare per creare una o più condizioni di attivazione della regola: **Hash file**, **Certificato**, **Categoria KL**, **Metadati** or **Percorso del file o della cartella**.

7. Salvare le modifiche.

Quando si aggiungono le condizioni, tenere conto delle seguenti considerazioni speciali per Controllo applicazioni:

- Kaspersky Endpoint Security supporta i caratteri `*` e `?` per l'immissione di una maschera nei metadati: **Nome file**, **Nome applicazione**, **Fornitore**.

- Kaspersky Endpoint Security non supporta un hash dei file MD5 e non controlla l'avvio delle applicazioni in base a un hash MD5. Un hash SHA256 è utilizzato come condizione di attivazione della regola.

- Non è consigliabile utilizzare solo i criteri **Autorità di emissione** ed **Soggetto del certificato** come condizioni di attivazione della regola. L'utilizzo di questi criteri non è affidabile.

- Se si utilizza un collegamento simbolico nel campo **Percorso del file o della cartella**, è consigliabile risolvere il collegamento simbolico per il corretto funzionamento della regola di Controllo applicazioni. A tale scopo, fare clic sul pulsante **Risolvi collegamento simbolico**.

Aggiunta di file eseguibili dalla cartella File eseguibili alla categoria di applicazioni

Nella cartella **File eseguibili** viene visualizzato l'elenco dei file eseguibili rilevati nei computer. Dopo l'esecuzione dell'attività di inventario, Kaspersky Endpoint Security genera un elenco dei file eseguibili.

Per aggiungere i file eseguibili dalla cartella File eseguibili alla categoria di applicazioni:

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura di Administration Console, selezionare **Avanzate** → **Gestione applicazioni** → **File eseguibili**.
3. Nell'area di lavoro selezionare i file eseguibili che si desidera aggiungere alla categoria di applicazioni.
4. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida relativo ai file eseguibili selezionati, quindi selezionare **Aggiungi a categoria**.
5. Nella finestra visualizzata, procedere come segue:
   - Nella parte superiore della finestra scegliere una delle seguenti opzioni:
     - **Aggiungi a una nuova categoria di applicazioni**. Selezionare questa opzione se si desidera creare una nuova categoria di applicazioni e aggiungervi i file eseguibili.
     - **Aggiungi a una categoria di applicazioni esistente**. Selezionare questa opzione se si desidera selezionare una categoria di applicazioni esistente e aggiungervi i file eseguibili.
   - Nella sezione **Tipo di regola**, selezionare una delle seguenti opzioni:
     - **Regole per l'&aggiunta alle inclusioni**. Selezionare questa opzione se si desidera creare una condizione che aggiunga i file eseguibili alla categoria di applicazioni.
     - **Regole per l'aggiunta alle e&sclusioni**. Selezionare questa opzione se si desidera creare una condizione che escluda i file eseguibili dalla categoria di applicazioni.
   - Nella sezione **Parametro utilizzato come condizione**, selezionare una delle seguenti opzioni:
     - **Dettagli del certificato (o hash SHA256 per i file senza certificato)**.
     - **Dettagli del certificato (i file senza certificato verranno ignorati)**.
     - **Solo SHA256 (i file senza hash verranno ignorati)**.
     - **Solo MD5 (modalità non più disponibile, solo per Kaspersky Endpoint Security 10 versione Service Pack 1)**.
6. Salvare le modifiche.

Aggiunta di file eseguibili correlati agli eventi alla categoria di applicazioni

Per aggiungere i file eseguibili associati agli eventi di Controllo applicazioni alla categoria di applicazioni:

1. Aprire Kaspersky Security Center Administration Console.
2. Nel nodo **Administration Server** della struttura di Administration Console selezionare la scheda **Eventi**.
3. Scegliere una selezione di eventi relativi all'esecuzione del componente Controllo Applicazioni (Visualizzazione degli eventi generati dall'esecuzione del componente Controllo Applicazioni, Visualizzazione degli eventi generati dall'operazione di test del componente Controllo Applicazioni) nell'elenco a discesa **Selezioni eventi**.

4. Fare clic sul pulsante **Esegui selezione**.

5. Selezionare gli eventi di cui si desidera aggiungere i file eseguibili alla categoria di applicazioni.

6. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida relativo agli eventi selezionati, quindi selezionare **Aggiungi a categoria**.

7. Nella finestra visualizzata, configurare le impostazioni della categorie di applicazioni:

   - Nella parte superiore della finestra scegliere una delle seguenti opzioni:

     - **Aggiungi a una nuova categoria di applicazioni**. Selezionare questa opzione se si desidera creare una nuova categoria di applicazioni e aggiungervi i file eseguibili.

     - **Aggiungi a una categoria di applicazioni esistente**. Selezionare questa opzione se si desidera selezionare una categoria di applicazioni esistente e aggiungervi i file eseguibili.

   - Nella sezione **Tipo di regola**, selezionare una delle seguenti opzioni:

     - **Regole per l'aggiunta alle inclusioni**. Selezionare questa opzione se si desidera creare una condizione che aggiunga i file eseguibili alla categoria di applicazioni.

     - **Regole per l'aggiunta alle esclusioni**. Selezionare questa opzione se si desidera creare una condizione che escluda i file eseguibili dalla categoria di applicazioni.

   - Nella sezione **Parametro utilizzato come condizione**, selezionare una delle seguenti opzioni:

     - **Dettagli del certificato (o hash SHA-256 per i file senza certificato)**.

     - **Dettagli del certificato (i file senza certificato verranno ignorati)**.

     - **Solo SHA-256 (i file senza hash verranno ignorati)**.

     - **Solo MD5 (modalità non più disponibile, solo per Kaspersky Endpoint Security 10 versione Service Pack 1)**.

8. Salvare le modifiche.

Aggiunta di una regola di Controllo applicazioni

Per aggiungere una regola di Controllo applicazioni tramite Kaspersky Security Center:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo applicazioni.

4. Fare clic su **Aggiungi**.

   Verrà visualizzata la finestra **Regola di Controllo applicazioni**.

5. Eseguire una delle seguenti operazioni:

   - Se si desidera creare una nuova categoria:

     a. Fare clic su **Crea una categoria**.

        Viene avviata la procedura guidata di creazione delle categorie utente.

     b. Seguire le istruzioni della procedura guidata di creazione della nuova categoria.

     c. Nell'elenco a discesa **Categoria** selezionare la categoria di applicazioni creata.

   - Se si desidera modificare una categoria esistente:

     a. Nell'elenco a discesa **Categoria** selezionare la categoria di applicazioni creata che si desidera modificare.

     b. Fare clic su **Proprietà**.

     c. Modificare le impostazioni della categoria di applicazioni selezionata.

     d. Salvare le modifiche.

     e. Nell'elenco a discesa **Categoria** selezionare la categoria di applicazioni in base alla quale creare una regola.

6. Nella tabella **Utenti e relativi diritti** fare clic sul pulsante **Aggiungi**.

   È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

7. Nella tabella **Utenti e relativi diritti**, procedere come segue:

   - Se si desidera consentire agli utenti e/o ai gruppi di utenti di avviare le applicazioni che appartengono alla categoria selezionata, selezionare la casella di controllo **Consenti** nelle righe corrispondenti.

   - Se si desidera impedire agli utenti e/o ai gruppi di utenti di avviare le applicazioni che appartengono alla categoria selezionata, selezionare la casella di controllo **Blocca** nelle righe corrispondenti.

8. Selezionare la casella di controllo **Nega per gli altri utenti** se si desidera impedire a tutti gli utenti che non compaiono nella colonna **Utente o gruppo** e che non fanno parte del gruppo di utenti specificati nella colonna **Utente o gruppo** di avviare le applicazioni che appartengono alla categoria selezionata.

9. Se si desidera che Kaspersky Endpoint Security consideri le applicazioni incluse nella categoria di applicazioni selezionata come programmi di aggiornamento attendibili a cui è consentito creare altri file eseguibili che potranno essere eseguiti successivamente, selezionare la casella di controllo **Programmi di aggiornamento attendibili**.

   Quando viene eseguita la migrazione delle impostazioni di Kaspersky Endpoint Security, viene eseguita anche la migrazione dell'elenco dei file eseguibili creato dai programmi di aggiornamento attendibili.

10. Salvare le modifiche.

Per aggiungere una regola di Controllo applicazioni:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
3. Fare clic sul pulsante **Applicazioni bloccate** o **Applicazioni consentite**.

   Verrà visualizzato l'elenco delle regole di Controllo applicazioni.
4. Fare clic su **Aggiungi**.

   Si apre la finestra delle impostazioni delle regole di controllo applicazioni.
5. Nella scheda **Impostazioni generali** definire le impostazioni principali della regola:

   a. Nel campo **Nome regola** immettere il nome della regola.

   b. Nel campo **Descrizione** immettere una descrizione della regola.

   c. Nella tabella **Utenti e relativi diritti** fare clic sul pulsante **Aggiungi**.

   È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.

   La regola viene applicata a tutti gli utenti per impostazione predefinita.

   > Se nella tabella non è specificato alcun utente, la regola non può essere salvata.

   d. Nella tabella **Utenti e relativi diritti** utilizzare l'interruttore per definire il diritto degli utenti di avviare le applicazioni.

   e. Selezionare la casella di controllo **Nega per gli altri utenti** se si desidera che l'applicazione impedisca l'esecuzione delle applicazioni che soddisfano le condizioni di attivazione della regola per tutti gli utenti non elencati nella tabella **Utenti e relativi diritti** e non sono membri dei gruppi di utenti nella tabella **Utenti e relativi diritti**.

   > Se la casella di controllo **Nega per gli altri utenti** è deselezionata, Kaspersky Endpoint Security non controlla l'avvio delle applicazioni da parte degli utenti che non sono specificati nella tabella **Utenti e relativi diritti** e che non appartengono ai gruppi di utenti specificati nella tabella **Utenti e relativi diritti**.

   f. Selezionare la casella di controllo **Programmi di aggiornamento attendibili** se si desidera che Kaspersky Endpoint Security consideri le applicazioni che soddisfano le condizioni di attivazione della regola come programmi di aggiornamento attendibili. *Programmi di aggiornamento attendibili* sono applicazioni che possono creare altri file eseguibili che potranno essere eseguiti successivamente.

   Se un'applicazione attiva più regole, Kaspersky Endpoint Security imposta il contrassegno *Programmi di aggiornamento attendibili* se sono soddisfatte le seguenti condizioni:

   - Tutte le regole consentono l'esecuzione dell'applicazione.
   - Almeno una regola ha la casella di controllo **Programmi di aggiornamento attendibili** selezionata.
6. Nella scheda **Condizioni: N**, creare o modificare l'elenco delle condizioni di inclusione per l'attivazione della regola.

7. Nella scheda **Esclusioni: N**, creare o modificare l'elenco delle condizioni di esclusione per l'attivazione della regola.

   Quando viene eseguita la migrazione delle impostazioni di Kaspersky Endpoint Security, viene eseguita anche la migrazione dell'elenco dei file eseguibili creato dai programmi di aggiornamento attendibili.

8. Salvare le modifiche.

Modifica dello stato di una regola di Controllo applicazioni tramite Kaspersky Security Center

Per modificare lo stato di una regola di Controllo applicazioni in Administration Console:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza → Controllo applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo applicazioni.

4. Nella colonna **Stato** fare clic con il pulsante sinistro del mouse per visualizzare il menu di scelta rapida, quindi selezionare una delle seguenti opzioni:

   - **Attivato**. Questo stato indica che la regola viene utilizzata durante l'esecuzione del componente Controllo applicazioni.
   - **Disattivato**. Questo stato indica che la regola viene ignorata durante l'esecuzione del componente Controllo applicazioni.
   - **Verifica**. Questo stato indica che Kaspersky Endpoint Security consente sempre l'avvio delle applicazioni a cui si applica la regola ma registra le informazioni relative all'avvio di tali applicazioni nel rapporto.

5. Salvare le modifiche.

Per modificare lo stato di una regola di Controllo applicazioni nell'interfaccia dell'applicazione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza → Controllo applicazioni**.
3. Fare clic sul pulsante **Applicazioni bloccate** o **Applicazioni consentite**.

   Verrà visualizzato l'elenco delle regole di Controllo applicazioni.

4. Nella colonna **Stato** aprire il menu di scelta rapida, quindi selezionare una delle seguenti opzioni:

   - **Abilitato**. Questo stato indica che la regola viene utilizzata durante l'esecuzione del componente Controllo applicazioni.
   - **Disabilitato**. Questo stato indica che la regola viene ignorata durante l'esecuzione del componente Controllo applicazioni.
   - **Modalità di test**. Questo stato indica che Kaspersky Endpoint Security consente sempre l'avvio delle applicazioni a cui si applica la regola ma registra le informazioni relative all'avvio di tali applicazioni nel rapporto.

5. Salvare le modifiche.

Esportazione e importazione delle regole di Controllo applicazioni

È possibile esportare l'elenco delle regole di Controllo applicazioni in un file XML. È possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco delle regole di Controllo applicazioni o per eseguire la migrazione dell'elenco in un server diverso.

Quando si esportano e si importano le regole di Controllo applicazioni, tenere a mente le seguenti considerazioni speciali:

- Kaspersky Endpoint Security esporta l'elenco delle regole solo per la modalità Controllo applicazioni attiva. In altre parole, se Controllo applicazioni opera in modalità Lista vietati, Kaspersky Endpoint Security esporta le regole solo per questa modalità. Per esportare l'elenco delle regole per la modalità Lista consentiti è necessario cambiare modalità ed eseguire nuovamente l'operazione di esportazione.
- Kaspersky Endpoint Security utilizza le categorie di applicazioni per il funzionamento delle regole di Controllo applicazioni. Durante la migrazione dell'elenco delle regole di Controllo applicazioni in un server diverso, è necessario eseguire la migrazione anche dell'elenco delle categorie di applicazioni. Per ulteriori dettagli sull'esportazione o l'importazione delle categorie di applicazioni, consultare la Guida di Kaspersky Security Center.

Come esportare e importare un elenco di regole di Controllo applicazioni in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
4. Per esportare l'elenco delle regole di Controllo applicazioni:
   a. Selezionare le regole che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.

      Se non è stata selezionata alcuna regola, Kaspersky Endpoint Security esporterà tutte le regole.

   b. Fare clic sul collegamento **Esporta**.
   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle regole e selezionare la cartella in cui si desidera salvare il file.
   d. Salvare il file.

      Kaspersky Endpoint Security esporta l'intero elenco di regole nel file XML.

5. Per importare un elenco di regole di Controllo applicazioni:

    a. Fare clic sul collegamento **Importa**.

    Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle regole.

    b. Aprire il file.

    Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

6. Salvare le modifiche.

Come esportare e importare un elenco di regole di Controllo applicazioni in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

    Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo app**.
5. In **Modalità operativa**, selezionare un elenco di regole: lista vietati e lista consentiti per le applicazioni.
6. Per esportare l'elenco delle regole:

    a. Selezionare le regole che si desidera esportare.

    b. Fare clic sul pulsante → **Esporta**.

    Kaspersky Endpoint Security esporta l'elenco delle regole in un file JSON nella cartella dei download predefinita.

7. Per importare l'elenco delle regole:

    a. Fare clic sul pulsante → **Importa**.

    Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco delle regole.

    b. Aprire il file.

    Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

8. Salvare le modifiche.

Visualizzazione degli eventi generati dall'esecuzione del componente Controllo applicazioni

Per visualizzare gli eventi generati dall'esecuzione del componente Controllo applicazioni ricevuti da Kaspersky Security Center:

1. Aprire Kaspersky Security Center Administration Console.
2. Nel nodo **Administration Server** della struttura di Administration Console selezionare la scheda **Eventi**.
3. Fare clic sul pulsante **Crea selezione**.
4. Nella finestra visualizzata, passare alla sezione **Eventi**.
5. Fare clic sul pulsante **Cancella tutto**.
6. Nella tabella **Eventi** selezionare la casella di controllo **Avvio dell'applicazione non consentito**.
7. Salvare le modifiche.
8. Nell'elenco a discesa **Selezioni eventi**, selezionare la selezione creata.
9. Fare clic sul pulsante **Esegui selezione**.

Visualizzazione di un rapporto sulle applicazioni bloccate

Per visualizzare il rapporto sulle applicazioni bloccate:

1. Aprire Kaspersky Security Center Administration Console.
2. Nel nodo **Administration Server** della struttura di Administration Console selezionare la scheda **Rapporti**.
3. Fare clic su **Nuovo modello di rapporto**.

   Verrà avviata la Creazione guidata nuovo modello di rapporto.
4. Attenersi alle istruzioni della Creazione guidata nuovo modello di rapporto. Al passaggio **Selezione del tipo di modello di rapporto**, selezionare **Altro** → **Rapporto sulle applicazioni proibite**.

   Dopo avere completato la Creazione guidata nuovo modello di rapporto, il nuovo modello di rapporto viene visualizzato nella tabella della scheda **Rapporti**.
5. Aprire il rapporto facendo doppio clic.

Verrà avviato il processo di generazione del rapporto. Il rapporto viene visualizzato in una nuova finestra.

Verifica delle regole di Controllo applicazioni

Per garantire che le regole di Controllo applicazioni non blocchino le applicazioni necessarie per le attività lavorative, è consigliabile abilitare la verifica delle regole di Controllo applicazioni e analizzare il relativo funzionamento dopo la creazione di nuove regole. Quando la verifica delle regole di Controllo Applicazioni è abilitata, Kaspersky Endpoint Security non bloccherà le applicazioni il cui avvio non è consentito da Controllo Applicazioni, ma invierà notifiche sul relativo avvio all'Administration Server.

L'analisi dell'esecuzione delle regole di Controllo applicazioni richiede la verifica dei relativi eventi di Controllo applicazioni segnalati a Kaspersky Security Center. Il mancato rilevamento di eventi di avvio bloccato per tutte le applicazioni necessarie a livello lavorativo per l'utente del computer da parte della modalità test indica che sono state create le regole corrette. In caso contrario, è consigliabile aggiornare le impostazioni delle regole create, creare regole aggiuntive o eliminare le regole esistenti.

Per impostazione predefinita, Kaspersky Endpoint Security consente l'avvio di tutte le applicazioni ad eccezione delle applicazioni vietate dalle regole.

Abilitazione e disabilitazione del test delle regole di controllo delle applicazioni

Per abilitare o disabilitare il test delle regole di Controllo applicazioni in Kaspersky Security Center:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo applicazioni.
4. Nell'elenco a discesa **Modalità controllo**, selezionare uno dei seguenti elementi:

   - **Lista vietati**. Se è selezionata questa opzione, Controllo applicazioni consente a tutti gli utenti di avviare qualsiasi applicazione, fatta eccezione per i casi in cui vengono soddisfatte le condizioni delle regole di blocco di Controllo applicazioni.
   - **Lista consentiti**. Se è selezionata questa opzione, Controllo applicazioni impedisce a tutti gli utenti di avviare qualsiasi applicazione, fatta eccezione per i casi in cui vengono soddisfatte le condizioni delle regole di permesso di Controllo applicazioni.
5. Eseguire una delle seguenti operazioni:

   - Se si desidera abilitare il test delle regole di Controllo applicazioni, selezionare l'opzione **Testa regole** nell'elenco a discesa **Azione**.
   - Se si desidera abilitare Controllo applicazioni per gestire l'avvio delle applicazioni sui computer degli utenti, nell'elenco a discesa selezionare **Applica regole**.
6. Salvare le modifiche.

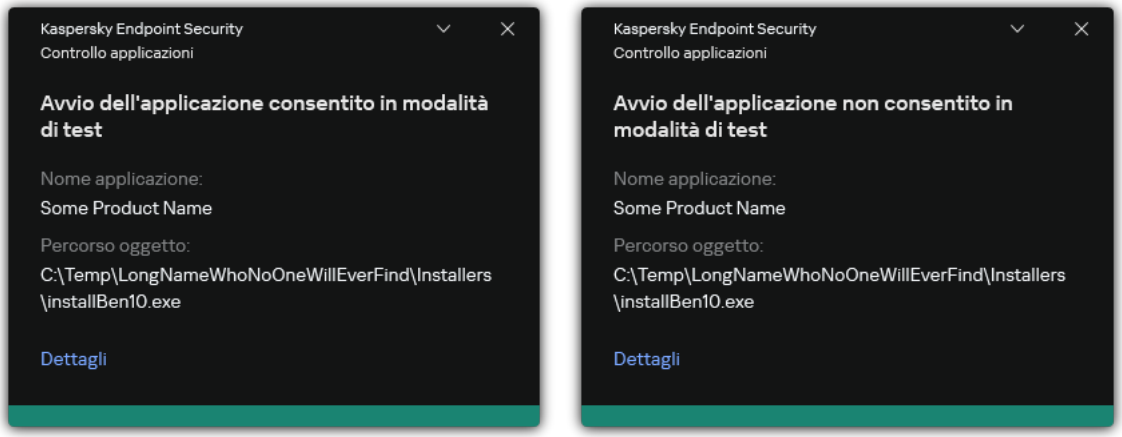
Per abilitare la verifica delle regole di Controllo applicazioni o per selezionare un'azione di blocco per Controllo applicazioni:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
3. Fare clic sul pulsante **Applicazioni bloccate** o **Applicazioni consentite**.

   Verrà visualizzato l'elenco delle regole di Controllo applicazioni.
4. Nella colonna **Stato** selezionare **Modalità di test**.

   Questo stato indica che Kaspersky Endpoint Security consente sempre l'avvio delle applicazioni a cui si applica la regola ma registra le informazioni relative all'avvio di tali applicazioni nel rapporto.
5. Salvare le modifiche.

Kaspersky Endpoint Security non bloccherà le applicazioni il cui avvio non è consentito dal componente Controllo Applicazioni, ma invierà notifiche sul relativo avvio all'Administration Server. È inoltre possibile configurare la visualizzazione delle notifiche sul test delle regole nel computer dell'utente (vedere la figura riportata di seguito).



Notifiche di Controllo applicazioni in modalità di test

Visualizzazione di un rapporto sulle applicazioni bloccate in modalità di test

Per visualizzare il rapporto sulle applicazioni bloccate in modalità di test:

1. Aprire Kaspersky Security Center Administration Console.
2. Nel nodo **Administration Server** della struttura di Administration Console selezionare la scheda **Rapporti**.
3. Fare clic su **Nuovo modello di rapporto**.

   Verrà avviata la Creazione guidata nuovo modello di rapporto.

4. Attenersi alle istruzioni della Creazione guidata nuovo modello di rapporto. Nel passaggio **Selezione del tipo di modello di rapporto**, selezionare **Altro → Rapporto sulle applicazioni vietate in modalità test**.

   Dopo avere completato la Creazione guidata nuovo modello di rapporto, il nuovo modello di rapporto viene visualizzato nella tabella della scheda **Rapporti**.

5. Aprire il rapporto facendo doppio clic.

Verrà avviato il processo di generazione del rapporto. Il rapporto viene visualizzato in una nuova finestra.

Visualizzazione degli eventi generati dall'operazione di test del componente Controllo applicazioni

Per visualizzare gli eventi di test di Controllo applicazioni ricevuti da Kaspersky Security Center:

1. Aprire Kaspersky Security Center Administration Console.
2. Nel nodo **Administration Server** della struttura di Administration Console selezionare la scheda **Eventi**.
3. Fare clic sul pulsante **Crea selezione**.
4. Nella finestra visualizzata, passare alla sezione **Eventi**.
5. Fare clic sul pulsante **Cancella tutto**.
6. Nella tabella **Eventi** selezionare le caselle di controllo **Avvio dell'applicazione non consentito in modalità di test** e **Avvio dell'applicazione consentito in modalità di test**.
7. Salvare le modifiche.
8. Nell'elenco a discesa **Selezioni eventi**, selezionare la selezione creata.
9. Fare clic sul pulsante **Esegui selezione**.

Monitor attività applicazioni

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server.

Monitor attività applicazioni è uno strumento progettato per la visualizzazione in tempo reale di informazioni sulle attività delle applicazioni nel computer di un utente.

L'utilizzo di Monitor attività applicazioni richiede l'installazione dei componenti Controllo applicazioni e Prevenzione Intrusioni Host. Se tali componenti non sono installati, la sezione Monitor attività applicazioni nella finestra principale dell'applicazione è nascosta.

Per avviare Monitor attività applicazioni:

Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **Monitor attività applicazioni**.

In questa finestra le informazioni sulle attività delle applicazioni nel computer dell'utente vengono presentate in tre schede:

- La scheda **Tutte le applicazioni** mostra le informazioni su tutte le applicazioni installate nel computer.
- La scheda **In esecuzione** mostra le informazioni sull'utilizzo delle risorse del computer da parte di ciascuna applicazione in tempo reale. Da questa scheda è anche possibile procedere alla configurazione delle autorizzazioni per una singola applicazione.
- La scheda **Esecuzione all'avvio** mostra l'elenco delle applicazioni avviate all'avvio del sistema operativo.

Se si desidera nascondere le informazioni sull'attività dell'applicazione sul computer dell'utente, è possibile limitare l'accesso dell'utente allo strumento Monitor attività applicazioni.

Come nascondere Monitor attività applicazioni nell'interfaccia dell'applicazione tramite Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Interfaccia**.
4. Utilizzare la casella di controllo **Nascondi sezione Monitor attività applicazioni** per concedere o revocare l'accesso allo strumento.
5. Salvare le modifiche.

Come nascondere Monitor attività applicazioni nell'interfaccia dell'applicazione tramite Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Interazione utente**.
5. Utilizzare la casella di controllo **Nascondi sezione Monitor attività applicazioni** per concedere o revocare l'accesso allo strumento.
6. Salvare le modifiche.

Regole per la creazione delle maschere dei nomi per file o cartelle

Una *maschera del nome di un file o di una cartella* è una rappresentazione del nome di una cartella o del nome e dell'estensione di un file in cui vengono utilizzati caratteri comuni.

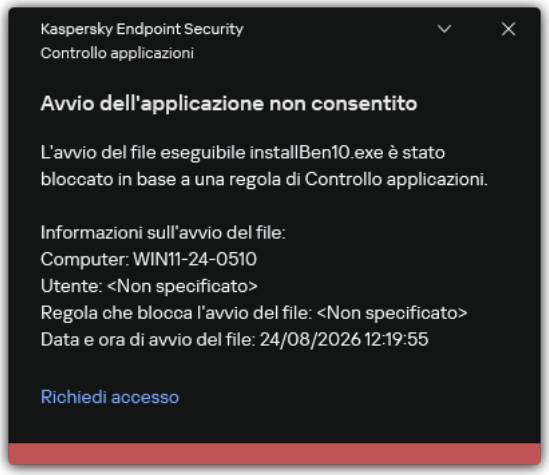
È possibile utilizzare i seguenti caratteri comuni per creare una maschera del nome di un file o di una cartella:

- Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri (incluso un set vuoto). Ad esempio, la maschera `C:\*.txt` includerà tutti i percorsi dei file con l'estensione `txt` situati nelle cartelle e nelle sottocartelle sull'unità (C:).

- Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

Modifica dei modelli dei messaggi di Controllo applicazioni

Quando un utente tenta di avviare un'applicazione bloccata da una regola di Controllo Applicazioni, Kaspersky Endpoint Security visualizza un messaggio che segnala che l'avvio dell'applicazione è stato bloccato. Gli esperti di Kaspersky forniscono un modello di messaggio all'utente in cui vengono descritti i motivi per cui l'applicazione è stata bloccata (vedere la figura seguente). Sono disponibili variabili speciali per la gestione del modello di messaggio (ad esempio `%USER_NAME%`). Le variabili consentono di utilizzare un unico modello di messaggio per computer diversi. Quando si genera un messaggio, Kaspersky Endpoint Security recupera il valore della variabile dalle impostazioni del sistema operativo e lo inserisce nel messaggio corrispondente al computer, all'utente e all'evento specifici.



Notifica di Controllo applicazioni

Se l'utente ritiene che l'avvio dell'applicazione sia stato bloccato per errore, può utilizzare il collegamento nel testo del messaggio per inviare un messaggio all'amministratore della rete aziendale locale. A tale scopo, l'utente deve fare clic sul pulsante **Richiedi accesso** e inviare un messaggio all'amministratore descrivendo la situazione. È inoltre possibile preparare un modello per il messaggio per l'amministratore, aggiungendovi dati che potrebbero aiutare a decidere se consentire o bloccare l'accesso all'applicazione. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'avvio di un'applicazione**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato.

Come modificare il modello di messaggio di Controllo applicazioni in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
4. Nel blocco **Impostazioni dei modelli di messaggio**, fare clic sul pulsante **Modelli**.
5. Viene visualizzata una finestra; in tale finestra, configurare i modelli di Controllo applicazioni:

   - **Messaggio relativo al blocco**. Modello del messaggio visualizzato quando viene attivata una regola di Controllo applicazioni che blocca l'avvio di un'applicazione.

     Non è possibile configurare modelli di messaggio per Controllo applicazioni in modalità di test. Controllo applicazioni in modalità di test mostra le notifiche preimpostate.

   - **Messaggio all'amministratore**. Modello del messaggio che un utente può inviare all'amministratore della LAN aziendale se l'utente ritiene che un'applicazione sia stata bloccata per errore.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

   È anche possibile ripristinare il testo predefinito del modello utilizzando il pulsante **Predefinito**.

6. Salvare le modifiche.

Come modificare il modello di messaggio di Controllo applicazioni in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Controllo app**.

5. Nel blocco **Modelli di messaggi**, fare clic sul collegamento **Messaggi relativi al blocco dell'avvio delle applicazioni** e configurare modelli per i messaggi di Controllo applicazioni:

   - **Messaggio all'utente**. Modello del messaggio visualizzato quando viene attivata una regola di Controllo applicazioni che blocca l'avvio di un'applicazione.

     Non è possibile configurare modelli di messaggio per Controllo applicazioni in modalità di test. Controllo applicazioni in modalità di test mostra le notifiche preimpostate.

   - **Messaggio all'amministratore**. Modello del messaggio che un utente può inviare all'amministratore della LAN aziendale se l'utente ritiene che un'applicazione sia stata bloccata per errore.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Aggiungi variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

   È anche possibile ripristinare il testo predefinito del modello utilizzando il pulsante **Ripristina condizioni originali**.

6. Salvare le modifiche.

Come modificare il modello di messaggio di Controllo applicazioni nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo applicazioni**.

3. Nel blocco **Modelli di messaggi sul blocco delle applicazioni**, configurare i modelli per i messaggi di Controllo applicazioni:

   - **Messaggio relativo al blocco**. Modello del messaggio visualizzato quando viene attivata una regola di Controllo applicazioni che blocca l'avvio di un'applicazione.

     Non è possibile configurare modelli di messaggio per Controllo applicazioni in modalità di test. Controllo applicazioni in modalità di test mostra le notifiche preimpostate.

   - **Messaggio all'amministratore**. Modello del messaggio che un utente può inviare all'amministratore della LAN aziendale se l'utente ritiene che un'applicazione sia stata bloccata per errore.

   Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Aggiungi variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

   È anche possibile ripristinare il testo predefinito del modello utilizzando il pulsante **Reimposta**.

4. Salvare le modifiche.

Variabili nei modelli di messaggi di Controllo applicazioni

È possibile utilizzare le seguenti variabili nei modelli di messaggi dell'utente o nei modelli di messaggi dell'amministratore:

- **Nome della regola attivata** - `%RULE%`.

  Nome della regola che ha bloccato l'esecuzione di un file.

- **Data corrente** - `%DATE%`.

  Data in cui l'esecuzione del file è stata bloccata nel formato DD.MM.YYYY.

- **Ora corrente** - `%TIME%`.

  Ora in cui è stata bloccata l'esecuzione del file nel formato HH:MM.

- **Nome utente** - `%USER_NAME%`.

  Nome dell'account utente corrente nel computer in cui è stata bloccata l'esecuzione del file, in formato `<device name>\<user alias>` (ad esempio, `DESKTOP-123\John.Smith`).

- **Nome computer** - `%COMPUTER_NAME%`.

  Nome del computer in cui è stata bloccata l'esecuzione del file.

- **Nome del file eseguibile** - `%FILE_NAME%`.

  Nome del file eseguibile dell'applicazione bloccata.

- **Categoria KL del file eseguibile** - `%KL_CAT%`.

  Categoria KL a cui appartiene l'applicazione bloccata (ad esempio, *Browser* o un'altra categoria).

- **Percorso del file eseguibile** - `%FILE_PATH%`.

  Percorso completo del file eseguibile dell'applicazione bloccata.

- **Versione del file eseguibile** - `%FILE_VERSION%`.

  Versione del file eseguibile dell'applicazione bloccata.

- **Nome originale del file eseguibile** - `%ORIGINAL_FILE_NAME%`.

  Nome originale del file eseguibile dell'applicazione bloccata. Il nome del file è specificato nelle proprietà del file eseguibile dell'applicazione.

- **Produttore** - `%FILE_PUBLISHER%`.

  Produttore dell'applicazione bloccata.

- **Nome applicazione** - `%FILE_PRODUCT_NAME%`.

  Nome dell'applicazione bloccata.

- **Versione dell'applicazione** - `%PRODUCT_VERSION%`.

  Versione dell'applicazione bloccata.

- **Hash del file eseguibile** - `%FILE_HASH%`.

  Hash del file eseguibile dell'applicazione bloccata.

- **Autorità di emissione del certificato** - `%CERT_ISSUER%`.

  Emittente del certificato con cui è firmato il file eseguibile.

- **Soggetto del certificato** - `%CERT_SUBJECT%`.

  Oggetto del certificato con cui è firmato il file eseguibile.

- **Identificazione personale certificato** - `%CERT_THUMBPRINT%`.

  Identificazione personale del certificato con cui è firmato il file eseguibile.

Procedure consigliate per l'inventario dei file eseguibili

L'attività *Inventario* raccoglie informazioni sui file eseguibili (ad esempio EXE, BAT e CMD), sui moduli DLL e sugli script (PowerShell, JS e altri). Queste informazioni sono necessarie per configurare le categorie di Controllo Applicazioni e le autorizzazioni delle applicazioni per il componente Prevenzione Intrusioni Host. L'attività *Inventario* deve essere eseguita periodicamente per mantenere aggiornate le informazioni. L'attività *Inventario*, analogamente all'attività *Scansione malware*, richiede un utilizzo intensivo delle risorse. Pertanto, è consigliabile configurare l'esecuzione dell'attività durante la notte o nei fine settimana.

Fasi dell'inventario dei file eseguibili

1. Selezionare il gruppo di computer di riferimento in cui è installato il set di software tipico. È consigliabile ridurre al minimo il numero di computer per la procedura di inventario dei file eseguibili. Minore è il numero di attività *Inventario*, minore è il carico su Kaspersky Security Center Administration Server.

2. Spostare i computer di riferimento in un gruppo di amministrazione separato nella console di Kaspersky Security Center. È possibile denominare il gruppo, ad esempio, *Computer di riferimento*.

3. Creare un'attività *Inventario* per il gruppo di amministrazione *Computer di riferimento*. È consigliabile mantenere le impostazioni predefinite dell'attività.

Esempio di inventario dei file eseguibili in un'organizzazione

Ad esempio, un'organizzazione dispone di 100 computer che eseguono Windows 11 25H2. Tutti i computer hanno la stessa release e la stessa localizzazione del sistema operativo. Anche il set di aggiornamenti installati nei computer è lo stesso.

In un'organizzazione di questo tipo non è necessario eseguire l'attività *Inventario* in tutti i computer. La maggior parte dei file eseguibili in questi computer è identica. È sufficiente creare un'attività per un solo computer di riferimento. È possibile creare ulteriori attività *Inventario* per i computer con una configurazione diversa da quella di riferimento.

Best practice per l'implementazione di un elenco di applicazioni consentite

Durante la pianificazione dell'implementazione di un elenco di applicazioni consentite, è consigliabile eseguire le seguenti azioni:

1. Formare i seguenti tipi di gruppi:

   - Gruppi di utenti. Gruppi di utenti per cui si desidera consentire l'utilizzo di diversi set di applicazioni.

   - Gruppi di amministrazione. Uno o più gruppi di computer a cui Kaspersky Security Center applicherà l'elenco delle applicazioni consentite. È necessario creare più gruppi di computer se per tali gruppi vengono utilizzate impostazioni della Lista consentiti diverse.

2. Creare un elenco di applicazioni per cui l'avvio deve essere consentito.

   Prima di creare un elenco, è consigliabile eseguire le seguenti operazioni:

   a. Eseguire l'attività di inventario.

      Le informazioni sulla creazione, la riconfigurazione e l'avvio di un'attività di inventario sono disponibili nella sezione Gestione attività.

   b. Visualizzare l'elenco dei file eseguibili.

Configurazione della modalità Lista consentiti per le applicazioni

Durante la configurazione della modalità Lista consentiti, è consigliabile eseguire le seguenti azioni:

1. Creare categorie di applicazioni contenenti applicazioni per cui l'avvio deve essere consentito.

   È possibile selezionare uno dei seguenti metodi per la creazione di categorie di applicazioni:

   - **Categoria con contenuto aggiunto manualmente**. È possibile aggiungere manualmente contenuti a questa categoria utilizzando le seguenti condizioni:
     - Metadati file. Kaspersky Security Center aggiunge tutti i file eseguibili insieme ai metadati specificati alla categoria di applicazioni.
     - Codice hash file. Kaspersky Security Center aggiunge tutti i file eseguibili con l'hash specificato alla categoria di applicazioni.

       L'utilizzo di questa condizione esclude la possibilità di installare automaticamente gli aggiornamenti poiché le diverse versioni dei file avranno hash diversi.

     - Certificato file. Kaspersky Security Center aggiunge tutti i file eseguibili firmati con il certificato specificato alla categoria di applicazioni.
     - Categoria KL. Kaspersky Security Center aggiunge tutte le applicazioni che si trovano nella categoria KL specificata alla categoria di applicazioni.
     - Cartella applicazione. Kaspersky Security Center aggiunge tutti i file eseguibili di questa cartella alla categoria di applicazioni.

       L'utilizzo della condizione **Cartella applicazione** può essere pericoloso poiché verrà consentito l'avvio di tutte le applicazioni della cartella specificata. È consigliabile applicare le regole che utilizzano le categorie di applicazioni con la condizione **Cartella applicazione** solo agli utenti per cui è necessario consentire l'installazione automatica degli aggiornamenti.

   - **Categoria che include file eseguibili di una cartella specifica**. È possibile specificare una cartella da cui i file eseguibili verranno assegnati automaticamente alla categoria di applicazioni creata.

- **Categoria che include i file eseguibili dei dispositivi selezionati**. È possibile specificare un computer per cui tutti i file eseguibili verranno assegnati automaticamente alla categoria di applicazioni creata.

  Quando si utilizza questo metodo per la creazione di categorie di applicazioni, Kaspersky Security Center riceve le informazioni sulle applicazioni nel computer dalla cartella **File eseguibili**.

2. Selezionare la modalità Lista consentiti per il componente Controllo applicazioni.

3. Creare le regole di Controllo applicazioni utilizzando le categorie di applicazioni create.

   La regola **Immagine gold** e la regola **Programmi di aggiornamento attendibili** sono inizialmente definite per la modalità Lista consentiti. Queste regole di Controllo applicazioni corrispondono alle categorie KL. La categoria KL "*Immagine gold*" include i programmi che garantiscono l'esecuzione standard del sistema operativo. La categoria KL "*Programmi di aggiornamento attendibili*" include i programmi di aggiornamento per i più affidabili produttori di software. È impossibile eliminare queste regole. Le impostazioni di queste regole non possono essere modificate. Per impostazione predefinita, la regola **Immagine gold** è abilitata e la regola **Programmi di aggiornamento attendibili** è disabilitata. Tutti gli utenti possono avviare le applicazioni che corrispondono alle condizioni di attivazione di queste regole.

4. Determinare le applicazioni per cui deve essere consentita l'installazione automatica degli aggiornamenti.

   È possibile consentire l'installazione automatica degli aggiornamenti in uno dei seguenti modi:

   - Specificare un elenco esteso delle applicazioni consentite permettendo l'avvio di tutte le applicazioni che appartengono a una categoria KL.

   - Specificare un elenco esteso delle applicazioni consentite permettendo l'avvio di tutte le applicazioni firmate con i certificati.

     Per consentire l'avvio di tutte le applicazioni firmate con certificati, è possibile creare una categoria con una condizione basata sul certificato che utilizza solo il parametro **Oggetto** con il valore `*`.

   - Per la regola di Controllo applicazioni selezionare il parametro **Programmi di aggiornamento attendibili**. Se questa casella di controllo è selezionata, Kaspersky Endpoint Security considera come Programmi di aggiornamento attendibili le applicazioni incluse nella regola. Kaspersky Endpoint Security consente l'avvio delle applicazioni installate o aggiornate dalle applicazioni incluse nella regola della categoria, a condizione che a tali applicazioni non si applichi alcuna regola di blocco.

     Quando viene eseguita la migrazione delle impostazioni di Kaspersky Endpoint Security, viene eseguita anche la migrazione dell'elenco dei file eseguibili creato dai programmi di aggiornamento attendibili.

   - Creare una cartella e inserirvi i file eseguibili delle applicazioni per cui si desidera consentire l'installazione automatica degli aggiornamenti. Creare quindi una categoria di applicazioni con la condizione **Cartella applicazione** e specificare il percorso di tale cartella. Creare quindi una regola di permesso e selezionare questa categoria.

     L'utilizzo della condizione **Cartella applicazione** può essere pericoloso poiché verrà consentito l'avvio di tutte le applicazioni della cartella specificata. È consigliabile applicare le regole che utilizzano le categorie di applicazioni con la condizione **Cartella applicazione** solo agli utenti per cui è necessario consentire l'installazione automatica degli aggiornamenti.

Test della modalità Lista consentiti

Per garantire che le regole di Controllo applicazioni non blocchino le applicazioni necessarie per le attività lavorative, è consigliabile abilitare la verifica delle regole di Controllo applicazioni e analizzare il relativo funzionamento dopo la creazione di nuove regole. Quando la verifica è abilitata, Kaspersky Endpoint Security non bloccherà le applicazioni il cui avvio non è consentito dalle regole di Controllo Applicazioni, ma invierà notifiche sul relativo avvio all'Administration Server.

Durante il test della modalità Lista consentiti, è consigliabile eseguire le seguenti azioni:

1. Determinare il periodo di test (da diversi giorni a due mesi).
2. Abilitare la verifica delle regole di Controllo applicazioni.
3. Esaminare gli eventi generati dal test dell'esecuzione di Controllo applicazioni e i rapporti sulle applicazioni bloccate in modalità di test per analizzare i risultati dei test.
4. In base ai risultati dell'analisi, apportare modifiche alle impostazioni della modalità Lista consentiti.

   In particolare, in base ai risultati dei test, è possibile aggiungere file eseguibili relativi agli eventi a una categoria di applicazioni.

Supporto per la modalità Lista consentiti

Dopo aver selezionato un'azione di blocco per Controllo applicazioni è consigliabile continuare a supportare la modalità Lista consentiti eseguendo le seguenti azioni:

- Esaminare gli eventi generati dell'esecuzione di Controllo applicazioni e i rapporti sulle esecuzioni bloccate per analizzare l'efficacia di Controllo applicazioni.
- Analizzare le richieste di accesso alle applicazioni degli utenti.
- Analizzare i file eseguibili sconosciuti verificandone la reputazione in Kaspersky Security Network.
- Prima dell'installazione degli aggiornamenti per il sistema operativo o per il software, installare tali aggiornamenti in un gruppo di test di computer per verificare la modalità con la quale verranno elaborati dalle regole di Controllo applicazioni.
- Aggiungere le applicazioni necessarie alle categorie utilizzate nelle regole di Controllo applicazioni.

Monitoraggio delle porte di rete

Durante l'esecuzione di Kaspersky Endpoint Security, i componenti Controllo Web, Protezione minacce di posta, Protezione minacce web, Rilevamento del Comportamento e Prevenzione Exploit monitorano i flussi di dati trasmessi tramite specifici protocolli e che attraversano specifiche porte TCP e UDP aperte nel computer dell'utente. Ad esempio, il componente Protezione minacce di posta analizza le informazioni trasmesse tramite SMTP, mentre il componente Protezione minacce web analizza le informazioni trasmesse tramite HTTP e FTP.

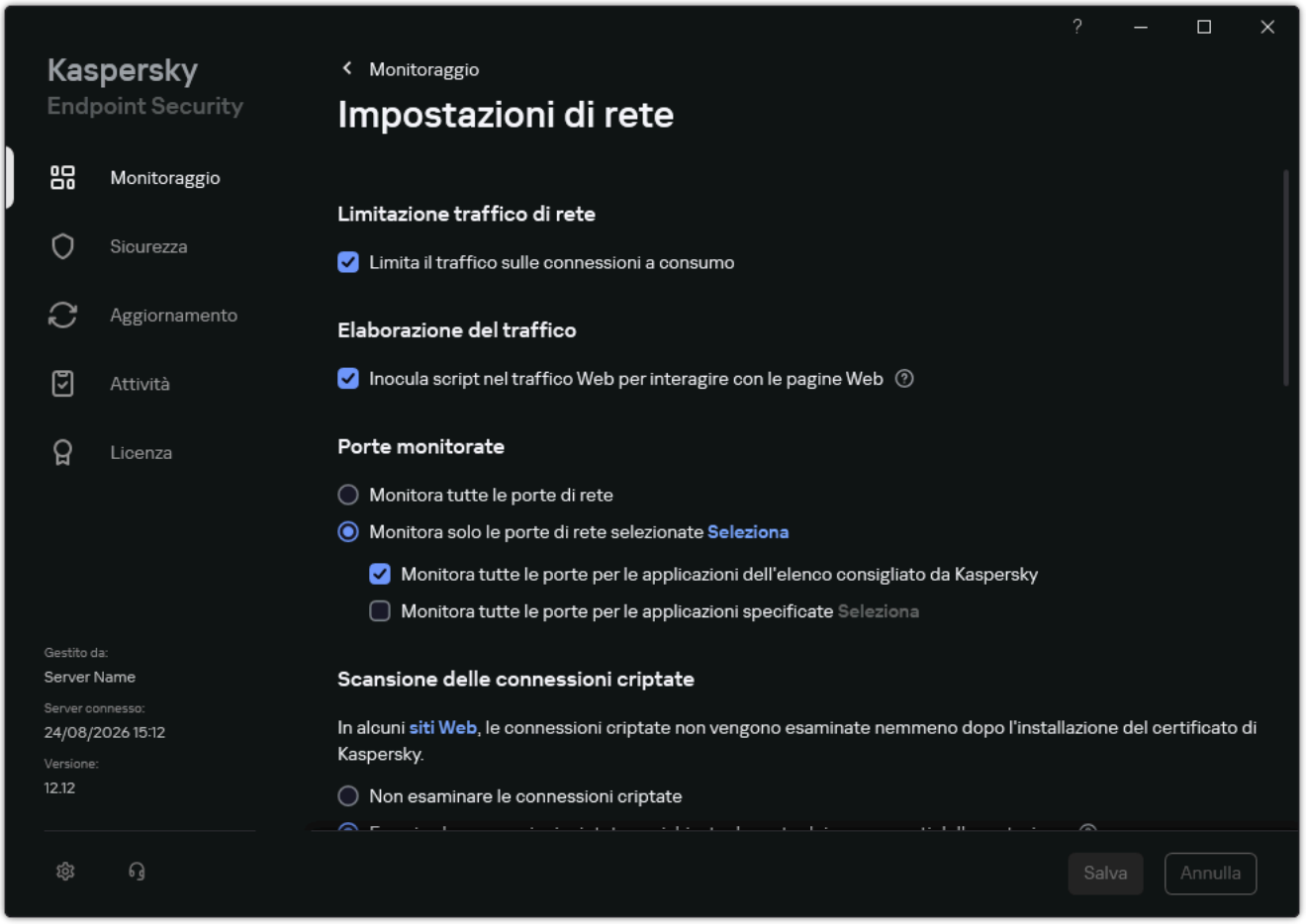
Kaspersky Endpoint Security suddivide le porte TCP e UDP del computer dell'utente in diversi gruppi, a seconda della probabilità che vengano compromesse. Alcune porte di rete sono riservate per i servizi vulnerabili. È consigliabile monitorare queste porte più attentamente poiché hanno più probabilità di essere colpite da un attacco di rete. Se si utilizzano servizi non standard che fanno uso di porte non standard, anche queste porte possono subire un attacco. È possibile specificare un elenco di porte di rete e un elenco di applicazioni che richiedono l'accesso alla rete. A queste porte e applicazioni viene quindi riservata un'attenzione particolare dai componenti Protezione minacce di posta e Protezione minacce web durante il monitoraggio del traffico di rete.

Per contribuire a garantire la protezione del computer, i componenti Rilevamento del Comportamento e Prevenzione Exploit monitorano inoltre i flussi di dati che transitano nelle porte di rete. I componenti monitorano continuamente il traffico di rete alla ricerca di singoli processi che potrebbero rappresentare una minaccia.

Abilitazione del monitoraggio di tutte le porte di rete

Per abilitare il monitoraggio di tutte le porte di rete:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.



Impostazioni di monitoraggio delle porte di rete

3. Nel blocco **Porte monitorate**, selezionare **Monitora tutte le porte di rete**.
4. Salvare le modifiche.

Creazione di un elenco di porte di rete monitorate

Per creare un elenco di porte di rete monitorate:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.
3. Nel blocco **Porte monitorate**, selezionare **Monitora solo le porte di rete selezionate**.
4. Fare clic su **Seleziona**.

   Verrà visualizzato un elenco di porte di rete normalmente utilizzate per la trasmissione del traffico di posta elettronica e di rete. Questo elenco di porte di rete è incluso nel pacchetto di Kaspersky Endpoint Security.
5. Utilizzare l'interruttore nella colonna **Stato** per abilitare o disabilitare il monitoraggio delle porte di rete.
6. Se una porta di rete non viene visualizzata nell'elenco delle porte di rete, aggiungerla eseguendo le seguenti operazioni:
   a. Fare clic su **Aggiungi**.
   b. Nella finestra visualizzata immettere il numero della porta di rete e una breve descrizione.
   c. Impostare lo stato **Attivo** o **Inattivo** per il monitoraggio delle porte di rete.
7. Salvare le modifiche.

Quando il protocollo FTP viene eseguito in modalità passiva, la connessione può essere stabilita tramite una porta di rete casuale non aggiunta all'elenco delle porte di rete monitorate. Per proteggere tali connessioni, abilitare il monitoraggio di tutte le porte di rete o configurare il controllo delle porte di rete per le applicazioni che stabiliscono connessioni FTP.

Creazione di un elenco di applicazioni per cui monitorare tutte le porte di rete

È possibile creare un elenco di applicazioni per cui Kaspersky Endpoint Security monitora tutte le porte di rete.

È consigliabile includere le applicazioni che ricevono o trasmettono i dati tramite il protocollo FTP nell'elenco delle applicazioni per cui Kaspersky Endpoint Security monitora tutte le porte di rete.

Per creare un elenco di applicazioni per cui monitorare tutte le porte di rete:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni di rete**.
3. Nel blocco **Porte monitorate**, selezionare **Monitora solo le porte di rete selezionate**.

4. Selezionare la casella di controllo **Monitora tutte le porte per le applicazioni dell'elenco consigliato da Kaspersky**.

   Se questa casella di controllo è selezionata, Kaspersky Endpoint Security monitora tutte le porte per le seguenti applicazioni:

   - Adobe Acrobat Reader.
   - Supporto delle applicazioni Apple.
   - Google Chrome.
   - Microsoft Edge.
   - Mozilla Firefox.
   - Internet Explorer.
   - Java.
   - mIRC.
   - Opera.
   - Pidgin.
   - Safari.
   - Mail.ru Agent.
   - Yandex Browser.

5. Selezionare la casella di controllo **Monitora tutte le porte per le applicazioni specificate**.
6. Fare clic su **Seleziona**.

   Verrà visualizzato un elenco di applicazioni per cui Kaspersky Endpoint Security monitora le porte di rete.

7. Utilizzare l'interruttore nella colonna **Stato** per abilitare o disabilitare il monitoraggio delle porte di rete.
8. Se un'applicazione non è inclusa nell'elenco delle applicazioni, aggiungerla nel modo seguente:

   a. Fare clic su **Aggiungi**.

   b. Nella finestra visualizzata immettere il percorso del file eseguibile dell'applicazione e una breve descrizione.

   c. Impostare lo stato **Attivo** o **Inattivo** per il monitoraggio delle porte di rete.

9. Salvare le modifiche.

Esportazione e importazione degli elenchi delle porte monitorate

Kaspersky Endpoint Security utilizza i seguenti elenchi per monitorare le porte di rete: elenco delle porte di rete ed elenco delle applicazioni le cui porte sono monitorate da Kaspersky Endpoint Security. È possibile esportare gli elenchi delle porte monitorate in un file XML. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di porte con la stessa descrizione. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup degli elenchi delle porte monitorate o per eseguire la migrazione degli elenchi in un server diverso.

Come esportare e importare gli elenchi delle porte monitorate in Administration Console (MMC)

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di rete**.
5. Per esportare l'elenco delle porte di rete:
   a. Nel blocco **Porte monitorate**, selezionare **Monitora solo le porte di rete selezionate**.
   b. Fare clic sul collegamento **selezionate N porte**.

      Verrà visualizzata la finestra **Porte di rete**. La finestra **Porte di rete** visualizza un elenco delle porte di rete normalmente utilizzate per la trasmissione del traffico di posta elettronica e di rete. Questo elenco di porte di rete è incluso nel pacchetto di Kaspersky Endpoint Security.
   c. Nell'elenco delle porte di rete selezionare le porte che si desidera esportare.
   d. Fare clic su **Esporta**.
   e. Nella finestra visualizzata, immettere il nome del file XML in cui si desidera esportare l'elenco di porte di rete e selezionare la cartella in cui si desidera salvare il file.
   f. Salvare il file.

      Kaspersky Endpoint Security esporta l'intero elenco delle porte di rete nel file XML.
6. Per esportare l'elenco delle applicazioni le cui porte sono monitorate da Kaspersky Endpoint Security:
   a. Nella sezione **Porte monitorate** selezionare la casella di controllo **Monitora tutte le porte per le applicazioni specificate**.
   b. Fare clic sul collegamento **selezionate N applicazioni**.
   c. Nell'elenco delle applicazioni selezionare le applicazioni che si desidera esportare.
   d. Fare clic su **Esporta**.
   e. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle applicazioni e selezionare la cartella in cui si desidera salvare il file.

f. Salvare il file.

Kaspersky Endpoint Security esporta l'intero elenco di applicazioni nel file XML.

7. Per importare l'elenco delle porte di rete:

a. Nell'elenco delle porte di rete fare clic sul pulsante **Importa**.

Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle porte di rete.

b. Aprire il file.

Se il computer dispone già di un elenco delle porte di rete, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

8. Per esportare un elenco di applicazioni le cui porte sono monitorate da Kaspersky Endpoint Security:

a. Nell'elenco delle applicazioni fare clic sul pulsante **Importa**.

Nella finestra visualizzata, selezionare il file XML da cui si desidera importare l'elenco delle applicazioni.

b. Aprire il file.

Se il computer dispone già di un elenco di applicazioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

9. Salvare le modifiche.

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni di rete**.

4. Nel blocco **Porte monitorate**, selezionare **Monitora solo le porte di rete selezionate**.

5. Fare clic su **Impostazioni**.

Verrà visualizzata la finestra **Porte di rete**. La finestra **Porte di rete** visualizza un elenco delle porte di rete normalmente utilizzate per la trasmissione del traffico di posta elettronica e di rete. Questo elenco di porte di rete è incluso nel pacchetto di Kaspersky Endpoint Security.

6. Per esportare l'elenco delle porte di rete:

a. Nell'elenco delle porte di rete selezionare le porte che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.

Se non è stata selezionata alcuna porta, Kaspersky Endpoint Security esporterà tutte le porte.

b. Fare clic su **Esporta**.

c. Nella finestra visualizzata, immettere il nome del file XML in cui si desidera esportare l'elenco di porte di rete e selezionare la cartella in cui si desidera salvare il file.

d. Salvare il file.

Kaspersky Endpoint Security esporta l'intero elenco delle porte di rete nel file XML.

7. Per esportare l'elenco delle applicazioni le cui porte sono monitorate da Kaspersky Endpoint Security:

   a. Selezionare la casella di controllo **Monitora tutte le porte per le applicazioni specificate**.

   b. Nell'elenco delle applicazioni selezionare le applicazioni che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.

      Se non è stata selezionata alcuna applicazione, Kaspersky Endpoint Security esporterà tutte le applicazioni.

   c. Fare clic su **Esporta**.

   d. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle applicazioni e selezionare la cartella in cui si desidera salvare il file.

   e. Salvare il file.

      Kaspersky Endpoint Security esporta l'intero elenco di applicazioni nel file XML.

8. Per importare l'elenco delle porte di rete:

   a. Nell'elenco delle porte di rete fare clic sul pulsante **Importa**.

      Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle porte di rete.

   b. Aprire il file.

      Se il computer dispone già di un elenco delle porte di rete, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

9. Per esportare un elenco di applicazioni le cui porte sono monitorate da Kaspersky Endpoint Security:

   a. Nell'elenco delle applicazioni fare clic sul pulsante **Importa**.

      Nella finestra visualizzata, selezionare il file XML da cui si desidera importare l'elenco delle applicazioni.

   b. Aprire il file.

      Se il computer dispone già di un elenco di applicazioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

10. Salvare le modifiche.

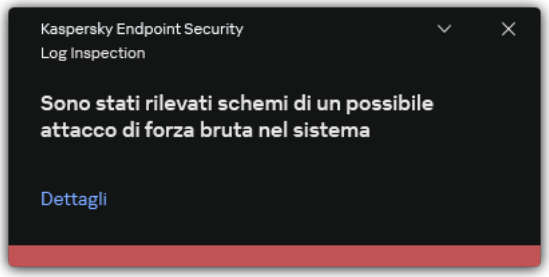
Log Inspection

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation.

Log Inspection monitora l'integrità dell'ambiente protetto in base all'analisi del Registro eventi di Windows. Quando l'applicazione rileva segnali di comportamento atipico nel sistema, ne informa l'amministratore, poiché questo comportamento potrebbe indicare un tentativo di attacco informatico.

Kaspersky Endpoint Security analizza i registri eventi di Windows e rileva le violazioni in base alle regole. Il componente include regole predefinite. Le regole predefinite sono basate sull'analisi euristica. È inoltre possibile aggiungere le proprie regole (regole personalizzate). Quando si attiva una regola, l'applicazione crea un evento con lo stato *Critico* (vedere la figura riportata di seguito).

Se si desidera utilizzare Log Inspection, verificare che le impostazioni di sicurezza del criterio di controllo siano configurate e che il sistema stia registrando gli eventi pertinenti (per ulteriori dettagli, visitare il sito Web dell'Assistenza tecnica Microsoft).



Notifica di Log Inspection

Configurazione delle regole predefinite

Le regole predefinite includono modelli di attività anomale nel computer protetto. Le attività anomale possono indicare un tentativo di attacco. Le regole predefinite sono basate sull'analisi euristica. Sono disponibili sette regole predefinite per Log Inspection. È possibile abilitare o disabilitare una qualsiasi delle regole. Le regole predefinite non possono essere eliminate.

È possibile configurare i criteri di attivazione per le regole che monitorano gli eventi per le seguenti operazioni:

- Rilevamento forza bruta password
- Rilevamento degli accessi di rete

Come configurare le regole predefinite in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Log Inspection**.
4. Verificare che la casella di controllo **Log Inspection** sia selezionata.
5. Nel blocco **Regole predefinite**, fare clic sul pulsante **Impostazioni**.
6. Selezionare o deselezionare le caselle di controllo per configurare le regole predefinite:
   - **Sono stati rilevati schemi di un possibile attacco di forza bruta nel sistema**.
   - **Sono state rilevate attività atipiche durante una sessione di accesso alla rete**.
   - **Sono stati rilevati schemi di un possibile abuso del Registro eventi di Windows**.

- **Rilevate azioni atipiche per conto di un nuovo servizio installato**.
- **Rilevato un accesso atipico che utilizza credenziali esplicite**.
- **Sono stati rilevati schemi di un possibile attacco PAC falsificato con Kerberos (MS14-068) nel sistema**.
- **Rilevate modifiche sospette nel gruppo Amministratori integrato con privilegi**.

7. Se necessario, configurare l'attività **Sono stati rilevati schemi di un possibile attacco di forza bruta nel sistema**:
   a. Fare clic sul pulsante **Impostazioni** sotto la regola.
   b. Nella finestra visualizzata, specificare il numero di tentativi e un periodo di tempo entro il quale devono essere eseguiti i tentativi di immissione di una password affinché la regola venga attivata.
   c. Fare clic su **OK**.
8. Se è stata selezionata la regola **Sono state rilevate attività atipiche durante una sessione di accesso alla rete**, è necessario configurarne le impostazioni:
   a. Fare clic sul pulsante **Impostazioni** sotto la regola.
   b. Nel blocco **Rilevamento degli accessi di rete**, specificare l'inizio e la fine dell'intervallo di tempo.
      Kaspersky Endpoint Security considera i tentativi di accesso eseguiti durante l'intervallo definito come attività anomale.
      Per impostazione predefinita, l'intervallo non è impostato e l'applicazione non monitora i tentativi di accesso. Per consentire all'applicazione di monitorare continuamente i tentativi di accesso, impostare l'intervallo tra le 00:00 e le 23:59. L'inizio e la fine dell'intervallo non devono coincidere. Se sono identici, l'applicazione non monitora i tentativi di accesso.
   c. Creare l'elenco degli utenti attendibili e degli indirizzi IP attendibili (IPv4 e IPv6).
      È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio. Kaspersky Endpoint Security non monitora i tentativi di accesso per questi utenti e computer.
   d. Fare clic su **OK**.
9. Salvare le modifiche.

Come configurare le regole predefinite in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Log Inspection**.
5. Verificare che l'interruttore **Log Inspection ABILITATA** sia attivato.

6. Nel blocco **Regole predefinite**, abilitare o disabilitare le regole predefinite utilizzando gli interruttori:

   - **Sono stati rilevati schemi di un possibile attacco di forza bruta nel sistema**.
   - **Sono state rilevate attività atipiche durante una sessione di accesso alla rete**.
   - **Sono stati rilevati schemi di un possibile abuso del Registro eventi di Windows**.
   - **Rilevate azioni atipiche per conto di un nuovo servizio installato**.
   - **Rilevato un accesso atipico che utilizza credenziali esplicite**.
   - **Sono stati rilevati schemi di un possibile attacco PAC falsificato con Kerberos (MS14-068) nel sistema**.

   a. **Rilevate modifiche sospette nel gruppo Amministratori integrato con privilegi**.

7. Se necessario, configurare l'attività **Sono stati rilevati schemi di un possibile attacco di forza bruta nel sistema**:

   a. Fare clic su **Impostazioni** sotto la regola.

   b. Nella finestra visualizzata, specificare il numero di tentativi e un periodo di tempo entro il quale devono essere eseguiti i tentativi di immissione di una password affinché la regola venga attivata.

   c. Fare clic su **OK**.

8. Se è stata selezionata la regola **Sono state rilevate attività atipiche durante una sessione di accesso alla rete**, è necessario configurarne le impostazioni:

   a. Fare clic su **Impostazioni** sotto la regola.

   b. Nel blocco **Rilevamento degli accessi di rete**, specificare l'inizio e la fine dell'intervallo di tempo.

   Kaspersky Endpoint Security considera i tentativi di accesso eseguiti durante l'intervallo definito come attività anomale.

   Per impostazione predefinita, l'intervallo non è impostato e l'applicazione non monitora i tentativi di accesso. Per consentire all'applicazione di monitorare continuamente i tentativi di accesso, impostare l'intervallo tra le 00:00 e le 23:59. L'inizio e la fine dell'intervallo non devono coincidere. Se sono identici, l'applicazione non monitora i tentativi di accesso.

   c. Nel blocco **Esclusioni**, aggiungere utenti attendibili e indirizzi IP attendibili (IPv4 e IPv6).

   È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio. Kaspersky Endpoint Security non monitora i tentativi di accesso per questi utenti e computer.

   d. Fare clic su **OK**.

9. Salvare le modifiche.

Come configurare le regole predefinite nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Log Inspection**.

3. Verificare che l'interruttore **Log Inspection** sia attivato.

4. Nel blocco **Regole predefinite**, fare clic sul pulsante **Configura**.

5. Selezionare o deselezionare le caselle di controllo per configurare le regole predefinite:

   - **Sono stati rilevati schemi di un possibile attacco di forza bruta nel sistema**.
   - **Sono state rilevate attività atipiche durante una sessione di accesso alla rete**.
   - **Sono stati rilevati schemi di un possibile abuso del Registro eventi di Windows**.
   - **Rilevate azioni atipiche per conto di un nuovo servizio installato**.
   - **Rilevato un accesso atipico che utilizza credenziali esplicite**.
   - **Sono stati rilevati schemi di un possibile attacco PAC falsificato con Kerberos (MS14-068) nel sistema**.

   a. **Rilevate modifiche sospette nel gruppo Amministratori integrato con privilegi**.

6. Se necessario, configurare l'attività **Sono stati rilevati schemi di un possibile attacco di forza bruta nel sistema**:

   a. Fare clic su **Impostazioni** sotto la regola.

   b. Nella finestra visualizzata, specificare il numero di tentativi e un periodo di tempo entro il quale devono essere eseguiti i tentativi di immissione di una password affinché la regola venga attivata.

7. Se è stata selezionata la regola **Sono state rilevate attività atipiche durante una sessione di accesso alla rete**, è necessario configurarne le impostazioni:

   a. Fare clic su **Impostazioni** sotto la regola.

   b. Nel blocco **Rilevamento degli accessi di rete**, specificare l'inizio e la fine dell'intervallo di tempo.

   Kaspersky Endpoint Security considera i tentativi di accesso eseguiti durante l'intervallo definito come attività anomale.

   Per impostazione predefinita, l'intervallo non è impostato e l'applicazione non monitora i tentativi di accesso. Per consentire all'applicazione di monitorare continuamente i tentativi di accesso, impostare l'intervallo tra le 00:00 e le 23:59. L'inizio e la fine dell'intervallo non devono coincidere. Se sono identici, l'applicazione non monitora i tentativi di accesso.

   c. Nel blocco **Esclusioni**, aggiungere utenti attendibili e indirizzi IP attendibili (IPv4 e IPv6).

   È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio. Kaspersky Endpoint Security non monitora i tentativi di accesso per questi utenti e computer.

8. Salvare le modifiche.

Come risultato, quando la regola si attiva, Kaspersky Endpoint Security crea un *Evento critico*.

Aggiunta delle regole personalizzate

È possibile impostare i propri criteri di attivazione della regola di Log Inspection. A tal fine, è necessario immettere un ID evento e selezionare un'origine evento. È possibile cercare l'ID evento sul sito Web dell'Assistenza tecnica di Microsoft. È possibile selezionare un'origine evento tra i registri standard: *Application*, *Security* o *System*. È inoltre possibile specificare il registro di un'applicazione di terzi. È possibile trovare il nome del registro dell'applicazione di terzi utilizzando lo strumento Visualizzatore eventi. I registri delle applicazioni di terzi vengono conservati nella cartella dei registri delle applicazioni e dei servizi (ad esempio, il registro di *Windows PowerShell*).

L'applicazione non verifica se il registro specificato è effettivamente presente nel registro eventi di Windows. Se è presente un errore nel nome del registro, l'applicazione non monitora gli eventi da tale registro.

L'elenco delle regole personalizzate include già tre regole create dagli esperti di Kaspersky.

Come aggiungere una regola personalizzata in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Log Inspection**.
4. Verificare che la casella di controllo **Log Inspection** sia selezionata.
5. Nel blocco **Regole personalizzate**, fare clic sul pulsante **Impostazioni**.
6. Nella finestra visualizzata, selezionare le caselle di controllo accanto alle regole personalizzate che si desidera abilitare.
7. Se necessario, fare clic su **Aggiungi** per creare le roprie regole personalizzate.
8. Viene visualizzata una finestra; in tale finestra, configurare la regola personalizzata:
   - **Nome regola**.
   - **Nome log**. Registri eventi di Windows. Sono disponibili i seguenti registri: *Application*, *Security*, *System*.
   - **Sorgente**. Log delle applicazioni di terzi. È possibile trovare il nome del registro dell'applicazione di terzi utilizzando lo strumento Visualizzatore eventi. I registri delle applicazioni di terzi vengono conservati nella cartella dei registri delle applicazioni e dei servizi (ad esempio, il registro di *Windows PowerShell*).
   - **Identificatori eventi**. ID eventi nel Registro eventi di Windows. È possibile cercare l'ID evento nella documentazione tecnica di Microsoft.
9. Salvare le modifiche.

Come aggiungere una regola personalizzata in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Controlli di sicurezza** → **Log Inspection**.
5. Verificare che l'interruttore **Log Inspection ABILITATA** sia attivato.
6. Nel blocco **Regole personalizzate**, selezionare le regole personalizzate che si desidera abilitare.
7. Se necessario, fare clic su **Aggiungi** per creare le roprie regole personalizzate.
8. Viene visualizzata una finestra; in tale finestra, configurare la regola personalizzata:
   - **Nome regola**.
   - **Nome registro personalizzato**. Registri eventi di Windows. Sono disponibili i seguenti registri: *Application*, *Security*, *System*.
   - **Origine**. Log delle applicazioni di terzi. È possibile trovare il nome del registro dell'applicazione di terzi utilizzando lo strumento Visualizzatore eventi. I registri delle applicazioni di terzi vengono conservati nella cartella dei registri delle applicazioni e dei servizi (ad esempio, il registro di *Windows PowerShell*).
   - **Identificatori eventi**. ID eventi nel Registro eventi di Windows. È possibile cercare l'ID evento nella documentazione tecnica di Microsoft.
9. Salvare le modifiche.

Come aggiungere una regola personalizzata nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Log Inspection**.
3. Verificare che l'interruttore **Log Inspection** sia attivato.
4. Nel blocco **Regole personalizzate**, fare clic sul pulsante **Configura**.
5. Nella finestra visualizzata, selezionare le caselle di controllo accanto alle regole personalizzate che si desidera abilitare.
6. Se necessario, fare clic su **Aggiungi** per creare le roprie regole personalizzate.
7. Viene visualizzata una finestra; in tale finestra, configurare la regola personalizzata:
   - **Nome regola**.
   - **Nome log**. Registri eventi di Windows. Sono disponibili i seguenti registri: *Application*, *Security*, *System*.

- **Sorgente**. Log delle applicazioni di terzi. È possibile trovare il nome del registro dell'applicazione di terzi utilizzando lo strumento Visualizzatore eventi. I registri delle applicazioni di terzi vengono conservati nella cartella dei registri delle applicazioni e dei servizi (ad esempio, il registro di *Windows PowerShell*).

- **Identificatore evento**. ID eventi nel Registro eventi di Windows. È possibile cercare l'ID evento nella documentazione tecnica di Microsoft.

8. Salvare le modifiche.

Come risultato, quando la regola si attiva, Kaspersky Endpoint Security crea l'evento *Critico*.

Monitoraggio integrità di sistema

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation.

A partire dalla versione 12.6, Kaspersky Endpoint Security for Windows include il componente Monitoraggio integrità di sistema anziché il componente Monitoraggio integrità file. Il componente Monitoraggio integrità di sistema include tutte le funzionalità di Monitoraggio integrità file e consente inoltre di monitorare le modifiche al Registro di sistema e la connessione dei dispositivi esterni.

Il componente Monitoraggio integrità di sistema monitora le modifiche nel sistema operativo che potrebbero indicare violazioni della sicurezza del computer. Quando vengono rilevate tali modifiche, Kaspersky Endpoint Security genera gli eventi corrispondenti e avvisa l'amministratore. Monitoraggio integrità di sistema può funzionare in modalità in tempo reale e può anche eseguire controlli dell'integrità del sistema su richiesta.

Monitoraggio integrità di sistema in tempo reale

In modalità in tempo reale, Monitoraggio integrità di sistema tiene traccia delle modifiche negli oggetti inclusi nell'ambito del componente (l'*ambito di monitoraggio*). Monitoraggio integrità di sistema consente inoltre di bloccare in tempo reale l'accesso non autorizzato a tali oggetti.

Controllo integrità di sistema su richiesta

Controllo integrità di sistema su richiesta è un'attività che è possibile eseguire manualmente o in base a una pianificazione. Per eseguire l'attività *Controllo integrità di sistema*, è necessario configurare l'ambito del componente (l'*ambito di monitoraggio*) e creare una linea di base. Una *linea di base* è uno stato registrato degli oggetti nel sistema che l'applicazione utilizza come riferimento per il confronto con lo stato corrente.

Migrazione delle impostazioni di Monitoraggio integrità file

Quando si aggiorna Kaspersky Endpoint Security alla versione 12.6, le impostazioni di Monitoraggio integrità file vengono migrate automaticamente. Durante la migrazione, l'applicazione sposta le regole di monitoraggio in Monitoraggio integrità di sistema. Le regole di Monitoraggio integrità file vengono migrate in Monitoraggio integrità di sistema anche quando si effettua la migrazione da KSWS a KES.

Per garantire il corretto funzionamento di Monitoraggio integrità di sistema, l'applicazione Kaspersky Endpoint Security e il plug-in di gestione devono essere aggiornati alla versione 12.6. Se è installata una versione precedente del plug-in di gestione, non è possibile configurare Monitoraggio integrità di sistema poiché il plug-in di gestione è assente nella sezione **Monitoraggio integrità di sistema**.

Informazioni sulle regole di Monitoraggio integrità di sistema

Per il corretto funzionamento di Monitoraggio integrità di sistema, è necessario aggiungere almeno una regola. Una *regola di Monitoraggio integrità di sistema* è un set di criteri che definiscono l'accesso degli utenti ai file e al Registro di sistema. Monitoraggio integrità di sistema rileva le modifiche nei file e nel Registro di sistema all'interno dell'*ambito di monitoraggio* specificato. L'ambito del monitoraggio è uno dei criteri di una regola di Monitoraggio integrità di sistema.

Monitoraggio integrità di sistema consente di monitorare i seguenti oggetti:

- File
- Registro di sistema
- Dispositivi esterni

Considerazioni speciali relative al monitoraggio dei file

Monitoraggio integrità di sistema monitora le modifiche in file e cartelle, nonché i file aggiunti all'ambito di monitoraggio o rimossi da esso. Queste modifiche possono indicare una violazione della sicurezza del computer. Si consiglia di aggiungere oggetti modificati raramente o a cui solo l'amministratore ha accesso. In questo modo, si riduce il numero di eventi di Monitoraggio integrità di sistema.

Monitoraggio dell'integrità di sistema non monitora le modifiche apportate ai file nelle cartelle condivise del server. Monitoraggio integrità di sistema può essere utilizzato solo in locale.

Kaspersky Endpoint Security monitora le modifiche di file e cartelle solo nei dischi che erano connessi al momento dell'avvio di Monitoraggio dell'integrità di sistema in tempo reale. Se un disco non era connesso quando è stata avviata l'esecuzione di Monitoraggio integrità di sistema in tempo reale, l'applicazione non monitora le modifiche di file e cartelle in tale disco anche se i file e le cartelle vengono aggiunti all'ambito di monitoraggio.

Considerazioni speciali relative al monitoraggio del Registro di sistema

Monitoraggio integrità di sistema monitora il Registro di sistema. Queste modifiche possono indicare una violazione della sicurezza del computer.

Monitoraggio integrità di sistema monitora le seguenti chiavi radice del Registro di sistema:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG` (disponibile solo in Monitoraggio integrità di sistema in tempo reale)
- `HKEY_CURRENT_USER` (disponibile solo in Monitoraggio integrità di sistema in tempo reale)

> L'attività *Controllo integrità di sistema* non supporta la chiave `HKEY_CURRENT_USER`. È possibile specificare una chiave in `HKEY_USERS` come `HKEY_USERS\<user profile ID>\<key>`.

Considerazioni speciali relative al monitoraggio dei dispositivi esterni

Monitoraggio integrità di sistema monitora la connessione e la disconnessione dei dispositivi esterni. Tale monitoraggio è necessario per proteggere il computer dalle minacce alla sicurezza che possono derivare dallo scambio di file con tali dispositivi. Monitoraggio integrità di sistema non monitora l'accesso ai dispositivi esterni e non blocca lo scambio di file. È possibile configurare l'accesso ai dispositivi utilizzando un diverso componente dell'applicazione, Controllo dispositivi.

> Quando si esegue l'attività *Monitoraggio integrità di sistema di riferimento*, l'applicazione ignora la riconnessione dei dispositivi esterni se i dispositivi hanno la stessa lettera di unità nel sistema operativo. Per essere registrati, i dispositivi riconnessi devono avere lettere di unità diverse.

Monitoraggio integrità di sistema monitora la connessione dei seguenti tipi di dispositivi esterni:

- Unità rimovibile (comprese le unità flash USB)
- Disco rigido
- Scheda di rete esterna

- Unità CD/DVD/Blu-ray
- Scanner/fotocamera

Monitoraggio integrità di sistema in tempo reale

Monitoraggio integrità di sistema consente di tenere traccia delle modifiche nel sistema operativo in tempo reale. È possibile tenere traccia delle modifiche che potrebbero indicare violazioni della sicurezza nel computer. Il componente consente di bloccare queste modifiche o semplicemente di registrare gli eventi di modifica.

Per il corretto funzionamento di Monitoraggio integrità di sistema, è necessario aggiungere almeno una regola. Una *regola di Monitoraggio integrità di sistema* è un set di criteri che definiscono l'accesso degli utenti ai file e al Registro di sistema. Monitoraggio integrità di sistema rileva le modifiche nei file e nel Registro di sistema all'interno dell'*ambito di monitoraggio* specificato. L'ambito del monitoraggio è uno dei criteri di una regola di Monitoraggio integrità di sistema.

Modalità di Monitoraggio integrità di sistema in tempo reale

Per assicurarsi che le regole di Monitoraggio integrità di sistema non blocchino le azioni con le risorse critiche per il funzionamento del sistema operativo o di altri servizi, è consigliabile abilitare la modalità Test e analizzare l'impatto del componente sul sistema. Con la modalità Test attivata, Kaspersky Endpoint Security non blocca le attività dell'utente vietate dalle regole, ma genera eventi di *Avviso* ⚠.

Il componente Monitoraggio integrità di sistema in tempo reale dispone di due modalità:

- Blocca

  In questa modalità, Monitoraggio integrità di sistema tiene traccia delle modifiche nel sistema ed esegue un'azione in base alle regole: **Consenti** o **Blocca**. Monitoraggio integrità di sistema genera inoltre un evento corrispondente e modifica lo stato del dispositivo nella console di Kaspersky Security Center.

- Informa

  In questa modalità, Monitoraggio integrità di sistema consente di eseguire azioni con file e chiavi del Registro di sistema nell'ambito del monitoraggio. Se l'azione con i file o il registro di sistema è vietata, l'applicazione genera un evento: *L'operazione vietata è stata consentita in modalità di test*. Per analizzare l'effetto delle regole sul sistema, è possibile esaminare i rapporti.

Abilitazione di Monitoraggio integrità di sistema in tempo reale

Come abilitare Monitoraggio integrità di sistema in tempo reale in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Monitoraggio integrità di sistema**.
4. Selezionare la casella di controllo **Monitoraggio integrità di sistema**.

5. In **Modalità operativa per le regole di blocco**, selezionare una modalità per Monitoraggio integrità di sistema in tempo reale:

   - **Blocca**. In questa modalità, Monitoraggio integrità di sistema blocca le azioni con file e chiavi del Registro di sistema dall'ambito di monitoraggio e genera un evento corrispondente.
   - **Informa**. In questa modalità, Monitoraggio integrità di sistema consente le azioni con file e chiavi del Registro di sistema dall'ambito di monitoraggio e genera un evento corrispondente.

6. Nella sezione **Monitoraggio integrità di sistema in tempo reale** selezionare la casella di controllo **Monitoraggio integrità di sistema in tempo reale**.

7. Configurare il monitoraggio dei dispositivi esterni:

   a. Selezionare la casella di controllo **Monitora i dispositivi**.

   b. Nell'elenco a discesa **Livello di gravità evento**, selezionare il livello di importanza degli eventi di monitoraggio dei dispositivi esterni: *Informativo*, *Avviso*, *Critico*.

   Monitoraggio integrità di sistema registra la connessione corrente dei dispositivi esterni. L'applicazione inizia a monitorare la connessione e la disconnessione dei dispositivi esterni dopo l'abilitazione del componente nelle impostazioni dell'applicazione. Successivamente, quando un dispositivo esterno viene connesso o disconnesso, l'applicazione genera un evento corrispondente.

8. Configurare il monitoraggio di file e Registro di sistema:

   a. Selezionare la casella di controllo **Monitora i file e il Registro di sistema**.

   b. Fare clic su **Impostazioni**.

   Viene aperto l'elenco delle regole di Monitoraggio integrità di sistema.

   c. Fare clic su **Aggiungi**.

   È inoltre possibile importare le regole da un'altra fonte.

   d. Configurare la regola di Monitoraggio integrità di sistema (vedere la tabella di seguito).

9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare Monitoraggio integrità di sistema in tempo reale in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza** → **Monitoraggio integrità di sistema**.

5. Attivare l'interruttore **Monitoraggio integrità di sistema ABILITATO**.

6. Selezionare la scheda **Windows**.

7. In **Monitoraggio integrità di sistema in tempo reale**, selezionare una modalità per Monitoraggio integrità di sistema in tempo reale:

   - **Applica regole**. In questa modalità, Monitoraggio integrità di sistema blocca le azioni con file e chiavi del Registro di sistema dall'ambito di monitoraggio e genera un evento corrispondente.
   - **Regole di test (segnala)**. In questa modalità, Monitoraggio integrità di sistema consente le azioni con file e chiavi del Registro di sistema dall'ambito di monitoraggio e genera un evento corrispondente.

8. Configurare il monitoraggio di file e Registro di sistema:

   a. Selezionare la casella di controllo **Monitora i file e il Registro di sistema**.

   b. Fare clic su **Regole**.

   Viene aperto l'elenco delle regole di Monitoraggio integrità di sistema.

   c. Fare clic su **Aggiungi**.

   È inoltre possibile importare le regole da un'altra fonte.

   d. Configurare la regola di Monitoraggio integrità di sistema (vedere la tabella di seguito).

9. Configurare il monitoraggio dei dispositivi esterni:

   a. Selezionare la casella di controllo **Monitora i dispositivi**.

   b. Nell'elenco a discesa **Livello di gravità evento**, selezionare il livello di importanza degli eventi di monitoraggio dei dispositivi esterni: *Informativo*, *Avviso*, *Critico*.

   Monitoraggio integrità di sistema registra la connessione corrente dei dispositivi esterni. L'applicazione inizia a monitorare la connessione e la disconnessione dei dispositivi esterni dopo l'abilitazione del componente nelle impostazioni dell'applicazione. Successivamente, quando un dispositivo esterno viene connesso o disconnesso, l'applicazione genera un evento corrispondente.

10. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare Monitoraggio integrità di sistema in tempo reale nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza → Monitoraggio integrità di sistema**.
3. Attivare l'interruttore **Monitoraggio integrità di sistema**.
4. In **Modalità operativa per le regole di blocco**, selezionare una modalità per Monitoraggio integrità di sistema in tempo reale:

   - **Blocca**. In questa modalità, Monitoraggio integrità di sistema blocca le azioni con file e chiavi del Registro di sistema dall'ambito di monitoraggio e genera un evento corrispondente.
   - **Informa**. In questa modalità, Monitoraggio integrità di sistema consente le azioni con file e chiavi del Registro di sistema dall'ambito di monitoraggio e genera un evento corrispondente.

5. Nella sezione **Monitoraggio integrità di sistema in tempo reale** selezionare la casella di controllo **Monitoraggio integrità di sistema in tempo reale**.

6. Configurare il monitoraggio dei dispositivi esterni:

   a. Selezionare la casella di controllo **Monitora i dispositivi**.

   b. Nell'elenco a discesa **Livello di gravità evento**, selezionare il livello di importanza degli eventi di monitoraggio dei dispositivi esterni: *Informativo* ⓘ, *Avviso* ⚠, *Critico* ⓘ.

   Monitoraggio integrità di sistema registra la connessione corrente dei dispositivi esterni. L'applicazione inizia a monitorare la connessione e la disconnessione dei dispositivi esterni dopo l'abilitazione del componente nelle impostazioni dell'applicazione. Successivamente, quando un dispositivo esterno viene connesso o disconnesso, l'applicazione genera un evento corrispondente.

7. Configurare il monitoraggio di file e Registro di sistema:

   a. Selezionare la casella di controllo **Monitora i file e il Registro di sistema**.

   b. Fare clic su **Configura**.

   Viene aperto l'elenco delle regole di Monitoraggio integrità di sistema.

   c. Fare clic su **Aggiungi**.

   È inoltre possibile importare le regole da un'altra fonte.

8. Configurare la regola di Monitoraggio integrità di sistema (vedere la tabella di seguito).

9. Salvare le modifiche.

Impostazioni delle regole di Monitoraggio integrità di sistema in tempo reale

Parametro	Descrizione
Nome regola	Nome della regola di Monitoraggio integrità di sistema in tempo reale
Operazioni con file e Registro di sistema	• **Consenti**. Monitoraggio integrità di sistema consente di eseguire azioni con file e chiavi del Registro di sistema nell'ambito del monitoraggio. • **Blocca**. Il comportamento di Monitoraggio integrità di sistema dipende dalla modalità selezionata. Se è stata selezionata la *Modalità di protezione del sistema*, Monitoraggio integrità di sistema blocca le azioni con file e chiavi del Registro di sistema dall'ambito di monitoraggio, genera un evento corrispondente e modifica lo stato del dispositivo nella console di Kaspersky Security Center. Se è stata selezionata la *modalità Test*, Monitoraggio integrità di sistema consente di eseguire azioni con file e chiavi del Registro di sistema nell'ambito del monitoraggio.

Parametro	Descrizione
Livello di gravità evento	Kaspersky Endpoint Security registra gli eventi di modifica dei file ogni volta che si modifica un file o una chiave del Registro di sistema nell'ambito del monitoraggio. Sono disponibili i seguenti livelli di gravità degli eventi: *Informativo*, *Avviso*, *Critico*.
Ambito del monitoraggio	• **File**. Elenco di file e cartelle monitorati dal componente. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. Utilizzare le maschere: • Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle. • Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida. • Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri. • **Registro di sistema**. Elenco di chiavi e valori del Registro di sistema monitorati dal componente. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:
Esclusioni	• **File**. Elenco delle esclusioni dall'ambito del monitoraggio. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. Ad esempio, `C:\Folder\Application\*.log`. Le voci di esclusione hanno una priorità maggiore rispetto alle voci dell'ambito del monitoraggio. Utilizzare le maschere: • Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle. • Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida. • Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri. • **Registro di sistema**. Elenco delle esclusioni dall'ambito del monitoraggio. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera: Le voci di esclusione hanno una priorità maggiore rispetto alle voci dell'ambito del monitoraggio.
Utenti e/o gruppi di utenti attendibili	Un *utente attendibile* è un utente autorizzato a eseguire azioni con file e chiavi del Registro di sistema nell'ambito di monitoraggio. Se Kaspersky Endpoint Security rileva un'azione eseguita da un utente attendibile, Monitoraggio integrità di sistema genera un evento *Informativo*. È possibile selezionare gli utenti in Active Directory, nell'elenco degli account in Kaspersky Security Center o immettendo manualmente un nome utente locale. Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio.
Marcatori operazioni sul file/Operazioni monitorate	Indicatori che caratterizzano l'azione con file o chiavi del Registro di sistema che verranno monitorati dall'applicazione.
Hashing	Calcolo di un hash di file in fase di modifica. Kaspersky Endpoint Security aggiunge informazioni sull'hash del file quando viene generato un evento.

Controllo integrità di sistema su richiesta

Controllo integrità di sistema su richiesta è un'attività che è possibile eseguire manualmente o in base a una pianificazione. Quando si esegue l'attività *Controllo integrità di sistema*, l'applicazione confronta lo stato corrente degli oggetti inclusi nell'ambito di monitoraggio con lo stato della relativa *linea di base*. A differenza di Monitoraggio integrità di sistema in tempo reale, l'attività *Controllo integrità di sistema* consente di limitare il numero di eventi e consente di generare un rapporto generale delle modifiche apportate al sistema operativo.

Per il corretto funzionamento di Monitoraggio integrità di sistema, è necessario aggiungere almeno una regola. Una *regola di Monitoraggio integrità di sistema* è un set di criteri che definiscono l'accesso degli utenti ai file e al Registro di sistema. Monitoraggio integrità di sistema rileva le modifiche nei file e nel Registro di sistema all'interno dell'*ambito di monitoraggio* specificato. L'ambito del monitoraggio è uno dei criteri di una regola di Monitoraggio integrità di sistema. È possibile configurare le regole per la condivisione da parte di Monitoraggio integrità di sistema in tempo reale e l'attività *Controllo integrità di sistema* oppure creare regole separate per l'attività. Per creare una linea di base, Kaspersky Endpoint Security applica l'ambito di monitoraggio dall'attività *Controllo integrità di sistema* all'attività *Aggiornamento di riferimento*.

Creazione e aggiornamento di una linea di base

Per funzionare, l'attività *Controllo integrità di sistema* richiede una linea di base. Una *linea di base* è uno stato registrato degli oggetti nel sistema che l'applicazione utilizza come riferimento per il confronto con lo stato corrente. Se lo stato corrente del sistema è diverso dallo stato del sistema registrato nella linea di base, Kaspersky Endpoint Security genera l'evento corrispondente. È possibile creare o aggiornare una linea di base tramite l'attività *Aggiornamento di riferimento*.

È possibile aggiornare la linea di base nei seguenti modi:

- Aggiornamento completo.

  L'applicazione aggiorna tutti gli oggetti nell'ambito di monitoraggio.

- Aggiornamento incrementale.

  L'applicazione rileva e aggiorna solo gli oggetti nuovi o modificati.

Come creare o aggiornare una linea di base in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Aggiornamento di riferimento**.

Passaggio 2. Selezione della modalità di aggiornamento della linea di base

Selezionare una modalità di aggiornamento della linea di base:

- **Aggiornamento completo**. L'applicazione aggiorna tutti gli oggetti nell'ambito di monitoraggio.
- **Aggiornamento incrementale**. L'applicazione rileva e aggiorna solo gli oggetti nuovi o modificati.

Passaggio 3. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 4. Definizione del nome dell'attività

Immettere il nome dell'attività, ad esempio *Linea di base 2024*.

Passaggio 5. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come creare o aggiornare una linea di base in Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Aggiornamento di riferimento**.

c. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Linea di base 2024*.

d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.
5. Selezione dell'account per eseguire l'attività. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.
6. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.
7. Fare clic sulla nuova attività.

   Verrà visualizzata la finestra delle proprietà dell'attività.
8. Selezionare la scheda **Impostazioni applicazione**.
9. Selezionare una modalità di aggiornamento della linea di base:
   - **Aggiornamento completo**. L'applicazione aggiorna tutti gli oggetti nell'ambito di monitoraggio.
   - **Aggiornamento incrementale**. L'applicazione rileva e aggiorna solo gli oggetti nuovi o modificati.
10. Salvare le modifiche.
11. Selezionare la casella di controllo accanto all'attività.
12. Fare clic su **Avvia**.

Configurazione dell'ambito di monitoraggio per l'attività Controllo integrità di sistema

Per impostazione predefinita, l'ambito di monitoraggio dell'attività *Controllo integrità di sistema* corrisponde all'ambito di monitoraggio di Monitoraggio integrità di sistema in tempo reale. È possibile configurare un ambito di monitoraggio diverso per l'attività.

> Monitoraggio integrità di sistema non supporta l'importazione delle chiavi `HKEY_CURRENT_USER` e `HKEY_CURRENT_CONFIG` per l'attività *Controllo integrità di sistema*. Se l'ambito di monitoraggio dell'attività contiene queste chiavi, l'applicazione genera l'evento *L'ambito del monitoraggio include oggetti errati*.

Come configurare un ambito di monitoraggio diverso per l'attività Controllo integrità di sistema in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza → Monitoraggio integrità di sistema**.
4. Selezionare la casella di controllo **Monitoraggio integrità di sistema**.

5. In **Controllo integrità di sistema**, selezionare la modalità di configurazione dell'attività: **Impostazioni personalizzate**.

6. Configurare il monitoraggio dei dispositivi esterni:

   a. Selezionare la casella di controllo **Monitora i dispositivi**.

   b. Nell'elenco a discesa **Livello di gravità evento**, selezionare il livello di importanza degli eventi di monitoraggio dei dispositivi esterni: *Informativo* ⓘ, *Avviso* ⚠, *Critico* ❗.

   Monitoraggio integrità di sistema registra le informazioni sui dispositivi esterni connessi nel momento in cui viene creata la linea di base. Successivamente, quando un dispositivo esterno viene connesso, l'applicazione genera un evento corrispondente. Quando si esegue l'attività *Controllo integrità di sistema*, l'applicazione non monitora la disconnessione dei dispositivi esterni.

7. Configurare il monitoraggio di file e Registro di sistema:

   a. Selezionare la casella di controllo **Monitora i file e il Registro di sistema**.

   b. Fare clic su **Impostazioni**.

   Viene aperto l'elenco delle regole di Monitoraggio integrità di sistema.

   c. Fare clic su **Aggiungi**.

   È inoltre possibile importare le regole da un'altra fonte.

   d. Configurare la regola di Monitoraggio integrità di sistema (vedere la tabella di seguito).

8. Salvare le modifiche.

Come configurare un ambito di monitoraggio diverso per l'attività Controllo integrità di sistema in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza** → **Monitoraggio integrità di sistema**.

5. Selezionare la scheda **Windows**.

6. Attivare l'interruttore **Monitoraggio integrità di sistema ABILITATO**.

7. In **Controllo integrità di sistema**, selezionare la modalità di configurazione dell'attività: **Impostazioni personalizzate**.

8. Configurare il monitoraggio dei dispositivi esterni:

   a. Selezionare la casella di controllo **Monitora i dispositivi**.

   b. Nell'elenco a discesa **Livello di gravità evento**, selezionare il livello di importanza degli eventi di monitoraggio dei dispositivi esterni: *Informativo* ⓘ, *Avviso* ⚠, *Critico* ❗.

Monitoraggio integrità di sistema registra le informazioni sui dispositivi esterni connessi nel momento in cui viene creata la linea di base. Successivamente, quando un dispositivo esterno viene connesso, l'applicazione genera un evento corrispondente. Quando si esegue l'attività *Controllo integrità di sistema*, l'applicazione non monitora la disconnessione dei dispositivi esterni.

9. Configurare il monitoraggio di file e Registro di sistema:

   a. Selezionare la casella di controllo **Monitora i file e il Registro di sistema**.

   b. Fare clic su **Regole**.

      Viene aperto l'elenco delle regole di Monitoraggio integrità di sistema.

   c. Fare clic su **Aggiungi**.

      È inoltre possibile importare le regole da un'altra fonte.

   d. Configurare la regola di Monitoraggio integrità di sistema (vedere la tabella di seguito).

10. Salvare le modifiche.

Come configurare un ambito di monitoraggio diverso per l'attività Controllo integrità di sistema nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Monitoraggio integrità di sistema**.
3. Attivare l'interruttore **Monitoraggio integrità di sistema**.
4. In **Controllo integrità di sistema**, selezionare la modalità di configurazione dell'attività: **Impostazioni personalizzate**.
5. Configurare il monitoraggio dei dispositivi esterni:

   a. Selezionare la casella di controllo **Monitora i dispositivi**.

   b. Nell'elenco a discesa **Livello di gravità evento**, selezionare il livello di importanza degli eventi di monitoraggio dei dispositivi esterni: *Informativo* ⓘ, *Avviso* ⚠, *Critico* ⓘ.

   Monitoraggio integrità di sistema registra le informazioni sui dispositivi esterni connessi nel momento in cui viene creata la linea di base. Successivamente, quando un dispositivo esterno viene connesso, l'applicazione genera un evento corrispondente. Quando si esegue l'attività *Controllo integrità di sistema*, l'applicazione non monitora la disconnessione dei dispositivi esterni.

6. Configurare il monitoraggio di file e Registro di sistema:

   a. Selezionare la casella di controllo **Monitora i file e il Registro di sistema**.

   b. Fare clic su **Configura**.

      Viene aperto l'elenco delle regole di Monitoraggio integrità di sistema.

c. Fare clic su **Aggiungi**.

È inoltre possibile importare le regole da un'altra fonte.

d. Configurare la regola di Monitoraggio integrità di sistema (vedere la tabella di seguito).

7. Salvare le modifiche.

Impostazioni di una regola dell'attività Controllo integrità di sistema

Parametro	Descrizione
Nome regola	Nome di una regola dell'attività *Controllo integrità di sistema*.
Livello di gravità evento	Kaspersky Endpoint Security registra gli eventi di modifica dei file ogni volta che si modifica un file o una chiave del Registro di sistema nell'ambito del monitoraggio. Sono disponibili i seguenti livelli di gravità degli eventi: *Informativo*, *Avviso*, *Critico*.
Ambito del monitoraggio	• **File**. Elenco di file e cartelle monitorati dal componente. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. Utilizzare le maschere: • Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle. • Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida. • Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri. • **Registro di sistema**. Elenco di chiavi e valori del Registro di sistema monitorati dal componente. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera:
Esclusioni	• **File**. Elenco delle esclusioni dall'ambito del monitoraggio. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. Ad esempio, `C:\Folder\Application\*.log`. Le voci di esclusione hanno una priorità maggiore rispetto alle voci dell'ambito del monitoraggio. Utilizzare le maschere: • Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle. • Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida. • Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri. • **Registro di sistema**. Elenco delle esclusioni dall'ambito del monitoraggio. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera: Le voci di esclusione hanno una priorità maggiore rispetto alle voci dell'ambito del monitoraggio.

Esecuzione dell'attività Controllo integrità di sistema

L'attività *Controllo integrità di sistema* consente di verificare la presenza di modifiche nei file o nelle chiavi del Registro di sistema, nonché di verificare la connessione dei dispositivi esterni. Per verificare la presenza di modifiche nei file, è possibile eseguire l'attività *Controllo integrità di sistema* nei seguenti modi:

- Scansione rapida.

  Durante il controllo delle modifiche nei file, le applicazioni controllano solo gli attributi dei file. L'applicazione non controlla il contenuto dei file.

- Scansione completa.

  Durante il controllo delle modifiche ai file, le applicazioni controllano tutti gli attributi dei file e il contenuto dei file.

La modalità in cui viene eseguita l'attività non influisce sul controllo del Registro di sistema o sui dispositivi esterni.

Come eseguire l'attività Controllo integrità di sistema in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.
3. Fare clic su **Nuova attività**.

   Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.
4. Selezionare **Kaspersky Endpoint Security → Monitoraggio integrità di sistema di riferimento**. Selezionare una modalità di Monitoraggio integrità di sistema:

   - **Scansione completa**. In questa modalità, l'applicazione controlla tutti gli attributi e gli hash dei file.
   - **Scansione rapida**. In questa modalità, l'applicazione controlla solo gli attributi dei file.
5. Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

   - Selezionare i computer rilevati da Administration Server nella rete – dispositivi non assegnati. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
   - Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.
   - Specificare la selezione dei dispositivi per cui si desidera eseguire l'attività.
   - Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
6. Selezione dell'account per eseguire l'attività. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.
7. Configurare una pianificazione per l'avvio di un'attività, ad esempio manualmente o in un giorno della settimana specifico.

8. Immettere un nome per l'attività.

9. Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come eseguire un'attività Controllo integrità di sistema in Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Controllo integrità di sistema**.

   c. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Controllo integrità di sistema settimanale*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Selezione dell'account per eseguire l'attività. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.

6. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Fare clic sulla nuova attività.

   Verrà visualizzata la finestra delle proprietà dell'attività.

8. Selezionare la scheda **Impostazioni applicazione**.

9. Selezionare una modalità di Controllo integrità di sistema:

   - **Scansione rapida**. L'applicazione controlla solo gli attributi dei file. L'applicazione non controlla il contenuto dei file.

   - **Scansione completa**. L'applicazione controlla tutti gli attributi dei file e il relativo contenuto.

10. Salvare le modifiche.

11. Selezionare la casella di controllo accanto all'attività.

12. Fare clic su **Avvia**.

Affinché l'attività *Controllo integrità di sistema* venga completata correttamente, l'ambito di monitoraggio dell'attività *Controllo integrità di sistema* deve corrispondere totalmente alla linea di base. Se l'ambito di monitoraggio è diverso, l'attività viene terminata con un errore. Per sincronizzare gli ambiti di monitoraggio, eseguire l'attività *Aggiornamento di riferimento* con un nuovo ambito di monitoraggio.

Esportazione e importazione delle regole di Monitoraggio integrità di sistema

È possibile esportare l'elenco delle regole di Monitoraggio integrità di sistema in un file XML. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di record dello stesso tipo. È possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco delle regole di Monitoraggio integrità di sistema o per eseguire la migrazione dell'elenco in un server diverso.

Monitoraggio integrità di sistema non supporta l'importazione delle chiavi `HKEY_CURRENT_USER` e `HKEY_CURRENT_CONFIG` per l'attività *Controllo integrità di sistema*. Se l'ambito di monitoraggio dell'attività contiene queste chiavi, l'applicazione genera l'evento *L'ambito del monitoraggio include oggetti errati*.

Come esportare e importare un elenco di regole di Monitoraggio integrità di sistema in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Controlli di sicurezza → Monitoraggio integrità di sistema**.
4. Per esportare o importare le *regole di Monitoraggio integrità di sistema*:
   a. Nel blocco **Monitoraggio integrità di sistema in tempo reale**, fare clic sul pulsante **Impostazioni**.
   b. Per esportare un elenco di regole di Monitoraggio integrità di sistema in tempo reale:
      1. Selezionare le regole che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.
         Se non è stata selezionata alcuna regola, Kaspersky Endpoint Security esporterà tutte le regole.
      2. Fare clic sul collegamento **Esporta**.
      3. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle regole e selezionare la cartella in cui si desidera salvare il file.
      4. Salvare il file.
         Kaspersky Endpoint Security esporta l'intero elenco di regole nel file XML.
   c. Per importare un elenco di regole di Monitoraggio integrità di sistema in tempo reale:
      1. Fare clic sul collegamento **Importa**.
         Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle regole.
      2. Aprire il file.
         Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

5. Per esportare o importare le *regole di Controllo integrità di sistema*:

   a. Nel blocco **Controllo integrità di sistema**, selezionare **Impostazioni personalizzate**.

   b. Fare clic su **Impostazioni**.

   c. Per esportare l'elenco delle regole di Controllo integrità di sistema:

      1. Selezionare le regole che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.

         Se non è stata selezionata alcuna regola, Kaspersky Endpoint Security esporterà tutte le regole.

      2. Fare clic sul collegamento **Esporta**.

      3. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle regole e selezionare la cartella in cui si desidera salvare il file.

      4. Salvare il file.

      Kaspersky Endpoint Security esporta l'intero elenco di regole nel file XML.

   d. Per importare un elenco di regole di Controllo integrità di sistema:

      1. Fare clic sul collegamento **Importa**.

         Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle regole.

      2. Aprire il file.

      Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

6. Salvare le modifiche.

Come esportare e importare un elenco di regole di Monitoraggio integrità di sistema in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Controlli di sicurezza → Monitoraggio integrità di sistema**.

5. Selezionare la scheda **Windows**.

6. Per esportare o importare le *regole di Monitoraggio integrità di sistema*:

   a. Nella sezione **Monitoraggio integrità di sistema in tempo reale**, fare clic sul collegamento **Regole**.

   b. Per esportare un elenco di regole di Monitoraggio integrità di sistema in tempo reale:

      1. Selezionare le regole che si desidera esportare.

      2. Fare clic sul pulsante → **Esporta**.

         Kaspersky Endpoint Security esporta l'elenco delle regole in un file JSON nella cartella dei download predefinita.

   c. Per importare un elenco di regole di Monitoraggio integrità di sistema in tempo reale:

      1. Fare clic sul pulsante → **Importa**.

         Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco degli indirizzi attendibili.

      2. Aprire il file.

         Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

7. Per esportare o importare le *regole di Controllo integrità di sistema*:

   a. Nel blocco **Controllo integrità di sistema su richiesta**, selezionare **Impostazioni personalizzate**.

   b. Fare clic sul collegamento **Regole**.

   c. Per esportare l'elenco delle regole di Controllo integrità di sistema:

      1. Selezionare le regole che si desidera esportare.

      2. Fare clic sul pulsante → **Esporta**.

         Kaspersky Endpoint Security esporta l'elenco delle regole in un file JSON nella cartella dei download predefinita.

   d. Per importare un elenco di regole di Controllo integrità di sistema:

      1. Fare clic sul pulsante → **Importa**.

         Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco degli indirizzi attendibili.

      2. Aprire il file.

         Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

8. Salvare le modifiche.

Visualizzazione dei rapporti di Monitoraggio integrità di sistema

Per analizzare le prestazioni delle regole di Monitoraggio integrità di sistema, è possibile esaminare i rapporti e gli eventi generati dall'applicazione. Kaspersky Endpoint Security genera i seguenti rapporti in merito al componente:

- Nell'interfaccia dell'applicazione:
  - Il rapporto di Monitoraggio integrità di sistema
  - Il rapporto di Controllo integrità di sistema
  - Il rapporto di aggiornamento della linea di base

  Il rapporto contiene gli eventi di Monitoraggio integrità di sistema.
- Nella console di Kaspersky Security Center:
  - Rapporti sui computer in cui sono state attivate le regole di monitoraggio il maggior numero di volte
  - Rapporto sulle regole di monitoraggio attivate più di frequente

  Per impostazione predefinita, viene creato un rapporto per i 30 giorni precedenti, inclusa la data di creazione del rapporto.

  Come visualizzare i rapporti di Monitoraggio integrità di sistema in Administration Console (MMC)

  1. Aprire Kaspersky Security Center Administration Console.
  2. Nel nodo **Administration Server** della struttura di Administration Console selezionare la scheda **Rapporti**.
  3. Fare clic su **Nuovo modello di rapporto**.

     Verrà avviata la Creazione guidata nuovo modello di rapporto.
  4. Attenersi alle istruzioni della Creazione guidata nuovo modello di rapporto. Nel passaggio **Selezione del tipo di modello di rapporto**, selezionare un rapporto Monitoraggio integrità del sistema (la sezione **Altro**):
     - **I 10 dispositivi in cui sono state attivate più frequentemente le regole di Monitoraggio integrità file/Monitoraggio integrità di sistema**.
     - **Le 10 regole di Monitoraggio integrità file/Monitoraggio integrità di sistema che sono state attivate più frequentemente nei dispositivi**.

     Dopo avere completato la Creazione guidata nuovo modello di rapporto, il nuovo modello di rapporto viene visualizzato nella tabella della scheda **Rapporti**.
  5. Aprire il rapporto facendo doppio clic.

  Verrà avviato il processo di generazione del rapporto. Il rapporto viene visualizzato in una nuova finestra.

Come visualizzare i rapporti di Monitoraggio integrità di sistema in Web Console

1. Nella finestra principale di Web Console, fare clic su **Monitoraggio → Rapporti**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuovo modello di rapporto.
3. In **Tipo di modello**, nella sezione **Altro**, selezionare un rapporto di Monitoraggio integrità di sistema:

   - **I 10 dispositivi in cui sono state attivate più frequentemente le regole di Monitoraggio integrità file/Monitoraggio integrità di sistema**.
   - **Le 10 regole di Monitoraggio integrità file/Monitoraggio integrità di sistema che sono state attivate più frequentemente nei dispositivi**.

   Dopo avere completato la Creazione guidata nuovo modello di rapporto, il nuovo modello di rapporto viene visualizzato nella tabella.
4. Selezionare ed eseguire il rapporto.

   Verrà avviato il processo di generazione del rapporto. Il rapporto viene visualizzato in una nuova finestra.

Per visualizzare gli eventi generati dall'applicazione, è inoltre possibile utilizzare le selezioni di eventi nella console di Kaspersky Security Center.

Ripristino dello stato di integrità del sistema

I computer nella console di Kaspersky Security Center hanno uno dei seguenti stati: *OK*, *Avviso* o *Critico*. Se Monitoraggio integrità di sistema rileva una modifica di file o chiavi del Registro di sistema nell'ambito di monitoraggio, lo stato del computer cambia in *Avviso* o *Critico*. Lo stato assegnato da Monitoraggio integrità di sistema è definito lo *stato di integrità di sistema*. È ad esempio possibile reimpostare lo stato di integrità di sistema se dopo l'analisi si è convinti che la modifica rilevata degli oggetti non influisca sulla sicurezza del computer.

Come reimpostare lo stato di integrità di sistema in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.
2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2) → Reimpostazione stato integrità sistema**.

Passaggio 2. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 3. Configurazione di una pianificazione di avvio dell'attività

Ad esempio, configurare manualmente la pianificazione dell'attività.

Passaggio 4. Definizione del nome dell'attività

Immettere il nome dell'attività, ad esempio *Reimpostazione dello stato dopo la modifica dell'ambito di monitoraggio*.

Passaggio 5. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come reimpostare lo stato di integrità di sistema in Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Reimpostazione stato integrità di sistema**.

   c. Nel campo **Nome attività**, immettere una breve descrizione, ad esempio *Reimpostazione dello stato dopo la modifica dell'ambito di monitoraggio*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Selezione dell'account per eseguire l'attività. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività con i diritti di un account utente locale.

6. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Selezionare la casella di controllo accanto all'attività.

8. Fare clic su **Avvia**.

Di conseguenza, se lo stato del computer viene modificato in *Avviso* o *Critico* a causa degli eventi di Monitoraggio integrità di sistema, lo stato del computer viene reimpostato su *OK*. Se lo stato del computer è stato modificato anche a causa di altri eventi, lo stato del computer rimane invariato.

Cloud Discovery

Cloud Discovery gestisce l'accesso degli utenti ai servizi cloud. I servizi cloud includono, ad esempio, Microsoft Teams, Salesforce e Microsoft Office 365. I servizi cloud sono raggruppati in categorie, ad esempio *Condivisione file*, *Software di messaggistica*, *E-mail*. Gli esperti di Kaspersky aggiornano regolarmente le categorie di Cloud Discovery e i servizi cloud classificati nelle categorie. Kaspersky Endpoint Security aggiorna il set di categorie e servizi cloud con i database dell'applicazione. In altre parole, Cloud Discovery non utilizza Kaspersky Security Network per classificare i servizi cloud.

Cloud Discovery fornisce le seguenti funzionalità:

- Monitoraggio dell'utilizzo dei servizi cloud
- Blocco dell'accesso degli utenti ai servizi cloud

Requisiti di sistema

Cloud Discovery è disponibile se sono soddisfatte le seguenti condizioni:

- L'applicazione è installata in un computer in cui viene eseguito Windows per workstation.

  Il componente non è disponibile per i server.

- Kaspersky Security Center versione 15.1 o successiva.

  Il componente non è disponibile in Administration Console (MMC). È possibile configurare Cloud Discovery in Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console.

- Licenza di Kaspersky Next.

Abilitare le funzionalità dell'applicazione richieste dal componente Cloud Discovery:

1. **Esegui scansione delle connessioni criptate**. Questo è necessario per il monitoraggio del traffico HTTPS. È possibile gestire questa funzionalità nella sezione **Impostazioni di rete**.

2. **Inocula script nel traffico Web per interagire con le pagine Web**. Lo script consente la registrazione degli eventi di Cloud Discovery. Lo script fornisce inoltre il blocco completo dell'accesso ai servizi cloud. Senza lo script, l'applicazione blocca l'accesso solo da parte dei domini del servizio cloud. È possibile gestire questa funzionalità nella sezione **Impostazioni di rete**.

È inoltre possibile abilitare la funzionalità **Registra l'apertura delle pagine consentite**. La funzionalità include il raggruppamento di eventi quando un utente visita pagine Web che appartengono allo stesso dominio. In questo modo, quando un utente utilizza un servizio cloud, Cloud Discovery registra solo un evento anziché più eventi per ciascuna pagina Web. È possibile gestire questa funzionalità nella sezione **Controllo Web**.

Monitoraggio dei servizi cloud

Quando un utente inizia a utilizzare un servizio cloud, Kaspersky Endpoint Security registra tale evento e crea una voce nel rapporto. Cloud Discovery controlla l'utilizzo dei servizi cloud nel browser e nelle applicazioni corrispondenti. Cloud Discovery controlla l'utilizzo dei servizi cloud su HTTP e HTTPS.

Come abilitare il monitoraggio dei servizi cloud in Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Comunicazione e protezione Web** → **Cloud Discovery**.

5. Attivare l'interruttore **Cloud Discovery ABILITATO**.

6. Salvare le modifiche.

Di conseguenza, l'applicazione inoltra a Kaspersky Security Center le informazioni sui servizi cloud utilizzati. È possibile visualizzare le informazioni sull'utilizzo dei servizi cloud nei rapporti. Se necessario, è possibile bloccare l'accesso ai servizi cloud.

Blocco dell'accesso ai servizi cloud

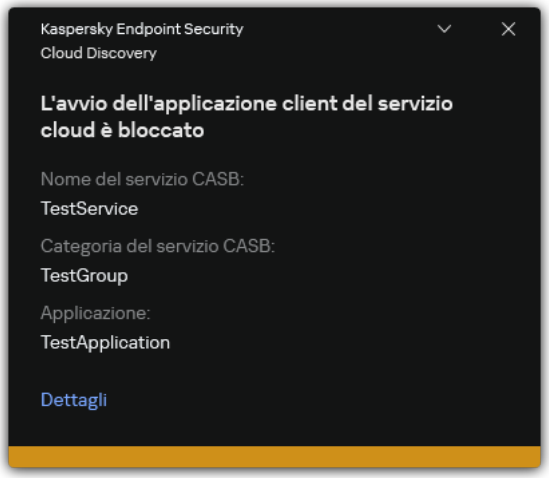
Il blocco dell'accesso ai servizi cloud è disponibile solo per la licenza di Kaspersky Next EDR Optimum e XDR Expert. Questa funzionalità non è disponibile per la licenza Kaspersky Next EDR Foundations. Confronto delle funzionalità dell'applicazione a seconda del tipo di licenza di Kaspersky Next. Vedere in Guida di Kaspersky Next.

L'amministratore può limitare l'accesso degli utenti alle categorie Cloud Discovery o ai singoli servizi cloud. In questo modo, l'amministratore può consentire solo servizi cloud sicuri ed evitare fughe di dati. Le *informazioni sul livello di rischio* vengono visualizzate per ciascun servizio cloud in Cloud Discovery. Il livello di rischio contribuisce a rilevare i servizi che non soddisfano i requisiti di sicurezza dell'organizzazione.

Il livello di rischio è una stima e non implica alcuna dichiarazione sulla qualità del servizio cloud o del suo fornitore. Il livello di rischio è soltanto un suggerimento degli esperti di Kaspersky.

I livelli di rischio dei servizi cloud vengono visualizzati nella sezione **Cloud Discovery** del criterio nell'elenco di tutti i servizi cloud controllati.

Altri componenti di Kaspersky Endpoint Security forniscono protezione dalle minacce e monitoraggio delle attività sospette degli utenti durante l'utilizzo dei servizi cloud.



Notifica di Cloud Discovery

Cloud Discovery non blocca le applicazioni cloud avviate prima di Kaspersky Endpoint Security.

Come bloccare l'accesso ai servizi cloud in Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Comunicazione e protezione Web** → **Cloud Discovery**.
5. Attivare l'interruttore **Cloud Discovery ABILITATO**.

   Viene visualizzato un elenco di tutti i servizi cloud. I servizi cloud sono raggruppati in categorie, ad esempio *Condivisione file*, *Software di messaggistica*, *E-mail*. Gli esperti di Kaspersky aggiornano regolarmente le categorie di Cloud Discovery e i servizi cloud classificati nelle categorie. Kaspersky Endpoint Security aggiorna il set di categorie e servizi cloud con i database dell'applicazione.
6. Utilizzare l'interruttore nella colonna **Accesso** per configurare l'accesso ai servizi cloud.
7. Salvare le modifiche.

Di conseguenza, l'applicazione controlla l'utilizzo dei servizi cloud nel browser e nelle applicazioni corrispondenti.

Area attendibile

Un'*area attendibile* è un elenco configurato dall'amministratore di sistema di oggetti e applicazioni che non vengono monitorati da Kaspersky Endpoint Security durante l'esecuzione.

L'amministratore crea l'area attendibile in modo indipendente, tenendo conto delle caratteristiche degli oggetti utilizzati e delle applicazioni installate nel computer. Può essere necessario includere oggetti e applicazioni nell'area attendibile quando Kaspersky Endpoint Security blocca l'accesso a un determinato oggetto o applicazione, se si è certi che l'oggetto o l'applicazione sia sicuro. Un amministratore può inoltre consentire a un utente di creare la propria area attendibile locale per un computer specifico. In questo modo gli utenti possono creare i propri elenchi locali di esclusioni e applicazioni attendibili oltre all'area attendibile generale in un criterio.

A partire da Kaspersky Endpoint Security 12.5 for Windows, è possibile aggiungere la telemetria EDR all'area attendibile. Questo consente di ottimizzare i dati inviati dall'applicazione al server di raccolta della telemetria per la soluzione Kaspersky Anti Targeted Attack Platform (EDR).

A partire da Kaspersky Endpoint Security 12.6 for Windows, le esclusioni dalle scansioni e le applicazioni attendibili vengono aggiunte all'area attendibile. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server.

A partire da Kaspersky Endpoint Security 12.8 for Windows, è possibile installare l'applicazione in modalità Light Agent per proteggere gli ambienti virtuali. Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono contribuire a configurare rapidamente Kaspersky Endpoint Security negli ambienti virtuali Citrix e VMware.

Creazione di un'esclusione dalla scansione

Un'*esclusione dalla scansione* è un set di condizioni che devono essere soddisfatte perché Kaspersky Endpoint Security non esegua la scansione di un determinato oggetto alla ricerca di virus e altre minacce. Le esclusioni dalla scansione consentono di utilizzare senza rischi il software legittimo che utenti malintenzionati possono sfruttare per danneggiare il computer o i dati dell'utente. Tali applicazioni non hanno necessariamente uno scopo dannoso, ma possono essere sfruttate dagli hacker. Per informazioni dettagliate sulle applicazioni legittime che gli intrusi possono utilizzare per compromettere il computer o i dati dell'utente, visitare il sito Web dell'Enciclopedia Kaspersky.

Tali applicazioni possono essere bloccate da Kaspersky Endpoint Security. Per impedirne il blocco, è possibile configurare le esclusioni dalla scansione per le applicazioni in uso. A tale scopo, aggiungere all'area attendibile il nome o la maschera per il nome elencati nell'Enciclopedia IT di Kaspersky. Ad esempio, spesso si utilizza l'applicazione Radmin per l'amministrazione remota dei computer. Kaspersky Endpoint Security considera sospetta questa attività e potrebbe bloccarla. Per impedire il blocco dell'applicazione, creare un'esclusione dalla scansione con il nome o la maschera per il nome elencati nell'Enciclopedia IT di Kaspersky.

Se un'applicazione che si occupa della raccolta e dell'invio delle informazioni per l'elaborazione è installata nel computer, Kaspersky Endpoint Security può classificare questa applicazione come malware. Per evitare che questo accada, è possibile escludere l'applicazione dalla scansione configurando Kaspersky Endpoint Security come descritto in questo documento.

Le esclusioni dalla scansione possono essere utilizzate dai seguenti componenti e attività dell'applicazione configurati dall'amministratore di sistema:

- Rilevamento del Comportamento.
- Prevenzione Exploit.
- Prevenzione Intrusioni Host.
- Protezione minacce file.
- Protezione minacce Web.
- Protezione minacce di posta.
- Attività *Scansione malware*

Kaspersky Endpoint Security non esamina un oggetto se l'unità o la cartella che contiene l'oggetto è inclusa nell'ambito della scansione all'avvio di una delle attività di scansione. L'esclusione dalla scansione non viene tuttavia applicata quando si avvia un'attività di scansione personalizzata per lo specifico oggetto.

Come creare un'esclusione dalla scansione in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.
5. Nel blocco **Esclusioni dalla scansione e applicazioni attendibili** → **Esclusioni dalla scansione**, fare clic sul pulsante **Impostazioni**.

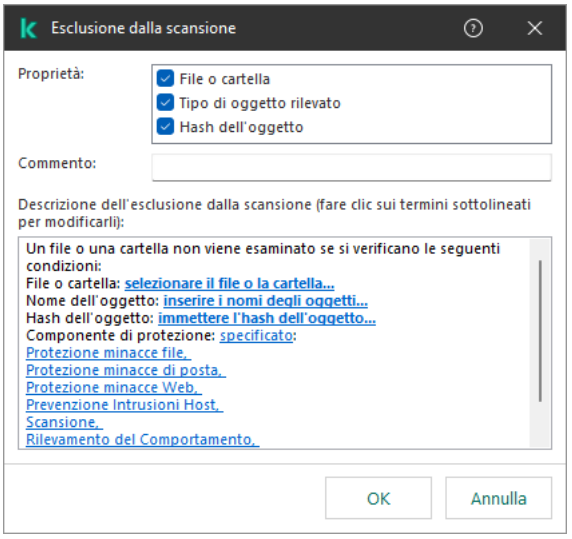
   Verrà visualizzata una finestra contenente un elenco di esclusioni.
6. Selezionare la casella di controllo **Unisci i valori quando vengono ereditati** se si desidera creare un elenco consolidato di esclusioni per tutti i computer dell'azienda. Gli elenchi delle esclusioni nei criteri padre e figlio verranno uniti. Gli elenchi verranno uniti a condizione che l'unione dei valori durante l'ereditarietà sia abilitata. Le esclusioni dal criterio padre vengono visualizzate nei criteri figlio in una visualizzazione di sola lettura. Non è possibile modificare o eliminare le esclusioni del criterio padre.
7. Selezionare la casella di controllo **Consenti l'utilizzo delle esclusioni locali** se si desidera consentire all'utente di creare un elenco locale di esclusioni. In questo modo un utente può creare il proprio elenco locale di esclusioni oltre all'elenco generale di esclusioni generato nel criterio. Un amministratore può utilizzare Kaspersky Security Center per visualizzare, aggiungere, modificare o eliminare gli elementi dell'elenco nelle proprietà del computer.

   Se la casella di controllo è deselezionata, l'utente può accedere solo all'elenco generale delle esclusioni generato nel criterio. Inoltre, se questa casella di controllo è deselezionata, Kaspersky Endpoint Security nasconde l'elenco consolidato delle esclusioni dalle scansioni nell'interfaccia utente dell'applicazione.

8. Fare clic su **Aggiungi** e selezionare un'azione:

- **Categoria**. È possibile raggruppare le esclusioni dalle scansioni in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'esclusione dalle scansioni alla categoria.
- **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova esclusione dalle scansioni alla radice dell'elenco.
- **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include le *esclusioni dalla scansione predefinite*. Sono state inoltre aggiunte esclusioni dalla scansione predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le esclusioni dalle scansioni predefinite a seconda dello scopo del server protetto.
- **Nuova esclusione nella categoria selezionata**. Per aggiungere una nuova esclusione dalla scansione a una categoria specifica, selezionare una categoria.

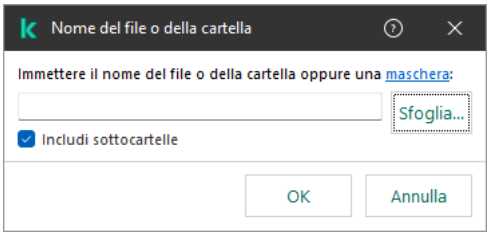
9. Per escludere un file o una cartella dalla scansione:



Impostazioni di esclusione

a. Nella sezione **Proprietà** selezionare la casella di controllo **File o cartella**.

b. Fare clic sul collegamento nel blocco per aprire la finestra **Nome del file o della cartella**.



Seleziona file o cartella

a. Immettere il nome del file o della cartella (oppure la maschera per il nome del file o della cartella) o selezionare il file o la cartella nella struttura delle cartelle facendo clic su **Sfoglia**.

Utilizzare le maschere:

- Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

- Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

- Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

È possibile utilizzare le maschere all'inizio, al centro o alla fine del percorso file. Ad esempio, se si desidera aggiungere una cartella per tutti gli utenti alle esclusioni, immettere la maschera `?:\Users\*\Folder\`.

Kaspersky Endpoint Security supporta le variabili di ambiente

È possibile escludere le cartelle di rete. A tale scopo, immettere manualmente il percorso della cartella di rete (ad esempio `\\Network Share\*`).

> Kaspersky Endpoint Security non supporta la variabile di ambiente `%userprofile%` quando si genera un elenco di esclusioni utilizzando la console Kaspersky Security Center. Per applicare la voce a tutti gli account utente, è possibile utilizzare il carattere `*` (ad esempio, `C:\Users\*\Documents\File.exe`). Ogni volta che si aggiunge una nuova variabile di ambiente, è necessario riavviare l'applicazione.

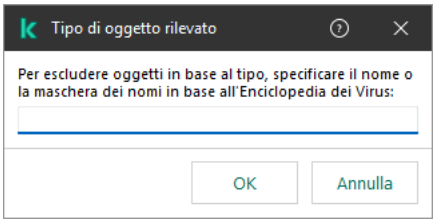
b. Se necessario, disabilitare la funzionalità **Includi sottocartelle**. Se questa funzionalità è abilitata, l'applicazione non esegue la scansione dei file in tutte le sottocartelle. Se questa funzionalità è disabilitata, l'applicazione esclude dall'ambito della scansione solo la cartella selezionata. Questa opzione è abilitata per impostazione predefinita.

c. Salvare le modifiche.

10. Per escludere dalla scansione oggetti con un nome specifico:

    a. Nella sezione **Proprietà** selezionare la casella di controllo **Tipo di oggetto rilevato**.

    b. Fare clic sul collegamento nel blocco per aprire la finestra **Tipo di oggetto rilevato**.



Seleziona oggetto

    a. Immettere il nome del tipo di oggetto in base alla classificazione dell'Enciclopedia Kaspersky (ad esempio `Email-Worm`, `Rootkit` o `RemoteAdmin`).

    È possibile utilizzare maschere con il carattere `?` (sostituisce un singolo carattere) e il carattere `*` (sostituisce un numero qualsiasi di caratteri). Se ad esempio viene specificata la maschera `Client*`, Kaspersky Endpoint Security esclude gli oggetti `Client-IRC`, `Client-P2P` e `Client-SMTP` dalle scansioni.

    b. Salvare le modifiche.

11. Se si desidera escludere un singolo file dalle scansioni:

    a. Nella sezione **Proprietà** selezionare la casella di controllo **Hash dell'oggetto**.

    b. Fare clic sul collegamento nel blocco per aprire la finestra **Hash dell'oggetto**.



Seleziona file

    a. Immettere l'hash del file o selezionare il file facendo clic sul pulsante **Sfoglia**.

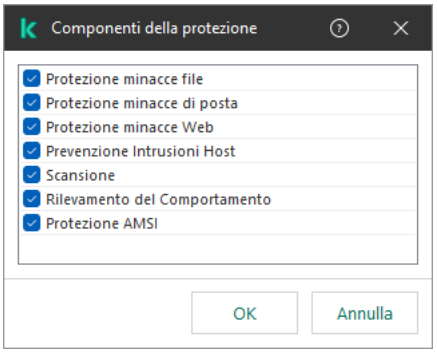
    Se il file viene modificato, verrà modificato anche l'hash del file. In tal caso, il file modificato non verrà aggiunto alle esclusioni.

    b. Salvare le modifiche.

12. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.

13. Specificare i componenti di Kaspersky Endpoint Security da cui verrà utilizzata l'esclusione dalla scansione:

    a. Fare clic sul collegamento nel blocco per aprire la finestra **Componenti della protezione**.



Seleziona componenti della protezione

    a. Selezionare le caselle di controllo accanto ai componenti a cui deve essere applicata l'esclusione dalla scansione.

    Se si specificano i componenti nelle impostazioni dell'esclusione dalla scansione, tale esclusione viene applicata solo durante la scansione da parte di questi componenti di Kaspersky Endpoint Security.

    Se non si specificano i componenti nelle impostazioni dell'esclusione dalla scansione, tale esclusione viene applicata durante la scansione da parte di tutti i componenti di Kaspersky Endpoint Security.

14. Fare clic su **OK**.

    La nuova esclusione verrà aggiunta all'elenco. È possibile disabilitare l'esclusione in qualsiasi momento utilizzando la casella di controllo accanto all'oggetto.

15. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come creare un'esclusione dalla scansione in Kaspersky Security Center Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare alla sezione **Area attendibile**.

5. Nella finestra visualizzata, fare clic sul collegamento **Esclusioni dalla scansione malware**.

6. Selezionare la casella di controllo **Unisci i valori quando vengono ereditati** se si desidera creare un elenco consolidato di esclusioni per tutti i computer dell'azienda. Gli elenchi delle esclusioni nei criteri padre e figlio verranno uniti. Gli elenchi verranno uniti a condizione che l'unione dei valori durante l'ereditarietà sia abilitata. Le esclusioni dal criterio padre vengono visualizzate nei criteri figlio in una visualizzazione di sola lettura. Non è possibile modificare o eliminare le esclusioni del criterio padre.

7. Selezionare la casella di controllo **Consenti l'utilizzo delle esclusioni locali** se si desidera consentire all'utente di creare un elenco locale di esclusioni. In questo modo un utente può creare il proprio elenco locale di esclusioni oltre all'elenco generale di esclusioni generato nel criterio. Un amministratore può utilizzare Kaspersky Security Center per visualizzare, aggiungere, modificare o eliminare gli elementi dell'elenco nelle proprietà del computer.

   Se la casella di controllo è deselezionata, l'utente può accedere solo all'elenco generale delle esclusioni generato nel criterio. Inoltre, se questa casella di controllo è deselezionata, Kaspersky Endpoint Security nasconde l'elenco consolidato delle esclusioni dalle scansioni nell'interfaccia utente dell'applicazione.

8. Fare clic su **Aggiungi** e selezionare un'azione:

   - **Categoria**. È possibile raggruppare le esclusioni dalle scansioni in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'esclusione dalle scansioni alla categoria.
   - **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova esclusione dalle scansioni alla radice dell'elenco.
   - **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include le *esclusioni dalla scansione predefinite*. Sono state inoltre aggiunte esclusioni dalla scansione predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le esclusioni dalle scansioni predefinite a seconda dello scopo del server protetto.

   Per aggiungere una nuova esclusione dalla scansione a una categoria specifica, selezionare la casella di controllo accanto a tale categoria e selezionare l'opzione **Nuova esclusione**.

9. Selezionare le modalità di aggiunta dell'esclusione: **Percorso del file o della cartella**, **Tipo di oggetto** o **Hash dell'oggetto**.

10. Per escludere un file o una cartella dalla scansione, immettere il percorso manualmente. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera:

    - Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.
    - Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.
    - Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

      È possibile utilizzare le maschere all'inizio, al centro o alla fine del percorso file. Ad esempio, se si desidera aggiungere una cartella per tutti gli utenti alle esclusioni, immettere la maschera `?:\Users\*\Folder\`.

      È possibile escludere le cartelle di rete. A tale scopo, immettere manualmente il percorso della cartella di rete (ad esempio `\\Network Share\*`).

11. Se si desidera escludere un tipo specifico di oggetto dalle scansioni, nel campo **Tipo di oggetto** immettere il nome del tipo di oggetto in base alla classificazione dell'Enciclopedia Kaspersky (ad esempio `Email-Worm`, `Rootkit` o `RemoteAdmin`).

    È possibile utilizzare maschere con il carattere `?` (sostituisce un singolo carattere) e il carattere `*` (sostituisce un numero qualsiasi di caratteri). Se ad esempio viene specificata la maschera `Client*`, Kaspersky Endpoint Security esclude gli oggetti `Client-IRC`, `Client-P2P` e `Client-SMTP` dalle scansioni.

12. Se si desidera escludere un singolo file dalle scansioni, immettere l'hash del file nel campo **Hash dell'oggetto**.

    Se il file viene modificato, verrà modificato anche l'hash del file. In tal caso, il file modificato non verrà aggiunto alle esclusioni.

13. Nella sezione **Applica esclusione a** selezionare i componenti a cui si desidera applicare l'esclusione dalla scansione.

14. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.

15. Fare clic su **OK**.

    La nuova esclusione verrà aggiunta all'elenco. È possibile utilizzare l'interruttore per interrompere un'esclusione in qualsiasi momento.

16. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

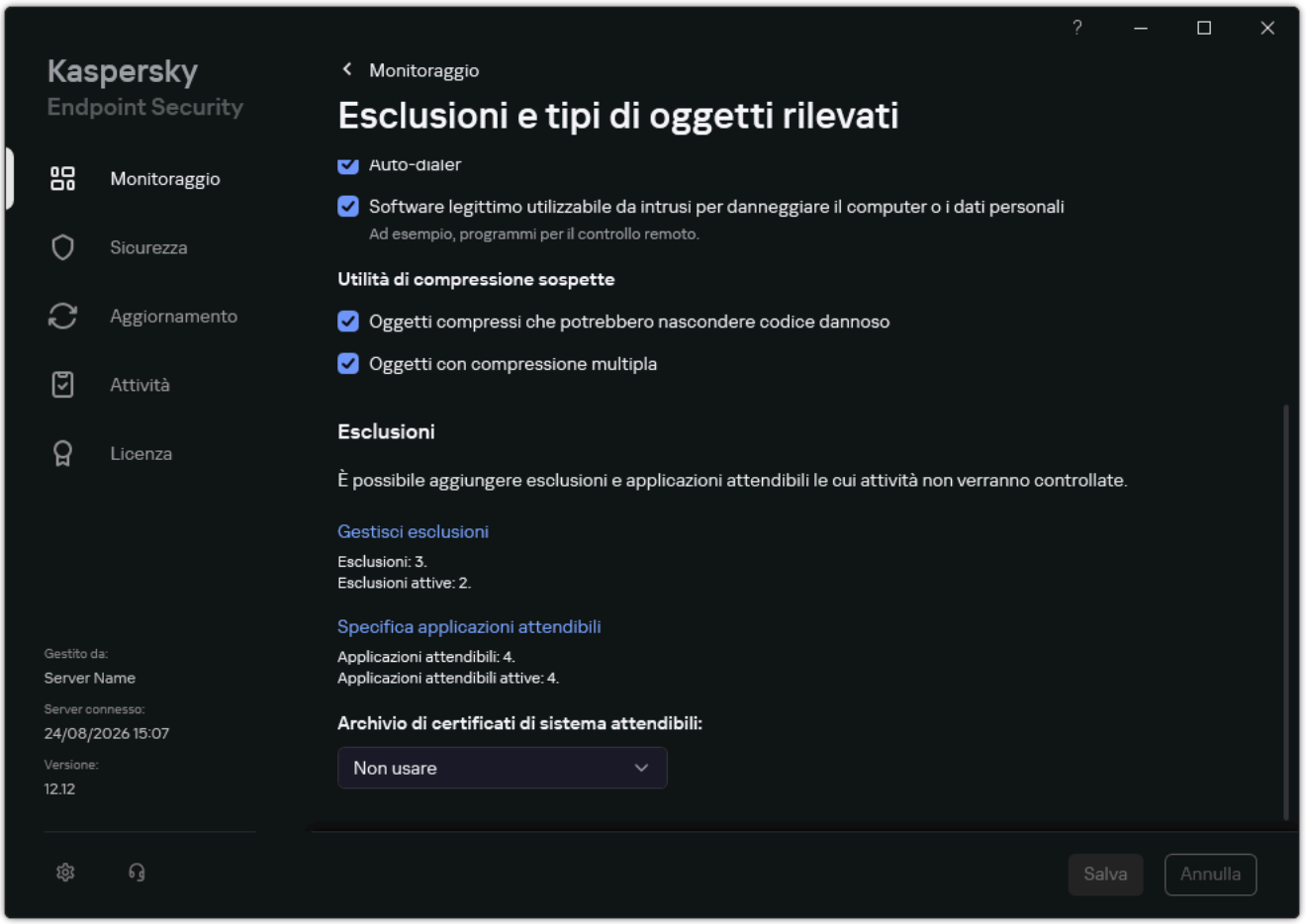
Come creare un'esclusione dalla scansione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali → Esclusioni e tipi di oggetti rilevati**.

3. Nella sezione **Esclusioni**, fare clic sul collegamento **Gestisci esclusioni**.

> Kaspersky Endpoint Security nasconde l'elenco delle esclusioni dalle scansioni nell'interfaccia utente dell'applicazione se la configurazione delle esclusioni dalle scansioni è bloccata dall'amministratore nella console (simbolo del "lucchetto chiuso") e le esclusioni delle scansioni locali sono vietate (la casella di controllo **Consenti l'utilizzo delle esclusioni locali** è deselezionata).



Impostazioni delle esclusioni

4. Fare clic su **Aggiungi** e selezionare un'azione:

   - **Categoria**. È possibile raggruppare le esclusioni dalle scansioni in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'esclusione dalle scansioni alla categoria.

   - **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova esclusione dalle scansioni alla radice dell'elenco.

   - **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include le *esclusioni dalla scansione predefinite*. Sono state inoltre aggiunte esclusioni dalla scansione predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le esclusioni dalle scansioni predefinite a seconda dello scopo del server protetto.

   Per aggiungere una nuova esclusione dalla scansione a una categoria specifica, selezionare la casella di controllo accanto a tale categoria e selezionare l'opzione **Nuova esclusione**.

5. Se si desidera escludere un file o una cartella dalle scansioni, selezionare il file o la cartella facendo clic sul pulsante **Sfoglia**.

   È inoltre possibile immettere il percorso manualmente. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera:

   - Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

   - Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

   - Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

     È possibile utilizzare le maschere all'inizio, al centro o alla fine del percorso file. Ad esempio, se si desidera aggiungere una cartella per tutti gli utenti alle esclusioni, immettere la maschera `?:\Users\*\Folder\`.

     È possibile escludere le cartelle di rete. A tale scopo, immettere manualmente il percorso della cartella di rete (ad esempio `\\Network Share\*`).

6. Se si desidera escludere un tipo specifico di oggetto dalle scansioni, nel campo **Tipi di oggetto rilevato** immettere il nome del tipo di oggetto in base alla classificazione dell'Enciclopedia Kaspersky (ad esempio `Email-Worm`, `Rootkit` o `RemoteAdmin`).

   È possibile utilizzare maschere con il carattere `?` (sostituisce un singolo carattere) e il carattere `*` (sostituisce un numero qualsiasi di caratteri). Se ad esempio viene specificata la maschera `Client*`, Kaspersky Endpoint Security esclude gli oggetti `Client-IRC`, `Client-P2P` e `Client-SMTP` dalle scansioni.

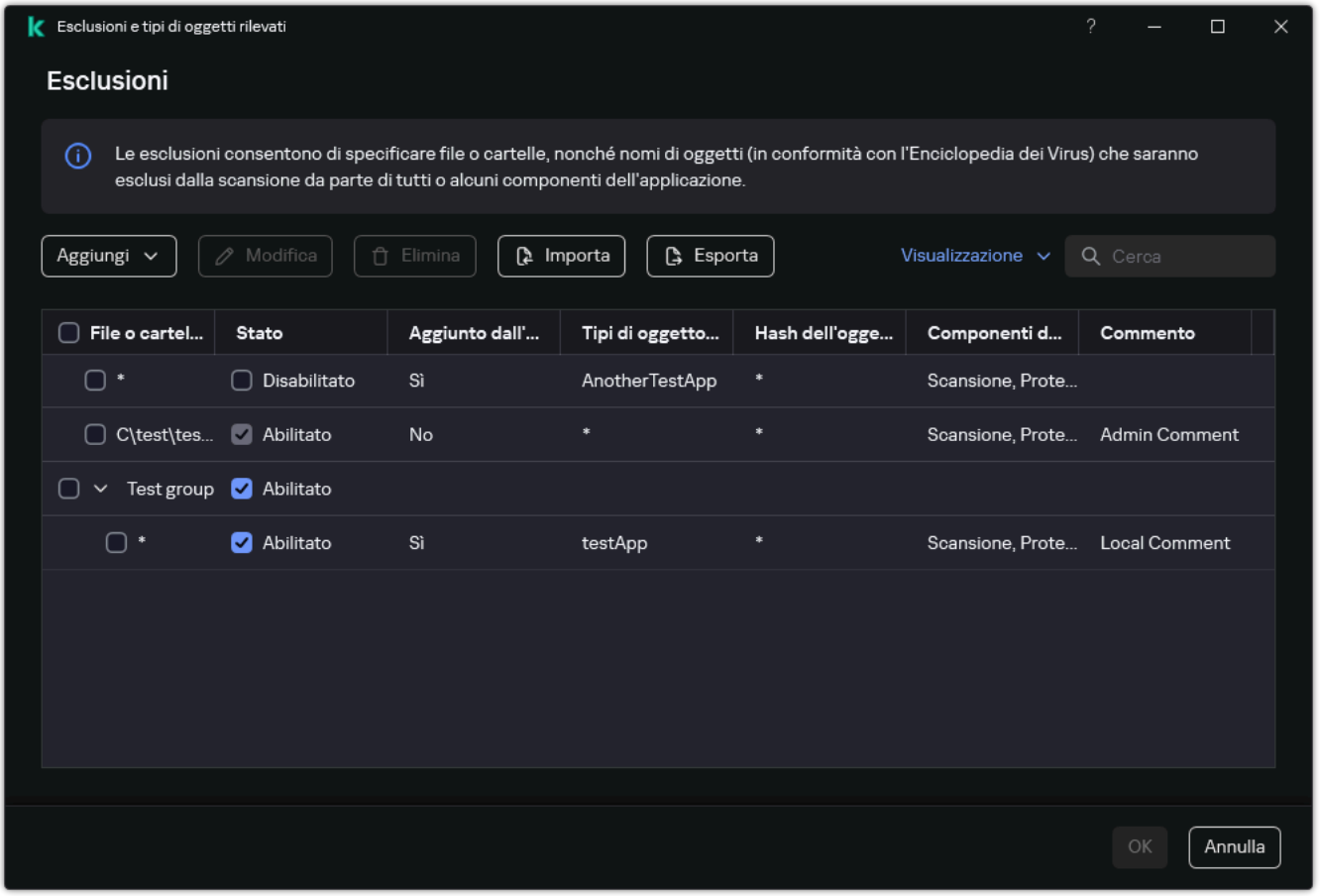
7. Se si desidera escludere un singolo file dalle scansioni, immettere l'hash del file nel campo **Hash dell'oggetto**.

   Se il file viene modificato, verrà modificato anche l'hash del file. In tal caso, il file modificato non verrà aggiunto alle esclusioni.

8. Nella sezione **Componenti della protezione** selezionare i componenti a cui si desidera applicare l'esclusione dalla scansione.

9. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.
10. Selezionare lo stato **Attivo** per l'esclusione.
11. Fare clic su **Aggiungi**.

    La nuova esclusione verrà aggiunta all'elenco. È possibile disabilitare l'esclusione in qualsiasi momento utilizzando la casella di controllo nella colonna **Stato**.
12. Salvare le modifiche.



Elenco delle esclusioni

Esempi di maschera del percorso:

È consigliabile specificare percorsi relativi anziché percorsi assoluti. Questo consente di escludere non solo gli oggetti del file system, ma anche gli oggetti fileless. Ad esempio, `*\Program Files (x86)\Folder\Subfolder`.

Percorsi dei file presenti in qualsiasi cartella:

- La maschera `*.exe` includerà tutti i percorsi dei file con estensione exe.
- La maschera `example*` includerà tutti i percorsi dei file denominati EXAMPLE.

Percorsi dei file presenti in una cartella specifica:

- La maschera `C:\dir\*.*` includerà tutti i percorsi dei file contenuti in `C:\dir\`, ma non nelle sottocartelle di `C:\dir\`.
- La maschera `C:\dir\*` includerà tutti i percorsi dei file contenuti nella cartella `C:\dir\`, incluse le sottocartelle.
- La maschera `C:\dir\` includerà tutti i percorsi dei file contenuti nella cartella `C:\dir\`, incluse le sottocartelle.
- La maschera `C:\dir\*.exe` includerà tutti i percorsi dei file con estensione EXE contenuti nella cartella `C:\dir\`, ma non nelle sottocartelle di `C:\dir\`.
- La maschera `C:\dir\test` includerà tutti i percorsi dei file denominati "test" contenuti nella cartella `C:\dir\`, ma non nelle sottocartelle di `C:\dir\`.
- La maschera `C:\dir\*\test` includerà tutti i percorsi dei file denominati "test" contenuti nella cartella `C:\dir\` e nelle sottocartelle di `C:\dir\`.
- La maschera `C:\dir1\*\dir3\` includerà tutti i percorsi dei file nelle sottocartelle dir3 di un livello nella cartella `C:\dir1\`.
- La maschera `C:\dir1\**\dirN\` includerà tutti i percorsi dei file nelle sottocartelle dirN nella cartalla `C:\dir1\` a qualsiasi livello.

Percorsi dei file contenuti in tutte le cartelle con un nome specifico:

- La maschera `dir\*.*` includerà tutti i percorsi dei file nelle cartelle denominate "dir", ma non nelle sottocartelle di tali cartelle.
- La maschera `dir\*` includerà tutti i percorsi dei file nelle cartelle denominate "dir", ma non nelle sottocartelle di tali cartelle.
- La maschera `dir\` includerà tutti i percorsi dei file nelle cartelle denominate "dir", ma non nelle sottocartelle di tali cartelle.
- La maschera `dir\*.exe` includerà tutti i percorsi dei file con estensione EXE nelle cartelle denominate "dir", ma non nelle sottocartelle di tali cartelle.
- La maschera `dir\test` includerà tutti i percorsi dei file denominati "test" nelle cartelle denominate "dir", ma non nelle sottocartelle di tali cartelle.

Creazione di un'esclusione in base al tipo di oggetti rilevati

Kaspersky Endpoint Security classifica gli oggetti rilevati come segue:

- **Virus e worm**

  Sottocategoria: virus e worm (Viruses_and_Worms)

  Livello di pericolo: Alto

  I virus e worm classici eseguono azioni non autorizzate dall'utente. Possono creare copie di se stessi in grado di replicarsi.

Virus classici

Dopo essere penetrato nel computer, un virus classico infetta un file, si attiva, esegue azioni dannose e aggiunge copie di se stesso in altri file.

Un virus classico si propaga solo nelle risorse locali del computer; non può penetrare in altri computer autonomamente. Può raggiungere un altro computer solo se aggiunge una copia di se stesso a un file memorizzato in una cartella condivisa o in un CD inserito oppure se l'utente inoltra un messaggio e-mail con un file allegato infetto.

Il codice dei virus classici può penetrare in varie aree dei computer, dei sistemi operativi e delle applicazioni. A seconda dell'ambiente, i virus vengono suddivisi in *virus di file*, *virus di avvio*, *virus di script* e *virus macro*.

I virus possono infettare i file utilizzando un'ampia varietà di tecniche. I *virus di Overwriting* scrivono il proprio codice sul codice del file infetto, cancellandone il contenuto. Il file infetto smette di funzionare e non può essere ripristinato. I *virus Parasitic* modificano i file, lasciandoli parzialmente o completamente funzionanti. I *virus Companion* non modificano i file, ma creano duplicati. Quando si apre un file infetto, ne viene avviato un duplicato, che di fatto è un virus. Si rilevano inoltre i seguenti tipi di virus: *virus Link*, *virus OBJ*, *virus LIB*, *virus del codice sorgente* e molti altri.

Worm

Come nel caso dei virus classici, il codice di un worm viene attivato ed esegue azioni dannose dopo essere penetrato in un computer. La caratteristica distintiva dei worm è la loro capacità di trasmettersi da un computer all'altro, senza che l'utente ne sia consapevole, inviando copie di se stessi attraverso vari canali.

La principale caratteristica che consente di differenziare i vari tipi di worm è la loro modalità di propagazione. Nella seguente tabella viene fornita una panoramica dei diversi tipi di worm, classificati in base alla modalità di propagazione.

Modalità di propagazione dei worm

Tipo	Nome	Descrizione
Email-Worm	Email-Worm	Si propagano tramite la posta elettronica. Un messaggio infetto contiene un file allegato con una copia di un worm oppure un collegamento a un file caricato su un sito Web, che può essere stato violato o creato appositamente a tale scopo. Quando l'utente apre il file allegato, il worm si attiva. Allo stesso modo, facendo clic sul collegamento, scaricando e aprendo il file, il worm inizia a eseguire le azioni dannose per cui è progettato. Il worm continua quindi a diffondere copie di se stesso, cercando altri indirizzi di posta elettronica e inviando messaggi infetti.
IM-Worm	Worm del client IM	Si diffondono attraverso client IM. In genere, tali worm inviano messaggi che contengono un collegamento a un file con una copia del worm in un sito Web, utilizzando l'elenco di contatti dell'utente. Quando l'utente scarica e apre il file, il worm si attiva.
IRC-Worm	Worm di chat Internet	Penetrano nei computer attraverso le Internet Relay Chats, sistemi utilizzati per comunicare con altre persone in tempo reale via Internet. Questo tipo di worm pubblica in una chat Internet un file contenente una copia di se stesso o un collegamento a tale file. Quando l'utente scarica e apre il file, il worm si attiva.
Net-Worm	Worm di rete	Questi worm si propagano tramite le reti di computer. A differenza di altri tipi di worm, questi worm vengono propagati senza la partecipazione dell'utente. I worm di questo tipo cercano nella rete locale i computer che utilizzano programmi con vulnerabilità. A tale scopo, inviano uno pacchetto di rete appositamente predisposto (exploit), che contiene il codice del worm o parte di esso. Se nella rete è presente un computer vulnerabile, questo riceve il pacchetto. Quando è penetrato completamente nel computer, il worm si attiva.
P2P-Worm	Worm di file sharing	Si propagano attraverso le reti peer-to-peer di file sharing. Per penetrare in una rete peer-to-peer, il worm si replica in una cartella di file sharing, in genere presente nel computer dell'utente. La rete peer-to-peer visualizza informazioni sul file, in modo che gli utenti della rete possano trovare, scaricare e aprire il file infetto come qualsiasi altro file. I worm più complessi imitano i protocolli di rete di una specifica rete peer-to-peer: offrono risposte positive alle ricerche e propongono copie di se stessi per il download.

Tipo	Nome	Descrizione
Worm	Altri tipi di worm	Gli altri tipi di worm includono: • Worm che propagano copie di se stessi tramite le risorse di rete. Utilizzando le funzioni del sistema operativo, esplorano le cartelle di rete disponibili, si connettono a computer su Internet e cercano di ottenere un accesso completo alle unità disco. A differenza dei worm descritti in precedenza, alcuni non si attivano autonomamente, ma l'utente deve aprire un file contenente una copia del worm per attivarlo. • Worm che non utilizzano alcuno dei metodi descritti nella tabella precedente per diffondersi (ad esempio, quelli distribuiti tramite telefoni cellulari).

- **Trojan (compreso il ransomware)**

  Sottocategoria: Trojan

  Livello di pericolo: Alto

  A differenza dei worm e dei virus, i programmi Trojan non replicano se stessi. Possono ad esempio penetrare in un computer tramite la posta elettronica o attraverso un browser, quando l'utente visita una pagina Web infetta. I programmi Trojan vengono avviati dall'utente. Iniziano a eseguire la loro azione dannosa non appena sono eseguiti.

  Il comportamento dei diversi programmi Trojan nei computer infetti può variare. La funzione principale di un programma Trojan è bloccare, modificare e cancellare i dati, compromettendo il funzionamento dei computer o delle reti. I programmi Trojan possono inoltre ricevere e inviare file, eseguirli, visualizzare messaggi, accedere a pagine Web, scaricare e installare programmi e riavviare il computer.

  Gli hacker spesso utilizzano "set" di vari programmi Trojan.

  Nella seguente tabella sono descritti i diversi tipi di comportamento dei programmi Trojan.

  Tipi di comportamento dei programmi Trojan in un computer infetto

Tipo	Nome	Descrizione
Trojan-ArcBomb	Programmi Trojan – "archivi bomba"	Una volta decompressi, questi archivi aumentano di dimensioni al punto tale da compromettere il funzionamento del computer. Quando l'utente tenta di decomprimere l'archivio, il computer può iniziare a rallentare o bloccarsi e il disco può riempirsi di dati "vuoti". Gli "archivi bomba" sono particolarmente pericolosi per i file server e i server di posta. Se un server utilizza un sistema automatico di elaborazione delle informazioni in arrivo, un "archivio bomba" può causarne l'arresto.
Backdoor	Programmi Trojan di amministrazione remota	Sono considerati il tipo di Trojan più pericoloso in assoluto. Dal punto di vista funzionale, sono simili alle applicazioni di amministrazione remota installate nei computer. Si installano senza che l'utente ne sia consapevole e consentono a un intruso di gestire il computer in remoto.
Programma Trojan	Trojan	Includono le seguenti applicazioni dannose: • **Programmi Trojan classici**. Questi programmi eseguono solo le funzioni principali dei programmi Trojan: blocco, modifica o cancellazione di dati allo scopo di compromettere il funzionamento dei computer o delle reti. Non dispongono delle caratteristiche avanzate di altri tipi di programmi Trojan descritti in questa tabella. • **Programmi Trojan versatili**. Dispongono delle caratteristiche avanzate tipiche di diversi tipi di programmi Trojan.
Trojan-Ransom	Trojan ransom	Questi programmi "prendono in ostaggio" le informazioni sul computer dell'utente, modificandole o bloccandole, oppure compromettono il funzionamento del computer in modo che l'utente non sia più in grado di utilizzare i dati. L'intruso richiede quindi all'utente un riscatto in cambio della promessa di inviare un'applicazione in grado di ripristinare l'utilizzabilità del computer e dei dati.
Trojan-Clicker	Trojan clicker	Accedono a pagine Web dal computer dell'utente, inviando direttamente comandi al browser o sostituendo gli indirizzi Web specificati nei file del sistema operativo. Utilizzando questi programmi, un intruso può sferrare attacchi di rete e aumentare il traffico verso determinati siti Web per aumentare la frequenza di visualizzazione dei banner pubblicitari.

Tipo	Nome	Descrizione
Trojan-Downloader	Trojan downloader	Accedono a una pagina Web, da cui scaricano e installano altre applicazioni dannose nel computer dell'utente. Contengono il nome dell'applicazione dannosa da scaricare o la ricevono dalla pagina Web a cui si collegano.
Trojan-Dropper	Trojan dropper	Contengono altri programmi Trojan che copiano nel disco rigido e quindi installano nel computer. Gli intrusi possono utilizzare i Trojan dropper per: • Installare un'applicazione dannosa senza che l'utente ne sia consapevole: i Trojan dropper non visualizzano alcun messaggio oppure visualizzano messaggi falsi, ad esempio notificando un errore in un archivio o l'utilizzo di una versione incompatibile del sistema operativo. • Impedire il rilevamento di un'altra applicazione dannosa: non tutti i programmi anti-virus sono in grado di rilevare un'applicazione dannosa contenuta all'interno di un Trojan dropper.
Trojan-Notifier	Trojan notifier	Segnalano a un intruso che il computer infetto è accessibile, inviando informazioni sul computer, come l'indirizzo IP, il numero della porta aperta o l'indirizzo e-mail. Comunicano con l'intruso via e-mail, tramite FTP, accedendo alla sua pagina Web o attraverso altri metodi. I Trojan notifier vengono spesso utilizzati in set che comprendono diversi programmi Trojan. Comunicano all'intruso che altri programmi Trojan sono stati installati nel computer dell'utente.
Trojan-Proxy	Trojan proxy	Consentono all'intruso di accedere in modo anonimo alle pagine Web utilizzando il computer dell'utente e vengono spesso utilizzati per inviare posta spam.
Trojan-PSW	Password-stealing-ware	I password-stealing-ware sono un tipo di programma Trojan che ruba gli account utente, ad esempio le informazioni di registrazione del software. Recuperano le informazioni riservate nei file di sistema e nel registro e le inviano all'autore dell'attacco via e-mail, tramite FTP, accedendo al sito Web dell'intruso o attraverso altri metodi. Alcuni di questi programmi Trojan sono classificati in tipi distinti descritti in questa tabella. Esistono programmi Trojan che trafugano conti bancari (Trojan-Banker), i dati degli utenti di client IM (Trojan-IM) e i dati degli utenti di giochi online (Trojan-GameThief).
Trojan-Spy	Programmi Trojan per lo spionaggio dell'utente	Vengono utilizzati per spiare l'utente, raccogliendo informazioni sulle sue azioni durante l'utilizzo del computer. Possono intercettare i dati inseriti dall'utente tramite la tastiera, acquisire schermate e raccogliere elenchi di applicazioni attive. Una volta ricevute tali informazioni, le trasferiscono all'intruso via e-mail, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.
Trojan-DDoS	Programmi Trojan per l'esecuzione di attacchi di rete	Inviano numerose richieste dal computer dell'utente a un server remoto. Il server esaurisce le risorse per l'elaborazione delle richieste ricevute e smette di funzionare (attacchi Denial-of-Service, o semplicemente DoS). Gli hacker spesso infettano numerosi computer con questi programmi, in modo da poterli utilizzare per attaccare simultaneamente un singolo server. I programmi DoS sferrano un attacco da un singolo computer, rivelando la propria presenza all'utente. I programmi DDoS (Distributed DoS) sferrano attacchi da diversi computer senza che l'utente del computer infetto ne sia consapevole.
Trojan-IM	Programmi Trojan che trafugano i dati personali degli utenti di client IM	Trafugano numeri di conti e password degli utenti di client IM. Tali informazioni vengono quindi trasferite all'intruso via e-mail, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.
Rootkit	Rootkit	Nascondono altre applicazioni dannose e la loro attività, prolungando quindi la presenza di tali applicazioni nel sistema operativo. Possono inoltre nascondere file e processi nella memoria di un computer infetto o chiavi di registro utilizzate dalle applicazioni dannose. I rootkit possono nascondere lo scambio di dati tra le applicazioni installate nel computer dell'utente e altri computer in rete.
Trojan-SMS	Programmi Trojan sotto forma di messaggi SMS	Infettano i telefoni cellulari e inviano messaggi SMS a numeri a pagamento.
Trojan-GameThief	Programmi Trojan che trafugano i dati personali degli utenti di giochi online	Rubano le credenziali degli account degli utenti di giochi online. Tali informazioni vengono quindi trasferite all'intruso via e-mail, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.
Trojan-Banker	Programmi Trojan che trafugano conti bancari	Sottraggono i dati di conti bancari o sistemi e-money. Tali informazioni vengono quindi trasferite all'hacker via e-mail, tramite FTP, accedendo a una pagina Web o attraverso altri metodi.
Trojan-Mailfinder	Programmi Trojan che raccolgono indirizzi e-mail	Raccolgono gli indirizzi e-mail sul computer e li trasferiscono all'intruso via e-mail, tramite FTP, accedendo al suo sito Web o attraverso altri metodi. L'intruso può utilizzare gli indirizzi raccolti per inviare spam.

- **Strumenti dannosi**

  Sottocategoria: Strumenti dannosi

Livello di pericolo: Medio

A differenza di altri tipi di malware, gli strumenti dannosi non eseguono specifiche azioni al momento dell'esecuzione. Possono essere memorizzati e avviati senza problemi sul computer dell'utente. Le funzionalità di questi programmi possono essere utilizzate per creare virus, worm e programmi Trojan, sferrare attacchi di rete contro server remoti, violare computer ed eseguire altre azioni dannose.

Nella seguente tabella sono descritte le varie caratteristiche degli strumenti dannosi, raggruppate per tipo.

Caratteristiche degli strumenti dannosi

Tipo	Nome	Descrizione
Constructor	Constructor	Consentono di creare nuovi virus, worm e programmi Trojan. Alcuni constructor presentano un'interfaccia standard di Windows che consente di selezionare il tipo di applicazione dannosa da creare, il modo per contrastare i debugger e altre caratteristiche.
DoS	Attacchi di rete	Inviano numerose richieste dal computer dell'utente a un server remoto. Il server esaurisce le risorse per l'elaborazione delle richieste ricevute e smette di funzionare (attacchi Denial-of-Service, o semplicemente DoS).
Exploit	Exploit	Un *exploit* è un set di dati o un codice di programma che utilizza le vulnerabilità dell'applicazione in cui viene elaborato per eseguire azioni dannose sul computer. Gli exploit possono ad esempio scrivere o leggere file o accedere a pagine Web infette. I diversi exploit utilizzano le vulnerabilità di diverse applicazioni o servizi di rete. Un exploit viene trasmesso tramite la rete a diversi computer, sotto forma di pacchetto di rete, alla ricerca di computer con servizi di rete vulnerabili. Gli exploit contenuti in un file DOC utilizzano le vulnerabilità degli editor di testo. Possono iniziare a eseguire le funzioni programmate dall'hacker quando l'utente apre un file infetto. Un exploit contenuto in un messaggio e-mail ricerca le vulnerabilità in tutti i client di posta elettronica. Può iniziare a eseguire azioni dannose non appena l'utente apre un messaggio infetto in questo client di posta elettronica. Gli exploit vengono utilizzati per propagare i worm di rete. Gli exploit Nuker sono pacchetti di rete che rendono i computer non operativi.
FileCryptor	Strumenti di criptaggio	Criptano altre applicazioni dannose per nasconderle alle applicazioni anti-virus.
Flooder	Programmi per il flooding delle reti	Inviano numerosi messaggi tramite i canali di rete. Questi strumenti comprendono ad esempio i programmi utilizzati per il flooding delle Internet Relay Chat. Questo tipo di software non include i programmi che eseguono il flooding del traffico di posta elettronica, dei client IM e dei sistemi SMS. Tali programmi vengono classificati in categorie distinte nella presente tabella (Email-Flooder, IM-Flooder e SMS-Flooder).
HackTool	Strumenti di hackeraggio	Vengono utilizzati per violare i computer in cui sono installati oppure per generare attacchi contro un altro computer (ad esempio, aggiungendo nuovi account di sistema senza l'autorizzazione dell'utente o cancellando i log di sistema al fine di nascondere le tracce della propria presenza nel sistema operativo). Questi strumenti includono sniffer che eseguono funzioni dannose, come ad esempio intercettare le password. Gli sniffer sono programmi che consentono di visualizzare il traffico di rete.
Hoax	Hoax	Questi programmi spaventano l'utente con messaggi simili a quelli generati dai virus: possono "rilevare" un virus in un file sicuro o visualizzare un messaggio relativo alla formattazione del disco, senza eseguirla effettivamente.
Spoofer	Strumenti di spoofing	Inviano messaggi e richieste di rete con l'indirizzo di un mittente fittizio. Gli spoofer vengono ad esempio utilizzati dagli intrusi per nascondere la propria identità e presentarsi come mittenti attendibili.
VirTool	Strumenti per la modifica di applicazioni dannose	Consentono di modificare altri programmi malware per nasconderli alle applicazioni anti-virus.
Email-Flooder	Programmi per il flooding degli indirizzi e-mail	Inviano numerosi messaggi a vari indirizzi di posta elettronica. La grande quantità di messaggi ricevuti impedisce agli utenti di visualizzare i messaggi legittimi.
IM-Flooder	Programmi che "contaminano" il traffico dei client IM	Inviano un numero elevato di messaggi agli utenti dei client IM. La grande quantità di messaggi impedisce agli utenti di visualizzare i messaggi legittimi.
SMS-Flooder	Programmi per il flooding del traffico con messaggi SMS	Inviano numerosi messaggi SMS ai telefoni cellulari.

- **Adware**

  Sottocategoria: Software pubblicitario (adware);

  Livello di pericolo: Medio

  Gli adware visualizzano informazioni pubblicitarie all'utente. Mostrano banner pubblicitari nell'interfaccia di altri programmi e ridirigono le query di ricerca verso siti pubblicitari. Alcuni programmi adware raccolgono informazioni di marketing sull'utente e le inviano ai loro sviluppatori, come ad esempio i nomi dei siti Web visitati o il contenuto delle ricerche effettuate. A differenza dei programmi di tipo Trojan-Spy, gli adware inviano queste informazioni allo sviluppatore con l'autorizzazione dell'utente.

- **Auto-dialer**

  Sottocategoria: Auto-Dialer (Dialer).

  Livello di pericolo: Medio

  Gli Auto-Dialer possono stabilire di nascosto connessioni telefoniche utilizzando un modem.

- **Software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali**

  Sottocategoria: software legittimo utilizzabile da malintenzionati per danneggiare il computer o i dati personali.

  Livello di pericolo: Medio

  Molte applicazioni di questo tipo sono utili, pertanto numerosi utenti le eseguono. Queste applicazioni includono client IRC, auto-dialer, programmi per il download di file, monitor delle attività di sistema dei computer, utilità per la gestione delle password e server Internet per FTP, HTTP e Telnet.

  Se tuttavia gli intrusi ottengono l'accesso a questi programmi o se li installano nel computer dell'utente, alcune delle funzionalità dei programmi possono essere utilizzate per violare la sicurezza.

  Queste applicazioni variano a seconda della funzione; i diversi tipi sono descritti nella seguente tabella.

Tipo	Nome	Descrizione
Client-IRC	Client di chat Internet	Gli utenti installano questi programmi per comunicare con altre persone nelle Internet Relay Chat. Gli intrusi li usano per diffondere malware.
Downloader	Programmi per il download di file	Questi programmi possono eseguire segretamente il download di file da pagine Web.
Monitor	Programmi di monitoraggio	Questi programmi consentono il monitoraggio dei computer in cui sono installati (visualizzazione delle applicazioni attive e di come scambiano dati con le applicazioni in altri computer).
PSWTool	Strumenti di recupero delle password	Consentono di visualizzare e ripristinare le password dimenticate. Gli intrusi li installano segretamente nei computer degli utenti esattamente con lo stesso obiettivo.
RemoteAdmin	Programmi di amministrazione remota	Questi programmi vengono spesso utilizzati dagli amministratori di sistema. Questi programmi consentono di accedere all'interfaccia di un computer remoto per monitorarlo e gestirlo. Gli intrusi li installano segretamente nei computer degli utenti esattamente con lo stesso obiettivo: monitorare e gestire computer remoti. I programmi legittimi di amministrazione remota sono diversi dai programmi Trojan di amministrazione remota di tipo Backdoor. I programmi Trojan sono in grado di infiltrarsi autonomamente nel sistema operativo e di installarsi, mentre i programmi legittimi non presentano questa caratteristica.
Server-FTP	Server FTP	Questi programmi operano come server FTP. Gli intrusi li installano nei computer degli utenti per ottenere l'accesso remoto tramite il protocollo FTP.
Server-Proxy	Server proxy	Questi programmi operano come server proxy. Gli intrusi li installano nei computer degli utenti per inviare spam a nome dell'utente.

Tipo	Nome	Descrizione
Server-Telnet	Server Telnet	Questi programmi operano come server Telnet. Gli intrusi li installano nei computer degli utenti per ottenere l'accesso remoto tramite il protocollo Telnet.
Server-Web	Server Web	Questi programmi operano come server Web. Gli intrusi li installano nei computer degli utenti per ottenere l'accesso remoto tramite il protocollo HTTP.
RiskTool	Strumenti per l'utilizzo del computer locale	Questi strumenti offrono agli utenti opzioni aggiuntive per l'utilizzo del computer. Consentono di nascondere i file o le finestre delle applicazioni attive e di chiudere i processi attivi.
NetTool	Strumenti di rete	Questi strumenti offrono all'utente opzioni aggiuntive per l'utilizzo di altri computer della rete. Consentono di riavviare altri computer, rilevare le porte aperte e avviare le applicazioni installate in tali computer.
Client-P2P	Programmi client Peer-to-Peer	Consentono di utilizzare le reti peer-to-peer. Gli intrusi possono utilizzarli per diffondere malware.
Client-SMTP	Client SMTP	Inviano messaggi e-mail a insaputa dell'utente. Gli intrusi li installano nei computer degli utenti per inviare spam a nome dell'utente.
WebToolbar	Barre degli strumenti Web	Aggiungono barre degli strumenti per l'utilizzo di motori di ricerca alle interfacce di altre applicazioni.
FraudTool	Programmi fraudolenti	Questi programmi si camuffano da altri programmi reali. Vi sono ad esempio programmi anti-virus fraudolenti che visualizzano messaggi sul rilevamento di malware. senza tuttavia rilevare o disinfettare alcun oggetto.

- **Oggetti compressi che potrebbero nascondere codice dannoso**

  Sottocategoria: file compressi che possono causare danni.

  Livello di pericolo: Medio.

  Il file viene compresso tramite uno speciale programma di compressione utilizzato per la compressione del malware: virus, worm, Trojan. Kaspersky Endpoint Security esamina il modulo del programma di decompressione contenuti negli archivi autoestraenti.

  Per nascondere il malware dal rilevamento da parte di un anti-virus, gli hacker lo comprimono utilizzando programmi di compressione speciali. Gli esperti di Kaspersky hanno identificato i programmi di compressione più diffusi tra gli hacker.

- **Oggetti con compressione multipla**

  Sottocategoria: file in più pacchetti.

  Livello di pericolo: Medio.

  Il file è stato compresso con uno o più programmi di compressione tre o più volte.

  Per nascondere il malware dal rilevamento da parte di un anti-virus, gli hacker possono comprimere un file più volte. Kaspersky Endpoint Security scansiona i file compressi.

Per impostazione predefinita, Kaspersky Endpoint Security rileva tutti i tipi di oggetti. È consigliabile lasciare abilitato il rilevamento di tutti i tipi di oggetti per migliorare la protezione del computer. Se si utilizzano utilità interne rilevate dall'applicazione come dannose, aggiungere queste utilità a un elenco di esclusioni, ma non disabilitare il rilevamento dell'intero tipo di oggetti.

Come selezionare i tipi di oggetti rilevabili in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.

3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.
5. Nel blocco **Tipi di oggetti rilevati**, fare clic sul pulsante **Impostazioni**.
6. Nella finestra che si apre, selezionare le caselle di controllo accanto ai tipi di oggetti che devono essere rilevati da Kaspersky Endpoint Security:
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come selezionare i tipi di oggetti rilevabili in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

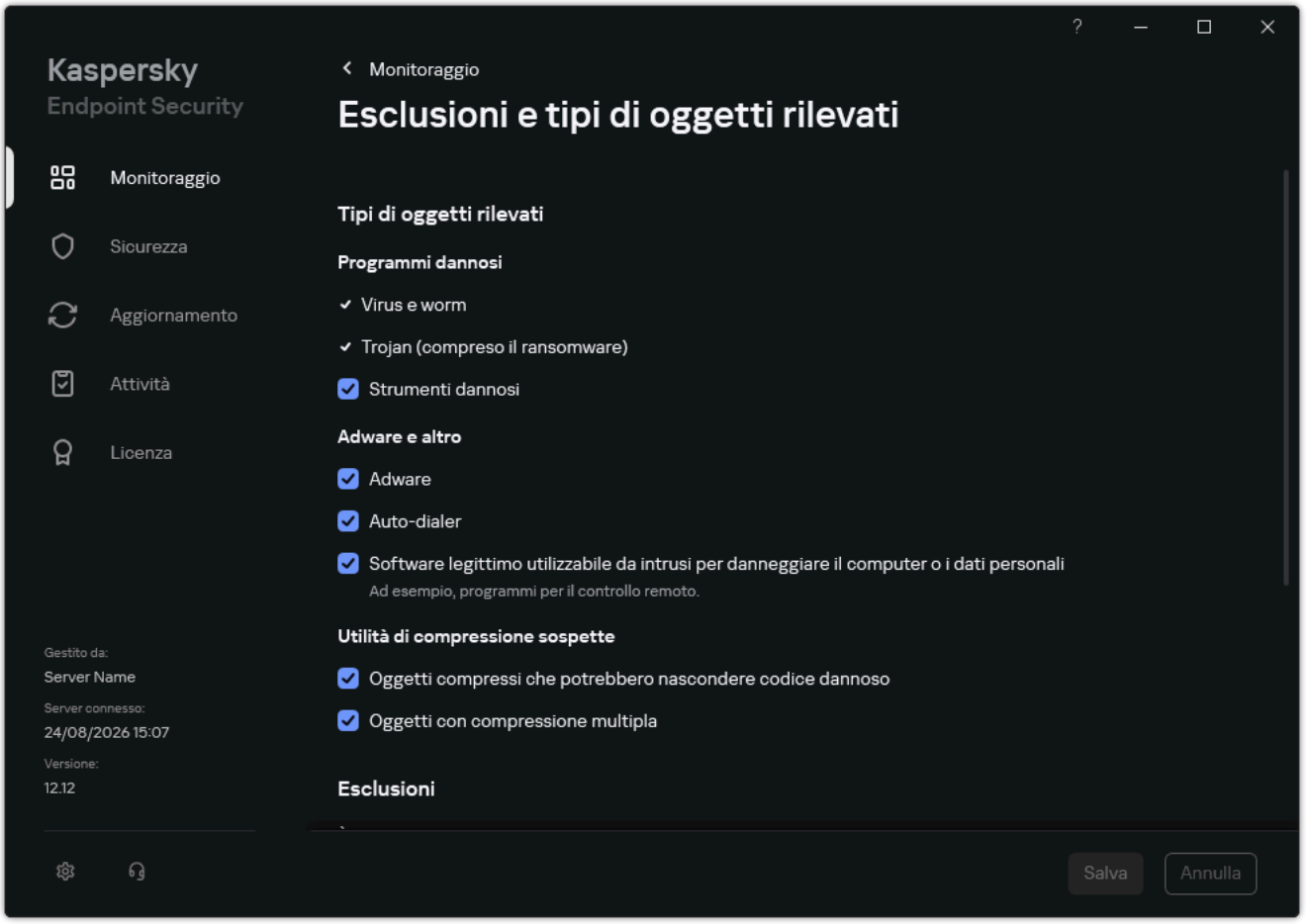
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di rilevamento**.
5. Nel blocco **Rilevamento di altri tipi di oggetti** selezionare le caselle di controllo accanto ai tipi di oggetti che devono essere rilevati da Kaspersky Endpoint Security.
6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come selezionare i tipi di oggetti rilevabili nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti rilevati**.

3. Nel blocco **Tipi di oggetti rilevati** selezionare le caselle di controllo accanto ai tipi di oggetti che devono essere rilevati da Kaspersky Endpoint Security.

4. Salvare le modifiche.



Tipi di oggetti rilevabili

Modifica dell'elenco di applicazioni attendibili

L'*elenco delle applicazioni attendibili* è un elenco di applicazioni per cui Kaspersky Endpoint Security non monitora le attività sui file e di rete (incluse le attività dannose) e l'accesso al Registro di sistema. Per impostazione predefinita, Kaspersky Endpoint Security monitora gli oggetti aperti, eseguiti o salvati da qualsiasi processo di applicazione e controlla l'attività di tutte le applicazioni e il traffico di rete che generano. Dopo aver aggiunto un'applicazione all'elenco delle applicazioni attendibili, Kaspersky Endpoint Security interrompe il monitoraggio delle attività dell'applicazione.

La differenza tra le esclusioni dalla scansione e le applicazioni attendibili è che per le esclusioni Kaspersky Endpoint Security non esamina i file, mentre per le applicazioni attendibili non controlla i processi avviati. Se un'applicazione attendibile crea un file dannoso in una cartella non inclusa nelle esclusioni dalla scansione, Kaspersky Endpoint Security rileverà il file ed eliminerà la minaccia. Se la cartella viene aggiunta alle esclusioni, Kaspersky Endpoint Security ignorerà questo file.

Se ad esempio si considerano sicuri gli oggetti utilizzati dall'applicazione Blocco note di Microsoft Windows, ovvero si ritiene attendibile questa applicazione, è possibile aggiungere Blocco note di Microsoft Windows all'elenco delle applicazioni attendibili affinché gli oggetti utilizzati da questa applicazione non vengano monitorati. In questo modo, si aumenteranno le prestazioni del computer, specialmente quando si utilizzano applicazioni server.

Inoltre, determinate azioni classificate da Kaspersky Endpoint Security come sospette possono essere sicure nel contesto della funzionalità di numerose applicazioni. Ad esempio, l'intercettazione del testo digitato sulla tastiera è un processo di routine per le applicazioni che commutano automaticamente i layout di tastiera, come Punto Switcher. Per tenere conto delle caratteristiche specifiche di tali applicazioni ed escluderne le attività dal monitoraggio, è consigliabile aggiungere le applicazioni di questo tipo all'elenco delle applicazioni attendibili.

Le applicazioni attendibili consentono di evitare problemi di compatibilità tra Kaspersky Endpoint Security e altre applicazioni (ad esempio, il problema della doppia scansione del traffico di rete di un computer di terzi da parte di Kaspersky Endpoint Security e di un'altra applicazione antivirus).

Il file eseguibile e il processo dell'applicazione attendibile sono comunque sottoposti a scansione alla ricerca di virus e altro malware. Utilizzando le esclusioni dalla scansione, è possibile escludere completamente un'applicazione dalla scansione da parte di Kaspersky Endpoint Security.

Come aggiungere un'applicazione all'elenco delle applicazioni attendibili in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.
5. Nel blocco **Esclusioni dalla scansione e applicazioni attendibili** → **Applicazioni attendibili**, fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata una finestra contenente un elenco di applicazioni attendibili.
6. Selezionare la casella di controllo **Unisci i valori quando vengono ereditati** se si desidera creare un elenco consolidato di applicazioni attendibili per tutti i computer dell'azienda. Gli elenchi delle applicazioni attendibili nei criteri padre e figlio verranno uniti. Gli elenchi verranno uniti a condizione che l'unione dei valori durante l'ereditarietà sia abilitata. Le applicazioni attendibili del criterio padre vengono visualizzate nei criteri figlio in una visualizzazione di sola lettura. Non è possibile modificare o eliminare le applicazioni attendibili del criterio padre.
7. Selezionare la casella di controllo **Consenti l'utilizzo delle applicazioni attendibili locali** se si desidera consentire all'utente di creare un elenco locale di applicazioni attendibili. In questo modo, un utente può creare il proprio elenco locale di applicazioni attendibili oltre all'elenco generale di applicazioni attendibili generato nel criterio. Un amministratore può utilizzare Kaspersky Security Center per visualizzare, aggiungere, modificare o eliminare gli elementi dell'elenco nelle proprietà del computer.

   Se la casella di controllo è deselezionata, l'utente può accedere solo all'elenco generale delle applicazioni attendibili generato nel criterio. Inoltre, se questa casella di controllo è deselezionata, Kaspersky Endpoint Security nasconde l'elenco consolidato delle applicazioni attendibili nell'interfaccia utente dell'applicazione.
8. Fare clic su **Aggiungi** e selezionare un'azione:

   - **Categoria**. È possibile raggruppare le applicazioni attendibili in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'applicazione attendibile alla categoria.
   - **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova applicazione attendibile alla radice dell'elenco.

- **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include *applicazioni attendibili predefinite*. Sono state inoltre aggiunte applicazioni attendibili predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le applicazioni attendibili predefinite a seconda dello scopo del server protetto.

- **Nuova esclusione nella categoria selezionata**. Per aggiungere una nuova applicazione attendibile a una categoria specifica, selezionare una categoria.

9. Selezionare i criteri di attendibilità:

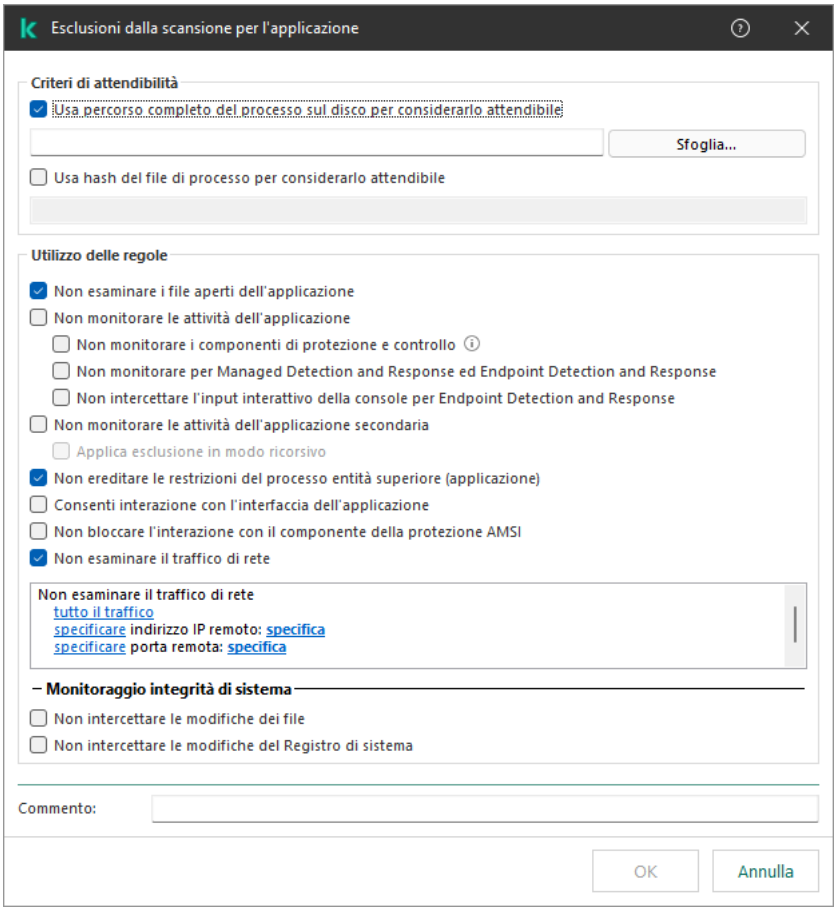
- **Usa percorso completo del processo sul disco per considerarlo attendibile**. Immettere il percorso completo del file eseguibile dell'applicazione attendibile.

  Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

  Kaspersky Endpoint Security considera il nome file di un'applicazione attendibile tenendo conto della distinzione tra maiuscole e minuscole. Se il nome file inserito ha una maiuscola e una minuscola errate, Kaspersky Endpoint Security non riconoscerà l'applicazione attendibile.

- **Usa hash del file di processo per considerarlo attendibile**.

Kaspersky Endpoint Security non supporta la variabile di ambiente `%userprofile%` quando si genera un elenco di applicazioni attendibili nella console Kaspersky Security Center. Per applicare la voce a tutti gli account utente, è possibile utilizzare il carattere * (ad esempio, `C:\Users\*\Documents\File.exe`). Ogni volta che si aggiunge una nuova variabile di ambiente, è necessario riavviare l'applicazione.



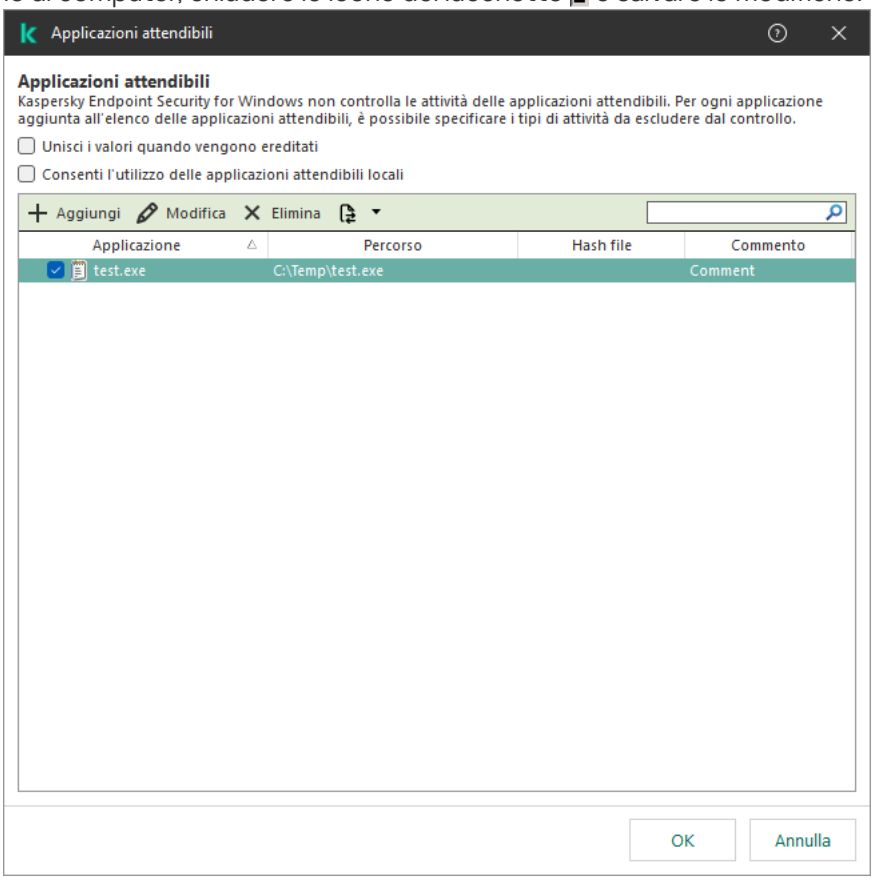
Impostazioni delle applicazioni attendibili

10. Configurare le impostazioni avanzate per l'applicazione attendibile (vedere la tabella seguente).

11. Fare clic su **OK**.

    La nuova applicazione attendibile verrà aggiunta all'elenco. È possibile escludere un'applicazione dall'area attendibile in qualsiasi momento utilizzando la casella di controllo accanto all'oggetto.

12. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.



Elenco di applicazioni attendibili

Come aggiungere un'applicazione all'elenco delle applicazioni attendibili in Kaspersky Security Center Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare alla sezione **Area attendibile**.

5. Nella finestra visualizzata, fare clic sul collegamento **Applicazioni**.

   Verrà visualizzata una finestra contenente un elenco di applicazioni attendibili.

6. Selezionare la casella di controllo **Unisci i valori quando vengono ereditati** se si desidera creare un elenco consolidato di applicazioni attendibili per tutti i computer dell'azienda. Gli elenchi delle applicazioni attendibili nei criteri padre e figlio verranno uniti. Gli elenchi verranno uniti a condizione che l'unione dei valori durante l'ereditarietà sia abilitata. Le applicazioni attendibili del criterio padre vengono visualizzate nei criteri figlio in una visualizzazione di sola lettura. Non è possibile modificare o eliminare le applicazioni attendibili del criterio padre.

7. Selezionare la casella di controllo **Consenti l'utilizzo delle esclusioni locali** se si desidera consentire all'utente di creare un elenco locale di applicazioni attendibili. In questo modo, un utente può creare il proprio elenco locale di applicazioni attendibili oltre all'elenco generale di applicazioni attendibili generato nel criterio. Un amministratore può utilizzare Kaspersky Security Center per visualizzare, aggiungere, modificare o eliminare gli elementi dell'elenco nelle proprietà del computer.

   Se la casella di controllo è deselezionata, l'utente può accedere solo all'elenco generale delle applicazioni attendibili generato nel criterio. Inoltre, se questa casella di controllo è deselezionata, Kaspersky Endpoint Security nasconde l'elenco consolidato delle applicazioni attendibili nell'interfaccia utente dell'applicazione.

8. Fare clic su **Aggiungi** e selezionare un'azione:

   - **Categoria**. È possibile raggruppare le applicazioni attendibili in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'applicazione attendibile alla categoria.
   - **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova applicazione attendibile alla radice dell'elenco.
   - **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include *applicazioni attendibili predefinite*. Sono state inoltre aggiunte applicazioni attendibili predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le applicazioni attendibili predefinite a seconda dello scopo del server protetto.

   Per aggiungere una nuova applicazione attendibile a una categoria specifica, selezionare la casella di controllo accanto a tale categoria e selezionare l'opzione **Nuova esclusione**.

9. Selezionare i criteri di attendibilità:

   - **Percorso del file o della cartella**. Immettere il percorso completo del file eseguibile dell'applicazione attendibile.

     Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

     Kaspersky Endpoint Security considera il nome file di un'applicazione attendibile tenendo conto della distinzione tra maiuscole e minuscole. Se il nome file inserito ha una maiuscola e una minuscola errate, Kaspersky Endpoint Security non riconoscerà l'applicazione attendibile.

   - **Hash applicazione**.

   Kaspersky Endpoint Security non supporta la variabile di ambiente %userprofile% quando si genera un elenco di applicazioni attendibili nella console Kaspersky Security Center. Per applicare la voce a tutti gli account utente, è possibile utilizzare il carattere `*` (ad esempio, `C:\Users\*\Documents\File.exe`). Ogni volta che si aggiunge una nuova variabile di ambiente, è necessario riavviare l'applicazione.

10. Configurare le impostazioni avanzate per l'applicazione attendibile (vedere la tabella seguente).

11. Fare clic su **OK**.

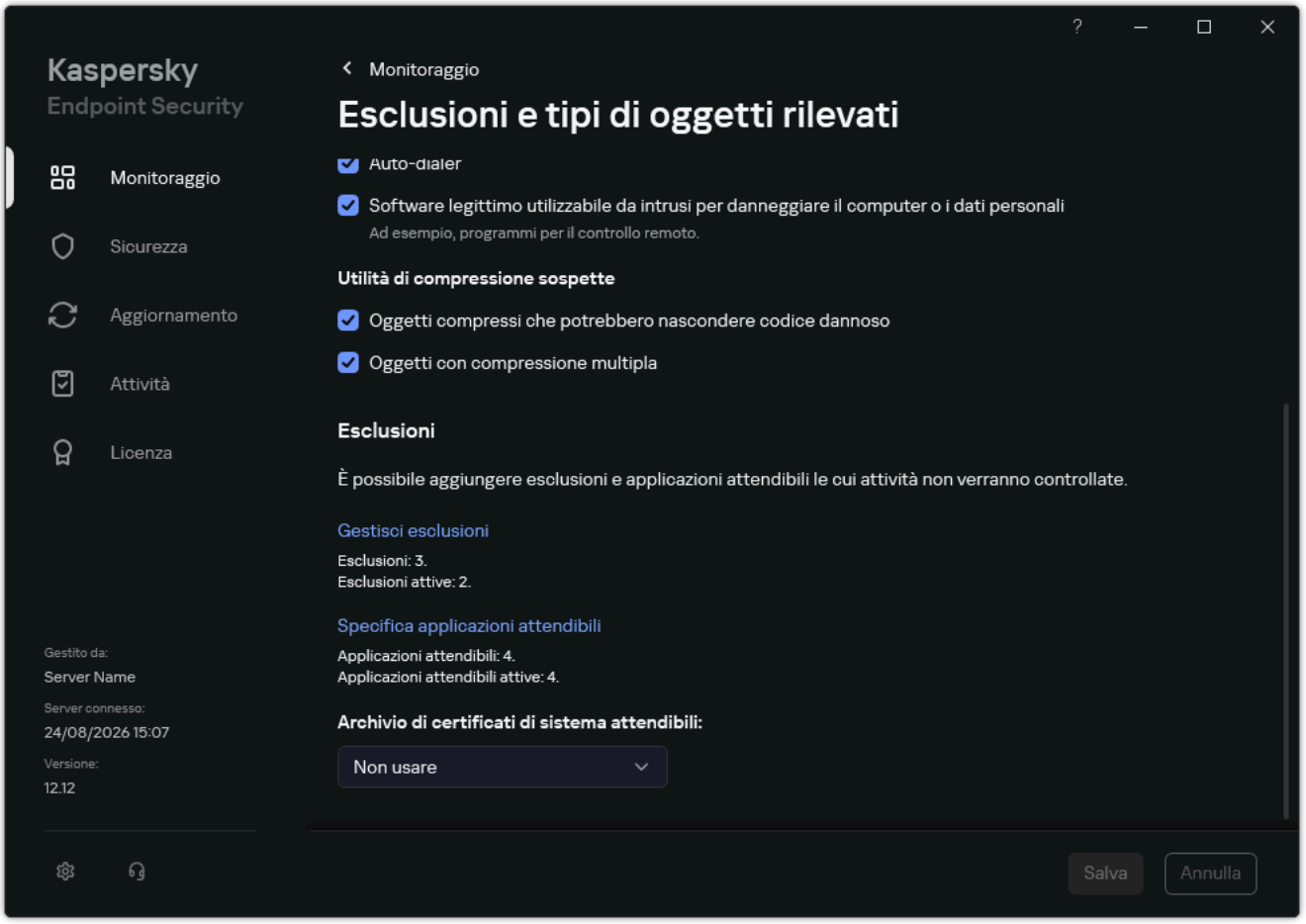
    La nuova applicazione attendibile verrà aggiunta all'elenco. È possibile escludere un'applicazione dall'area attendibile in qualsiasi momento utilizzando la casella di controllo nel colonna **Stato**.

12. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come aggiungere un'applicazione all'elenco delle applicazioni attendibili nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti rilevati**.
3. Nella sezione **Esclusioni**, fare clic sul collegamento **Specifica applicazioni attendibili**.

Kaspersky Endpoint Security nasconde l'elenco consolidato delle applicazioni attendibili nell'interfaccia utente dell'applicazione se la configurazione delle applicazioni attendibili è bloccata dall'amministratore nella console (simbolo del "lucchetto chiuso") e le applicazioni attendibili locali sono vietate (la casella di controllo **Consenti l'utilizzo delle applicazioni attendibili locali** è deselezionata).



Impostazioni delle esclusioni

4. Fare clic su **Aggiungi** e selezionare un'azione:

- **Categoria**. È possibile raggruppare le applicazioni attendibili in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'applicazione attendibile alla categoria.
- **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova applicazione attendibile alla radice dell'elenco.
- **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include *applicazioni attendibili predefinite*. Sono state inoltre aggiunte applicazioni attendibili predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le applicazioni attendibili predefinite a seconda dello scopo del server protetto.

Per aggiungere una nuova applicazione attendibile a una categoria specifica, selezionare la casella di controllo accanto a tale categoria e selezionare l'opzione **Nuova esclusione**.

5. Selezionare i criteri di attendibilità:

   - **Usa percorso completo del processo sul disco per considerarlo attendibile**. Immettere il percorso completo del file eseguibile dell'applicazione attendibile.

     Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

     Kaspersky Endpoint Security considera il nome file di un'applicazione attendibile tenendo conto della distinzione tra maiuscole e minuscole. Se il nome file inserito ha una maiuscola e una minuscola errate, Kaspersky Endpoint Security non riconoscerà l'applicazione attendibile.

   - **Usa hash del file di processo per considerarlo attendibile**.

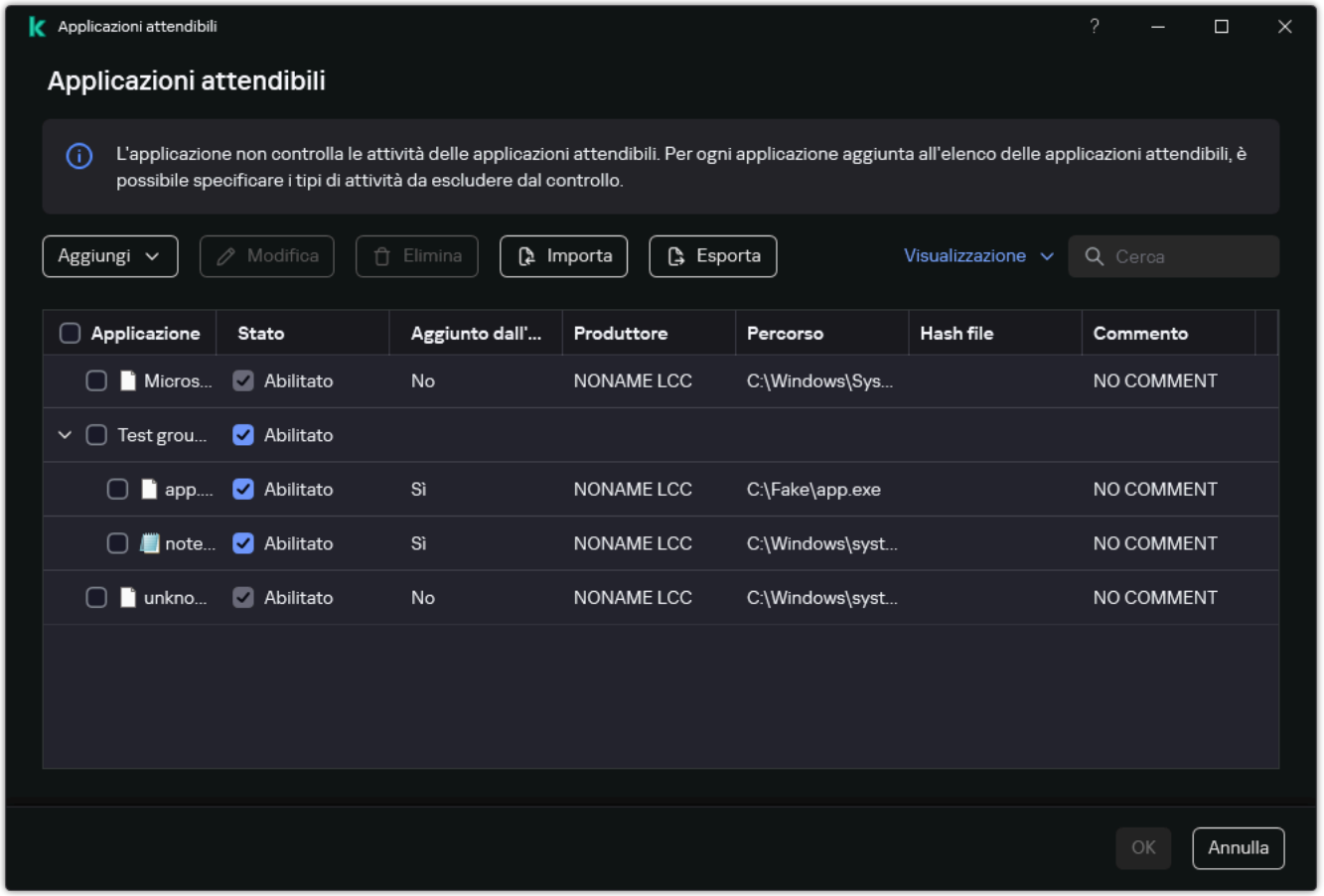
   Kaspersky Endpoint Security supporta le variabili di ambiente e converte il percorso nell'interfaccia locale dell'applicazione. In altre parole, se si immette il percorso file `%userprofile%\Documents\File.exe`, viene aggiunto un record `C:\Users\Fred123\Documents\File.exe` nell'interfaccia utente dell'applicazione per l'utente Fred123. Di conseguenza, Kaspersky Endpoint Security ignora il programma attendibile `File.exe` per gli altri utenti. Per applicare la voce a tutti gli account utente, è possibile utilizzare il carattere `*` (ad esempio, `C:\Users\*\Documents\File.exe`). Ogni volta che si aggiunge una nuova variabile di ambiente, è necessario riavviare l'applicazione.

6. Nella finestra delle proprietà dell'applicazione attendibile, configurare le impostazioni avanzate.

7. Fare clic su **OK**.

   La nuova applicazione attendibile verrà aggiunta all'elenco. È possibile escludere un'applicazione dall'area attendibile in qualsiasi momento utilizzando la casella di controllo nel colonna **Stato**.

8. Salvare le modifiche.



Elenco di applicazioni attendibili

Impostazioni delle applicazioni attendibili

Parametro	Descrizione
Non esaminare i file aperti dall'applicazione	Tutti i file aperti dall'applicazione sono esclusi dalle scansioni di Kaspersky Endpoint Security. Se ad esempio si utilizzano applicazioni per eseguire il backup dei file, questa funzionalità consente di ridurre l'utilizzo di risorse da parte di Kaspersky Endpoint Security.
Non monitorare le attività dell'applicazione	Kaspersky Endpoint Security non monitorerà l'attività file e rete dell'applicazione nel sistema operativo. È possibile configurare il monitoraggio delle attività delle applicazioni per diversi componenti di Kaspersky Endpoint Security: • **Non monitorare i componenti di protezione e controllo**. L'attività dell'applicazione è monitorata dai seguenti componenti: Rilevamento del Comportamento, Prevenzione Exploit, Prevenzione Intrusioni Host, Motore di Remediation e Firewall. • **Non monitorare per Managed Detection and Response ed Endpoint Detection and Response**. Le attività dell'applicazione sono monitorate dall'agente MDR integrato e dall'agente EDR (KATA) integrato. • **Non intercettare l'input interattivo della console per Endpoint Detection and Response**. Kaspersky Endpoint Security non invia dati di telemetria sulla gestione dell'applicazione nella console. I dati di telemetria vengono utilizzati da Kaspersky Anti Targeted Attack Platform (EDR).
Non monitorare le attività dell'applicazione secondaria	Kaspersky Endpoint Security non monitorerà l'attività file o l'attività di rete delle applicazioni avviate dall'applicazione. È possibile applicare l'esclusione in modo ricorsivo. In modo che l'applicazione non monitori le attività dell'intera catena di applicazioni secondarie.
Non ereditare le restrizioni dal processo entità superiore (applicazione)	Le restrizioni configurate per il processo principale non verranno applicate da Kaspersky Endpoint Security a un processo secondario. Il processo principale viene avviato da un'applicazione per la quale sono configurati i diritti dell'applicazione (Prevenzione Intrusioni Host) e le regole di rete delle applicazioni (Firewall).
Non monitorare le attività dell'applicazione secondaria	Kaspersky Endpoint Security non monitorerà l'attività file o l'attività di rete delle applicazioni avviate dall'applicazione. È possibile applicare l'esclusione in modo ricorsivo. In modo che l'applicazione non monitori le attività dell'intera catena di applicazioni secondarie.
Consenti interazione con l'interfaccia dell'applicazione	Auto-difesa di Kaspersky Endpoint Security blocca tutti i tentativi di gestire i servizi delle applicazioni da un computer remoto. Se la casella di controllo è selezionata, l'applicazione di accesso remoto può gestire le impostazioni di Kaspersky Endpoint Security tramite l'interfaccia di Kaspersky Endpoint Security.
Non bloccare l'interazione con il componente della protezione AMSI	Kaspersky Endpoint Security non monitorerà le richieste dell'applicazione attendibile per gli oggetti che verranno esaminati dal componente Protezione AMSI.

Parametro	Descrizione
Non esaminare il traffico di rete	Il traffico di rete avviato dall'applicazione verrà escluso dalle scansioni di Kaspersky Endpoint Security. È possibile escludere tutto il traffico o solo il traffico criptato dalle scansioni. È inoltre possibile escludere singoli indirizzi IP e numeri di porta dalle scansioni. Kaspersky Endpoint Security versione 14.0 o precedente non supporta l'esclusione del traffico di rete se viene specificato un hash per un'applicazione attendibile anziché un percorso.
Non intercettare le modifiche dei file *(disponibile solo in Kaspersky Security Center Console)*	Kaspersky Endpoint Security non monitora le modifiche nei file dall'ambito di monitoraggio Monitoraggio integrità di sistema. L'applicazione applica l'esclusione a tutte le modalità di monitoraggio dell'integrità del sistema: Monitoraggio integrità di sistema in tempo reale e Controllo integrità di sistema su richiesta.
Non intercettare le modifiche del Registro di sistema *(disponibile solo in Kaspersky Security Center Console)*	Kaspersky Endpoint Security non monitora le modifiche alle chiavi del Registro di sistema dall'ambito di monitoraggio Monitoraggio integrità di sistema. L'applicazione applica l'esclusione a tutte le modalità di monitoraggio dell'integrità del sistema: Monitoraggio integrità di sistema in tempo reale e Controllo integrità di sistema su richiesta.
Commento	Se necessario, è possibile specificare un breve commento per l'applicazione attendibile. I commenti consentono di semplificare le ricerche e l'ordinamento delle applicazioni attendibili.
Stato	Stato dell'applicazione attendibile: • Lo stato **Attivo** indica che l'applicazione si trova nell'area attendibile. • Lo stato **Inattivo** indica che l'applicazione è esclusa dall'area attendibile.

Creazione di un'area attendibile locale

L'utente ora può creare la propria area attendibile locale per un computer specifico. In questo modo, l'utente può creare i propri elenchi locali di esclusioni e applicazioni attendibili oltre all'area attendibile generale in un criterio. Un amministratore può consentire o bloccare l'uso di esclusioni locali o applicazioni attendibili locali nelle impostazioni dei criteri. A tale scopo, utilizzare le caselle di controllo **Consenti l'utilizzo delle esclusioni locali** e **Consenti l'utilizzo delle applicazioni attendibili locali** nella sezione **Esclusioni** del criterio.

Se la creazione di un'area attendibile locale è consentita da un amministratore, l'utente può aggiungere le proprie esclusioni di scansione e applicazioni attendibili nell'interfaccia utente dell'applicazione. Allo stesso tempo, l'utente non dispone delle autorizzazioni per modificare o eliminare oggetti dalla zona attendibile configurata nel criterio. L'amministratore può anche visualizzare, aggiungere, modificare o eliminare elementi dell'elenco nella console di Kaspersky Security Center se è necessario aggiungere esclusioni per un singolo computer.

Kaspersky Endpoint Security nasconde gli elenchi delle esclusioni dalle scansioni e delle applicazioni attendibili nell'interfaccia utente dell'applicazione se la configurazione dell'area attendibile è bloccata dall'amministratore nella console (simbolo del "lucchetto chiuso") e le esclusioni dalle scansioni locali e le applicazioni attendibili sono vietate.

Come aggiungere un oggetto all'area attendibile locale in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, aprire la cartella con il nome del gruppo di amministrazione a cui appartengono i computer client desiderati.
3. Nell'area di lavoro, selezionare la scheda **Dispositivi**.
4. Fare doppio clic per aprire la finestra delle proprietà del computer.

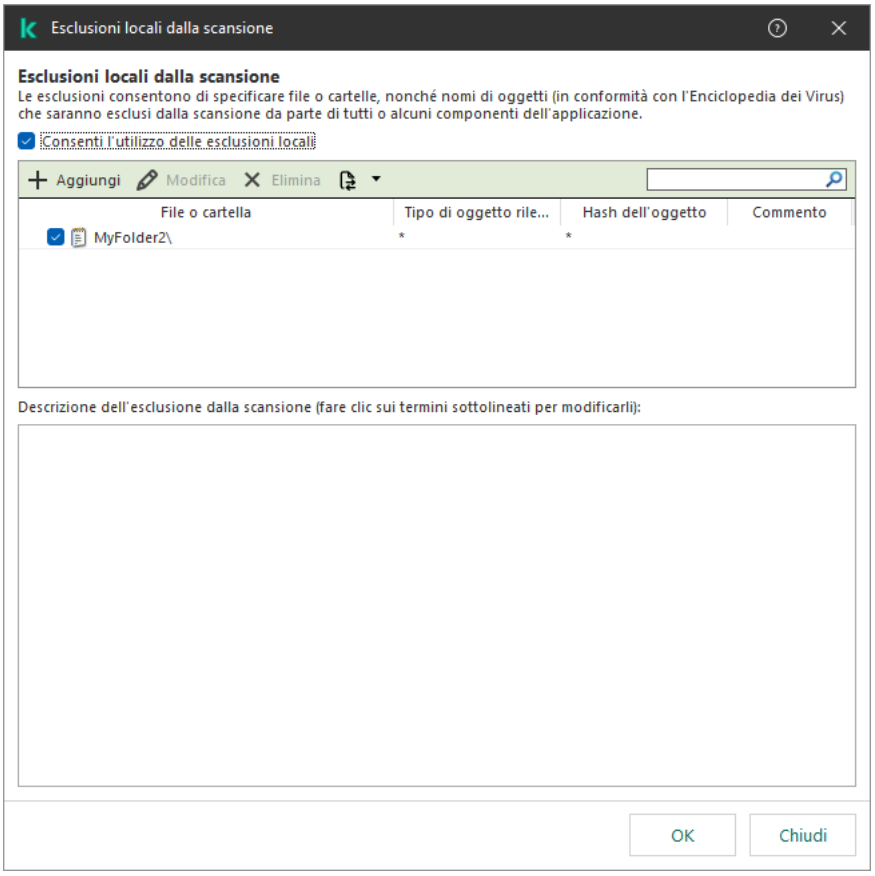
5. Nella finestra delle proprietà del computer, selezionare la sezione **Applicazioni**.

6. Nell'elenco delle applicazioni Kaspersky installate nel computer selezionare **Kaspersky Endpoint Security for Windows (14.2)** e fare doppio clic per aprire le proprietà dell'applicazione.

7. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.

8. Nel blocco **Esclusioni dalla scansione e applicazioni attendibili** → **Esclusioni locali dalla scansione**, fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata una finestra contenente un elenco di esclusioni locali.



Impostazioni delle aree attendibili

9. Creare un elenco delle esclusioni locali dalla scansione.

   Le regole per la creazione di esclusioni locali dalla scansione sono gli stessi delle esclusioni generiche. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

10. Nel blocco **Esclusioni dalla scansione e applicazioni attendibili** → **Applicazioni attendibili locali**, fare clic sul pulsante **Impostazioni**.

    Verrà visualizzata una finestra contenente un elenco di applicazioni attendibili locali.

11. Creare un elenco di applicazioni attendibili locali.

    Le regole per aggiungere applicazioni all'elenco delle applicazioni attendibili locali sono le stesse delle regole per aggiungerle all'elenco generale. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

12. Salvare le modifiche.

Come aggiungere un oggetto all'area attendibile locale in Kaspersky Security Center Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Fare clic sul nome del computer sul quale si desidera consentire a un utente di eseguire un'azione bloccata.
3. Selezionare la scheda **Applicazioni**.
4. Fare clic su **Kaspersky Endpoint Security for Windows**.

   Verranno visualizzate le impostazioni locali dell'applicazione.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti rilevati**.
7. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili**, fare clic sul collegamento **Esclusioni locali dalla scansione**.
8. Creare un elenco delle esclusioni locali dalla scansione.

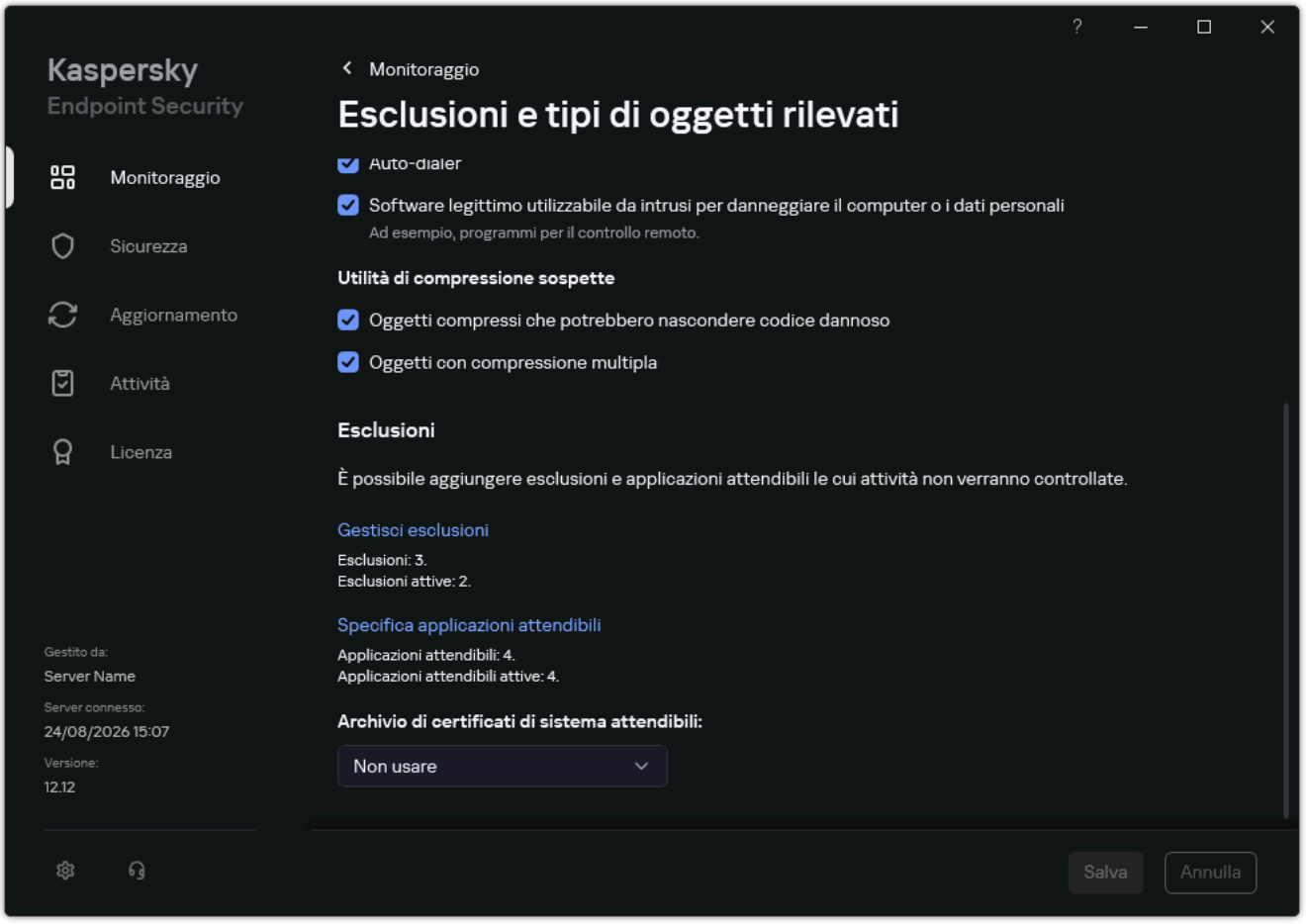
   Le regole per la creazione di esclusioni locali sono le stesse delle regole per la creazione delle esclusioni generiche. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.
9. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili**, fare clic sul collegamento **Applicazioni attendibili locali**.
10. Creare un elenco di applicazioni attendibili locali.

    Le regole per aggiungere applicazioni all'elenco delle applicazioni attendibili locali sono le stesse delle regole per aggiungerle all'elenco generale. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.
11. Salvare le modifiche.

Come creare un'esclusione locale dalla scansione nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti rilevati**.
3. Nella sezione **Esclusioni**, fare clic sul collegamento **Gestisci esclusioni**.

Kaspersky Endpoint Security nasconde l'elenco delle esclusioni dalle scansioni nell'interfaccia utente dell'applicazione se la configurazione delle esclusioni dalle scansioni è bloccata dall'amministratore nella console (simbolo del "lucchetto chiuso") e le esclusioni delle scansioni locali sono vietate (la casella di controllo **Consenti l'utilizzo delle esclusioni locali** è deselezionata).



Impostazioni delle esclusioni

4. Fare clic su **Aggiungi** e selezionare un'azione:

   - **Categoria**. È possibile raggruppare le esclusioni dalle scansioni in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'esclusione dalle scansioni alla categoria.
   - **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova esclusione dalle scansioni alla radice dell'elenco.
   - **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include le *esclusioni dalla scansione predefinite*. Sono state inoltre aggiunte esclusioni dalla scansione predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le esclusioni dalle scansioni predefinite a seconda dello scopo del server protetto.

   Per aggiungere una nuova esclusione dalla scansione a una categoria specifica, selezionare la casella di controllo accanto a tale categoria e selezionare l'opzione **Nuova esclusione**.

5. Se si desidera escludere un file o una cartella dalle scansioni, selezionare il file o la cartella facendo clic sul pulsante **Sfoglia**.

È inoltre possibile immettere il percorso manualmente. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera:

- Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

- Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.

- Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

  È possibile utilizzare le maschere all'inizio, al centro o alla fine del percorso file. Ad esempio, se si desidera aggiungere una cartella per tutti gli utenti alle esclusioni, immettere la maschera `?:\Users\*\Folder\`.

  È possibile escludere le cartelle di rete. A tale scopo, immettere manualmente il percorso della cartella di rete (ad esempio `\\Network Share\*`).

6. Se si desidera escludere un tipo specifico di oggetto dalle scansioni, nel campo **Tipi di oggetto rilevato** immettere il nome del tipo di oggetto in base alla classificazione dell'Enciclopedia Kaspersky (ad esempio `Email-Worm`, `Rootkit` o `RemoteAdmin`).

   È possibile utilizzare maschere con il carattere `?` (sostituisce un singolo carattere) e il carattere `*` (sostituisce un numero qualsiasi di caratteri). Se ad esempio viene specificata la maschera `Client*`, Kaspersky Endpoint Security esclude gli oggetti `Client-IRC`, `Client-P2P` e `Client-SMTP` dalle scansioni.

7. Se si desidera escludere un singolo file dalle scansioni, immettere l'hash del file nel campo **Hash dell'oggetto**.

   Se il file viene modificato, verrà modificato anche l'hash del file. In tal caso, il file modificato non verrà aggiunto alle esclusioni.

8. Nella sezione **Componenti della protezione** selezionare i componenti a cui si desidera applicare l'esclusione dalla scansione.

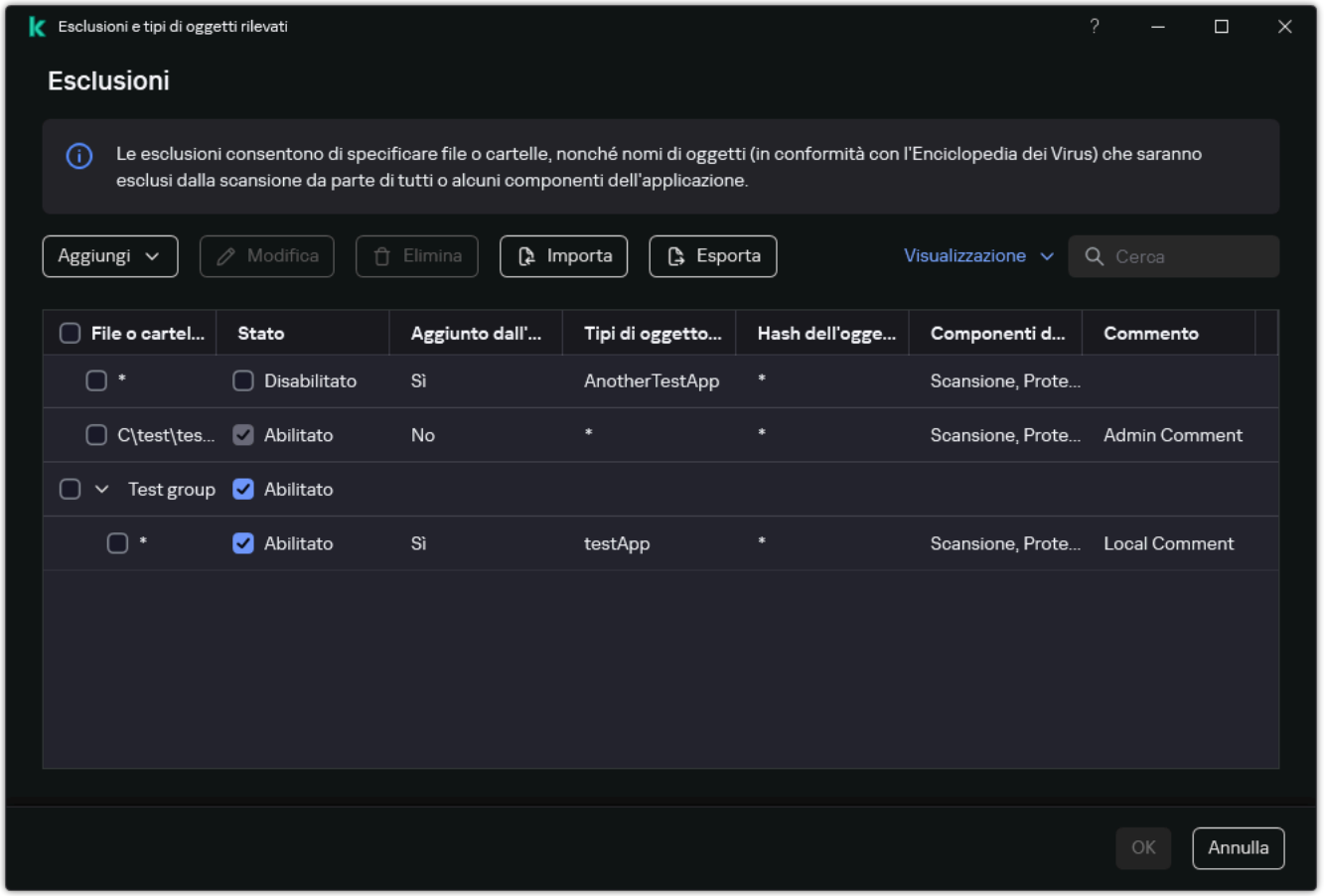
9. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.

10. Selezionare lo stato **Attivo** per l'esclusione.

11. Fare clic su **Aggiungi**.

    La nuova esclusione verrà aggiunta all'elenco. È possibile disabilitare l'esclusione in qualsiasi momento utilizzando la casella di controllo nella colonna **Stato**.

12. Salvare le modifiche.



Elenco delle esclusioni

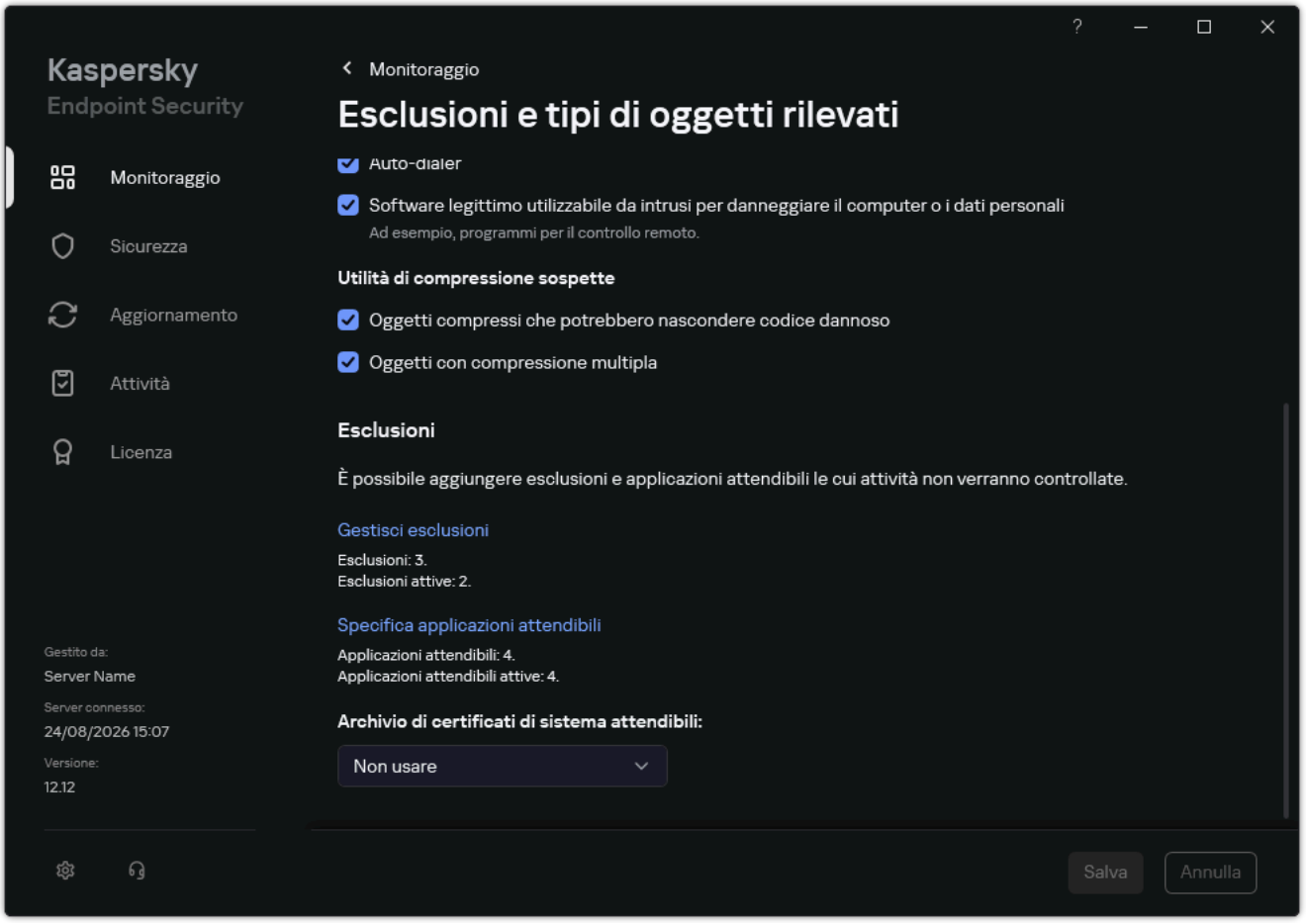
Come aggiungere un'applicazione all'elenco delle applicazioni attendibili locali nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali → Esclusioni e tipi di oggetti rilevati**.

3. Nella sezione **Esclusioni**, fare clic sul collegamento **Specifica applicazioni attendibili**.

Kaspersky Endpoint Security nasconde l'elenco consolidato delle applicazioni attendibili nell'interfaccia utente dell'applicazione se la configurazione delle applicazioni attendibili è bloccata dall'amministratore nella console (simbolo del "lucchetto chiuso") e le applicazioni attendibili locali sono vietate (la casella di controllo **Consenti l'utilizzo delle applicazioni attendibili locali** è deselezionata).



Impostazioni delle esclusioni

4. Fare clic su **Aggiungi** e selezionare un'azione:

   - **Categoria**. È possibile raggruppare le applicazioni attendibili in categorie separate. Per creare una nuova categoria, immettere il nome della categoria e aggiungere almeno un'applicazione attendibile alla categoria.
   - **Nuova esclusione**. Kaspersky Endpoint Security aggiunge una nuova applicazione attendibile alla radice dell'elenco.
   - **Selezionare l'esclusione dall'elenco**. Per configurare rapidamente Kaspersky Endpoint Security nei server SQL, nei server Microsoft Exchange e System Center Configuration Manager, l'applicazione include *applicazioni attendibili predefinite*. Sono state inoltre aggiunte applicazioni attendibili predefinite per supportare la configurazione delle applicazioni negli ambienti virtuali Citrix e VMware. È necessario selezionare le applicazioni attendibili predefinite a seconda dello scopo del server protetto.

   Per aggiungere una nuova applicazione attendibile a una categoria specifica, selezionare la casella di controllo accanto a tale categoria e selezionare l'opzione **Nuova esclusione**.

5. Selezionare i criteri di attendibilità:

   - **Usa percorso completo del processo sul disco per considerarlo attendibile**. Immettere il percorso completo del file eseguibile dell'applicazione attendibile.

Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

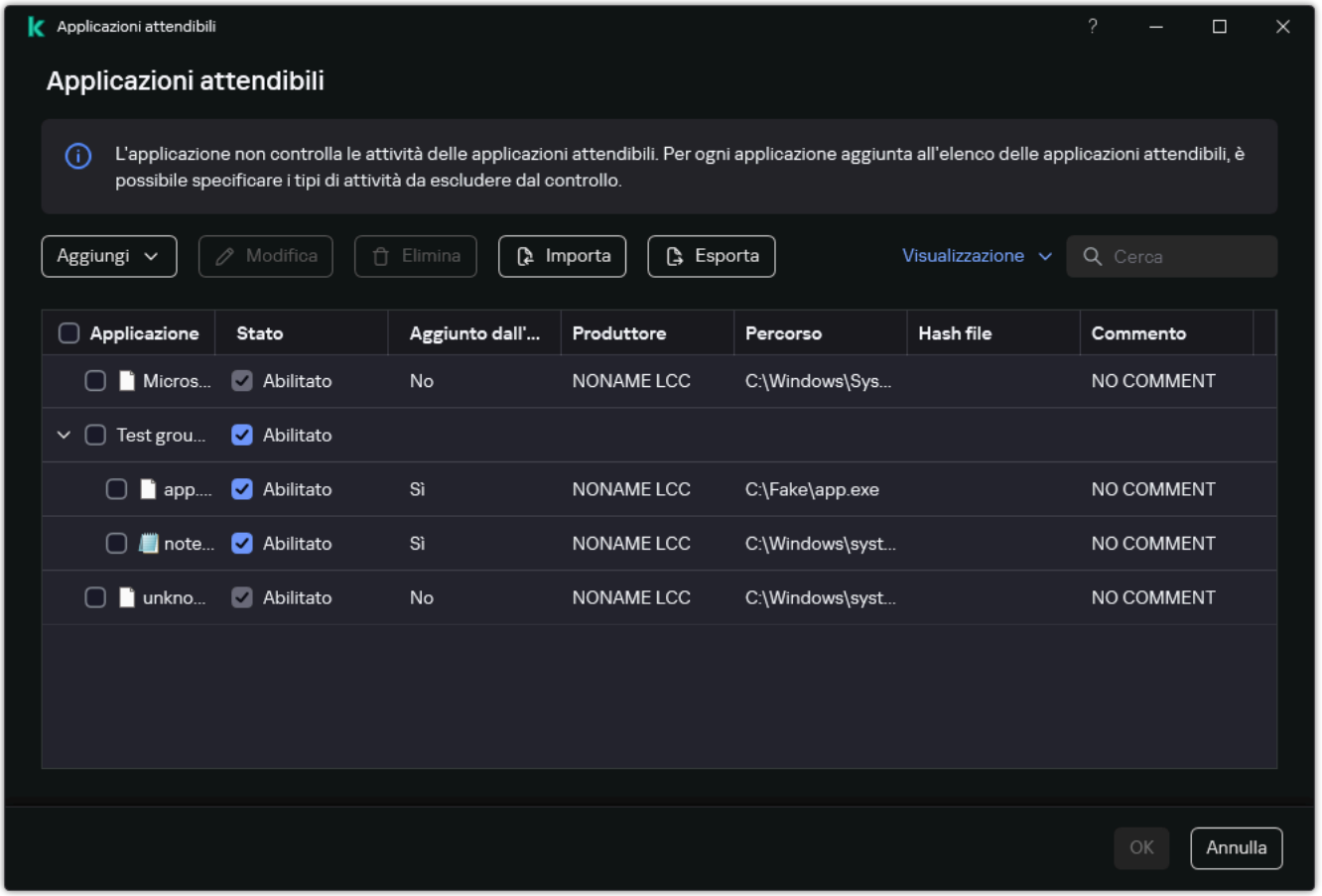
Kaspersky Endpoint Security considera il nome file di un'applicazione attendibile tenendo conto della distinzione tra maiuscole e minuscole. Se il nome file inserito ha una maiuscola e una minuscola errate, Kaspersky Endpoint Security non riconoscerà l'applicazione attendibile.

- **Usa hash del file di processo per considerarlo attendibile**.

Kaspersky Endpoint Security supporta le variabili di ambiente e converte il percorso nell'interfaccia locale dell'applicazione. In altre parole, se si immette il percorso file `%userprofile%\Documents\File.exe`, viene aggiunto un record `C:\Users\Fred123\Documents\File.exe` nell'interfaccia utente dell'applicazione per l'utente Fred123. Di conseguenza, Kaspersky Endpoint Security ignora il programma attendibile `File.exe` per gli altri utenti. Per applicare la voce a tutti gli account utente, è possibile utilizzare il carattere `*` (ad esempio, `C:\Users\*\Documents\File.exe`). Ogni volta che si aggiunge una nuova variabile di ambiente, è necessario riavviare l'applicazione.

6. Nella finestra delle proprietà dell'applicazione attendibile, configurare le impostazioni avanzate.
7. Fare clic su **OK**.

   La nuova applicazione attendibile verrà aggiunta all'elenco. È possibile escludere un'applicazione dall'area attendibile in qualsiasi momento utilizzando la casella di controllo nel colonna **Stato**.
8. Salvare le modifiche.



Elenco di applicazioni attendibili

Esportazione e importazione dell'area attendibile

Un'*area attendibile* è un elenco configurato dall'amministratore di sistema di oggetti e applicazioni che non vengono monitorati da Kaspersky Endpoint Security durante l'esecuzione. L'area attendibile è costituita dai seguenti elenchi: *esclusioni dalla scansione* e *applicazioni attendibili*. È possibile esportare questi elenchi in file XML e altri formati. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di esclusioni dello stesso tipo. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco delle esclusioni e l'elenco di applicazioni attendibili o per eseguire la migrazione degli elenchi in un altro server.

L'applicazione utilizza i seguenti formati per l'esportazione e l'importazione dell'*elenco delle esclusioni*:

- XML è disponibile in Administration Console (MMC), Web Console e Cloud Console.
- DAT è disponibile solo per l'importazione in Administration Console (MMC). Lo scopo di questo formato è mantenere la compatibilità con le versioni precedenti dell'applicazione. È possibile convertire un file DAT in XML in Administration Console (MMC) per eseguire la migrazione degli elenchi di esclusione a Web Console.
- CSV è disponibile solo nell'interfaccia locale dell'applicazione.

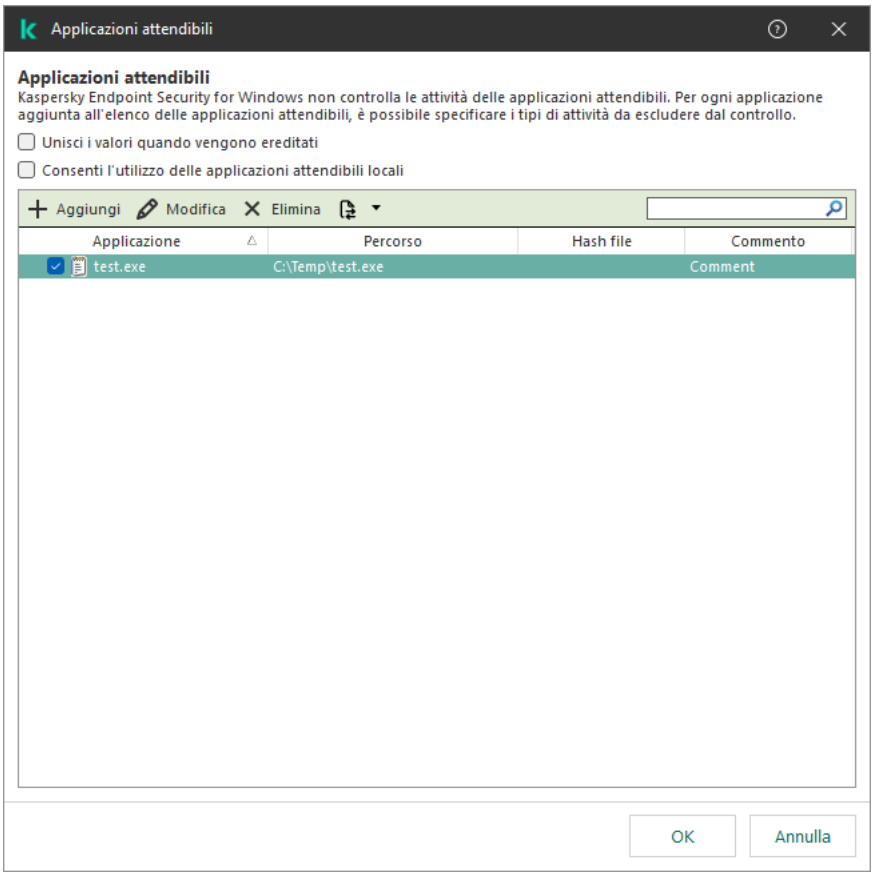
Kaspersky Endpoint Security utilizza il formato XML per l'esportazione e l'importazione dell'*elenco di applicazioni attendibili*.

Come esportare e importare l'area attendibile in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.
4. In **Esclusioni dalla scansione e applicazioni attendibili**, selezionare il componente dell'area attendibile che si desidera esportare o importare: **Esclusioni dalla scansione** o **Applicazioni attendibili**.
5. Fare clic su **Impostazioni**.
6. Per esportare l'elenco delle regole:
   a. Selezionare le esclusioni che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.
      Se non è stata selezionata alcuna esclusione, Kaspersky Endpoint Security esporterà tutte le esclusioni.
   b. Fare clic sul pulsante → **Esporta**.
   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle esclusioni e selezionare la cartella in cui si desidera salvare il file.

d. Salvare il file.

Kaspersky Endpoint Security esporta l'intero elenco di esclusioni nel file XML. Kaspersky Endpoint Security supporta anche l'esportazione dell'elenco di esclusioni in un file DAT.



Elenco di applicazioni attendibili

7. Per importare l'elenco delle esclusioni:

a. Fare clic sul pulsante → **Importa**.

b. Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle esclusioni.

c. Aprire il file.

Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML. Kaspersky Endpoint Security supporta anche l'importazione di un elenco di esclusioni da un file DAT.

8. Salvare le modifiche.

Come esportare o importare l'area attendibile in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare alla sezione **Area attendibile**.

5. Per esportare l'elenco delle regole:

   a. Fare clic sul collegamento **Esclusioni dalla scansione malware**.

   b. Selezionare le esclusioni che si desidera esportare.

   c. Fare clic sul pulsante → **Esporta**.

      Kaspersky Endpoint Security esporta l'elenco delle esclusioni in un file JSON nella cartella dei download predefinita.

6. Per esportare l'elenco delle applicazioni attendibili:

   a. Selezionare le applicazioni attendibili che si desidera esportare.

   b. Fare clic sul pulsante → **Esporta**.

      Kaspersky Endpoint Security esporta l'elenco delle applicazioni attendibili in un file JSON nella cartella dei download predefinita.

7. Per importare l'elenco delle esclusioni:

   a. Fare clic sul collegamento **Esclusioni dalla scansione malware**.

   b. Fare clic sul pulsante → **Importa**.

      Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco delle esclusioni.

   c. Aprire il file.

      Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

8. Per importare un elenco di applicazioni attendibili:

   a. Fare clic sul collegamento **Applicazioni**.

   b. Fare clic sul pulsante → **Importa**.

      Verrà visualizzata una finestra; in questa finestra, selezionare il file JSON da cui si desidera importare l'elenco di applicazioni attendibili.

   c. Aprire il file.

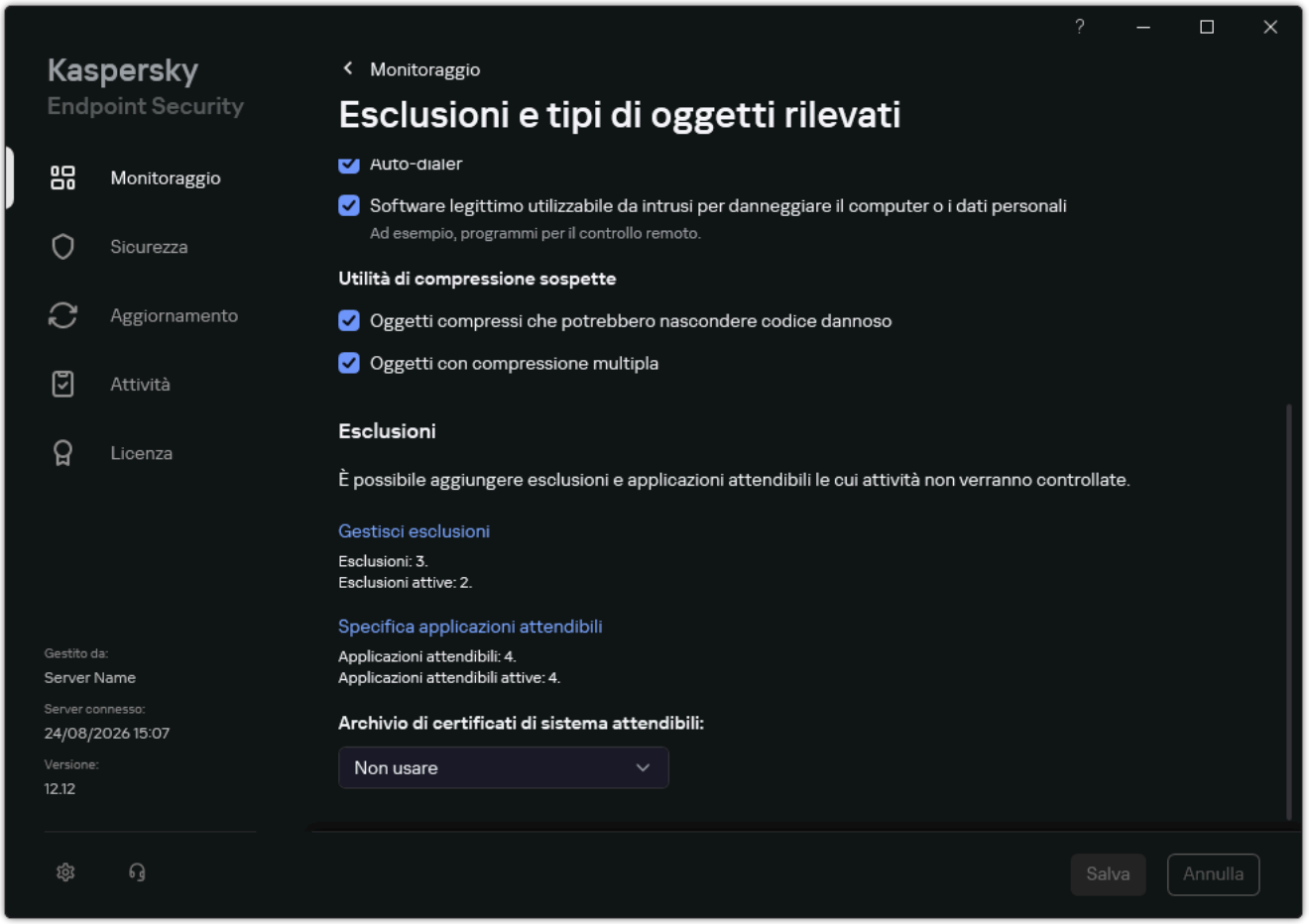
      Se il computer dispone già di un elenco di applicazioni attendibili, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

9. Salvare le modifiche.

Come esportare o importare l'area attendibile nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti rilevati**.



Impostazioni delle esclusioni

3. Per esportare l'elenco delle regole:

   a. Nella sezione **Esclusioni**, fare clic sul collegamento **Gestisci esclusioni**.

   b. Selezionare le esclusioni che si desidera esportare.

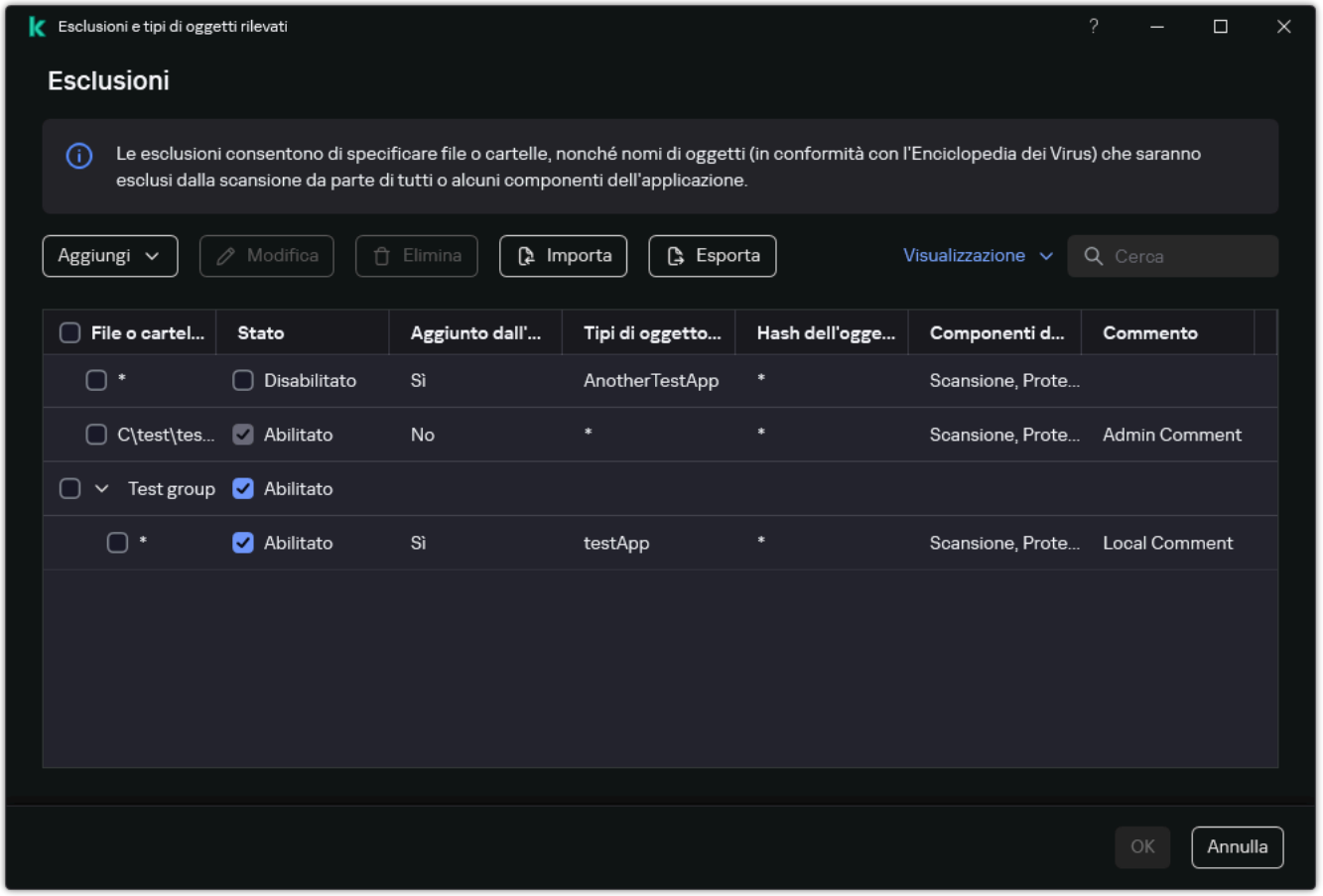
   c. Fare clic su **Esporta**.

   d. Confermare di voler esportare solo le esclusioni selezionate o esportare l'intero elenco di esclusioni.

   e. Nella finestra visualizzata specificare il nome del file CSV in cui si desidera esportare l'elenco delle esclusioni e selezionare la cartella in cui si desidera salvare il file.

f. Salvare il file.

Kaspersky Endpoint Security esporta l'intero elenco di esclusioni nel file CSV.



Elenco delle esclusioni

4. Per esportare l'elenco delle applicazioni attendibili:

   a. Nella sezione **Esclusioni**, fare clic sul collegamento **Specifica applicazioni attendibili**.

   b. Selezionare le applicazioni attendibili che si desidera esportare.

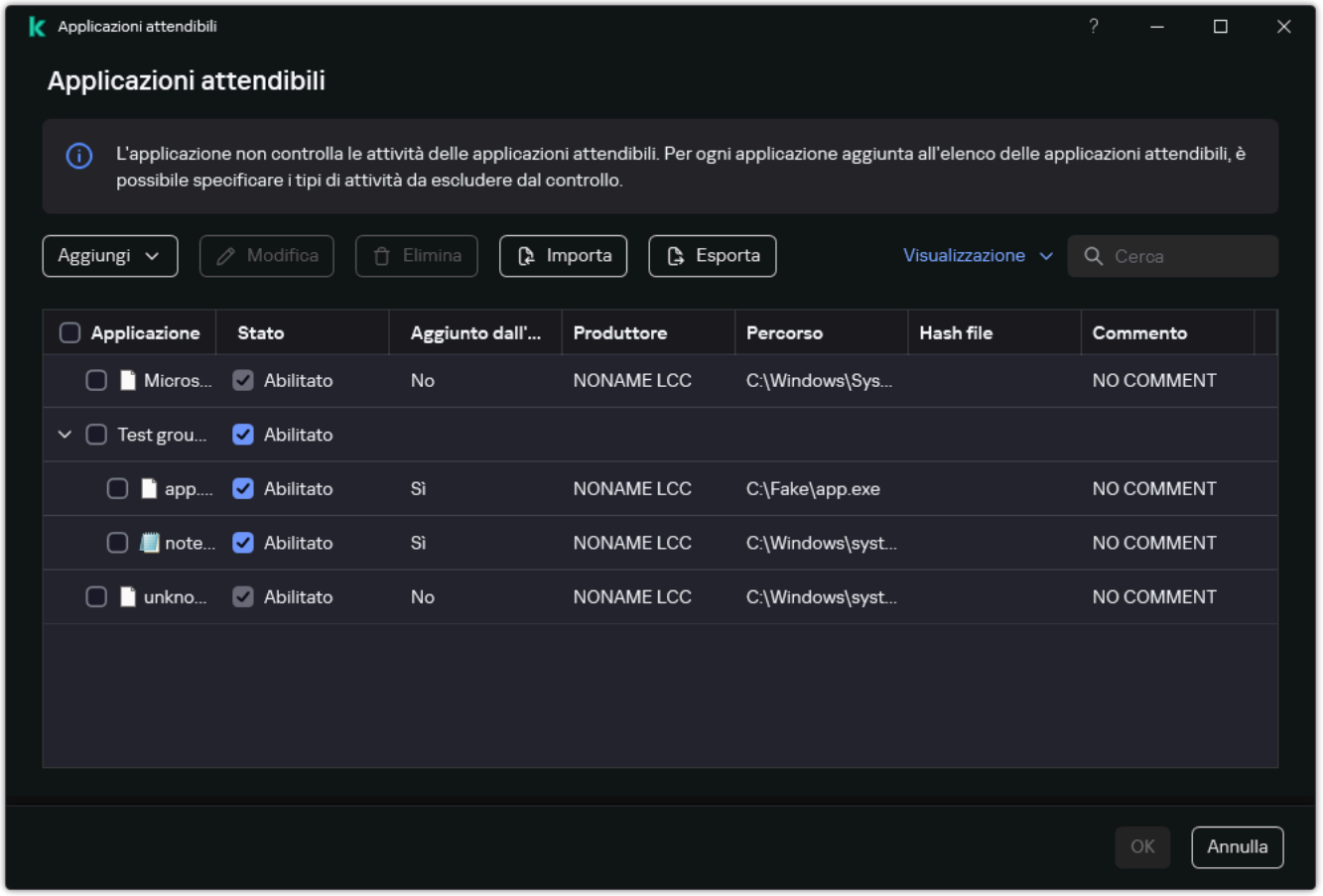
   c. Fare clic su **Esporta**.

   d. Confermare di voler esportare solo le applicazioni attendibili selezionate o esportare l'intero elenco.

   e. Viene visualizzata una finestra; in questa finestra, immettere il nome del file XML in cui si desidera esportare l'elenco di applicazioni attendibili e selezionare la cartella in cui si desidera salvare il file.

f. Salvare il file.

Kaspersky Endpoint Security esporta l'intero elenco di applicazioni attendibili nel file XML.



Elenco di applicazioni attendibili

5. Per importare l'elenco delle esclusioni:

a. Nella sezione **Esclusioni**, fare clic sul collegamento **Gestisci esclusioni**.

b. Fare clic su **Importa**.

c. Nella finestra visualizzata selezionare il file CSV da cui si desidera importare l'elenco delle esclusioni.

d. Aprire il file.

Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file CSV.

6. Per importare un elenco di applicazioni attendibili:

a. Nella sezione **Esclusioni**, fare clic sul collegamento **Specifica applicazioni attendibili**.

b. Fare clic su **Importa**.

c. Verrà visualizzata una finestra; in questa finestra, selezionare il file XML da cui si desidera importare l'elenco di applicazioni attendibili.

d. Aprire il file.

Se il computer dispone già di un elenco di applicazioni attendibili, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

7. Salvare le modifiche.

Gestione delle applicazioni con una firma digitale attendibile

L'utilizzo dell'archivio di certificati di sistema consente di escludere dalle scansioni virus le applicazioni dotate di una firma digitale attendibile. Kaspersky Endpoint Security assegna automaticamente tali applicazioni al gruppo *Attendibili*.

Come avviare l'utilizzo di un archivio dei certificati di sistema attendibili in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.
4. Nella sezione **Archivio di certificati di sistema attendibili** selezionare la casella di controllo **Usa archivio di certificati di sistema attendibili**.
5. Nell'elenco a discesa selezionare l'archivio di sistema che deve essere considerato attendibile da Kaspersky Endpoint Security.
6. Salvare le modifiche.

Come avviare l'utilizzo di un archivio dei certificati di sistema attendibili in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare alla sezione **Area attendibile**.
5. Nella finestra visualizzata, fare clic sul collegamento **Certificati radice**.
6. Nella finestra visualizzata, selezionare la casella di controllo **Usa archivio di certificati di sistema attendibili**.
7. Selezionare l'archivio di sistema che deve essere considerato attendibile da Kaspersky Endpoint Security.
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come avviare l'utilizzo di un archivio dei certificati di sistema attendibili nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti rilevati**.
3. Nell'elenco a discesa **Archivio di certificati di sistema attendibili** selezionare l'archivio di sistema che deve essere considerato attendibile da Kaspersky Endpoint Security.
4. Salvare le modifiche.

Appendice. Esclusioni dalle scansioni predefinite e applicazioni attendibili.

A partire da Kaspersky Endpoint Security 12.6 for Windows, le esclusioni dalle scansioni e le applicazioni attendibili vengono aggiunte all'area attendibile. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server. A partire da Kaspersky Endpoint Security 12.8 for Windows, è possibile installare l'applicazione in modalità Light Agent per proteggere gli ambienti virtuali. Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono contribuire a configurare rapidamente Kaspersky Endpoint Security negli ambienti virtuali Citrix e VMware.

È possibile selezionare le esclusioni predefinite e le applicazioni attendibili nei seguenti modi:

- Installazione dell'applicazione.
  - Installazione dell'applicazione in locale tramite la procedura guidata
  - Proprietà del pacchetto di installazione
- Impostazione del criterio.
  - Creazione guidata nuovo criterio
  - Proprietà dei criteri: esclusioni dalle scansioni e applicazioni attendibili.

Microsoft SQL Server

Quando si installa Kaspersky Endpoint Security in un server SQL, è necessario creare un'area attendibile dalle esclusioni e dalle applicazioni attendibili predefinite per assicurarsi che il funzionamento del server non subisca interferenze.

Esclusioni dalle scansioni predefinite

Percorso	Versione SQL
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange Server

Quando si installa Kaspersky Endpoint Security in un server Microsoft Exchange, è necessario creare un'area attendibile dalle esclusioni e dalle applicazioni attendibili predefinite per assicurarsi che il funzionamento del server non subisca interferenze.

Esclusioni dalle scansioni predefinite

Percorso	Versione di Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019

Percorso	Versione di Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Applicazioni attendibili predefinite

Percorso	Versione di Microsoft Exchange
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

Microsoft System Center Configuration Manager

Se Microsoft System Center Configuration Manager è installato nel sistema operativo del computer protetto, è necessario aggiungere un'esclusione predefinita all'elenco delle esclusioni dalla scansione per garantire il funzionamento stabile della soluzione.

Esclusioni dalle scansioni predefinite

Percorso	Versione di System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Quando si installa Kaspersky Endpoint Security in un ambiente virtuale Citrix, è necessario creare un'area attendibile dalle esclusioni e dalle applicazioni attendibili predefinite per assicurarsi che il funzionamento del server non subisca interferenze.

Esclusioni dalle scansioni predefinite

Percorso
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf

Percorso
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

Applicazioni attendibili predefinite

Percorso	Soluzione Citrix
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Desktop e app virtuali
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Desktop e app virtuali

Percorso	Soluzione Citrix
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Desktop e app virtuali
%SystemRoot%\System32\drivers\CVhdFilter.sys	Desktop e app virtuali
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Desktop e app virtuali
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Desktop e app virtuali
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Desktop e app virtuali
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Desktop e app virtuali
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Desktop e app virtuali
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Desktop e app virtuali
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Desktop e app virtuali
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	App area di lavoro
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	App area di lavoro
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	App area di lavoro
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	App area di lavoro
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	App area di lavoro
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	App area di lavoro
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	App area di lavoro

Percorso	Soluzione Citrix
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	App area di lavoro
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	App area di lavoro
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	App area di lavoro
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisioning
%SystemRoot%\System32\drivers\bnistack6.sys	Provisioning
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisioning
%SystemRoot%\System32\drivers\cnicteam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisioning
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

Quando si installa Kaspersky Endpoint Security in un ambiente virtuale VMware, è necessario creare un'area attendibile dalle applicazioni attendibili predefinite per assicurarsi che il funzionamento del server non subisca interferenze.

Applicazioni attendibili predefinite

Percorso	Soluzione VMware
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon

Percorso	Soluzione VMware
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

Deduplicazione dei dati in Microsoft Windows Server

Se la deduplicazione dei dati è abilitata nel sistema operativo Microsoft Windows Server in cui è installato Kaspersky Endpoint Security, è necessario aggiungere un'applicazione attendibile predefinita all'elenco delle applicazioni attendibili per ottimizzare Kaspersky Endpoint Security e ridurre il carico sulla CPU.

Applicazioni attendibili predefinite

Percorso	Versione di Microsoft Windows Server
`%SystemRoot%\system32\fsdmhost.exe`	Tutte le versioni supportate

Gestione di Backup

Backup archivia le copie di backup dei file eliminati o modificati durante la disinfezione. Una *copia di backup* è una copia del file creata prima della disinfezione o dell'eliminazione del file. Le copie di backup dei file vengono archiviate in un formato speciale e non rappresentano una minaccia.

Le copie di backup dei file vengono archiviate nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Agli utenti del gruppo Amministratori è concessa l'autorizzazione completa per l'accesso a questa cartella. All'utente il cui account è stato utilizzato per installare Kaspersky Endpoint Security vengono concessi diritti di accesso limitati alla cartella.

Kaspersky Endpoint Security non consente la possibilità di configurare le autorizzazioni per l'accesso dell'utente alle copie di backup dei file.

Talvolta non è possibile mantenere l'integrità dei file durante la disinfezione. Se dopo la disinfezione non è possibile accedere alle informazioni contenute in un file disinfettato o a una parte di esse, è possibile tentare di ripristinare il file dalla copia di backup nella cartella originale.

Se Kaspersky Endpoint Security viene eseguito nell'ambito della gestione di Kaspersky Security Center, le copie di backup dei file possono essere trasmesse a Kaspersky Security Center Administration Server. Per informazioni dettagliate sulla gestione delle copie di backup dei file in Kaspersky Security Center, consultare la Guida di Kaspersky Security Center.

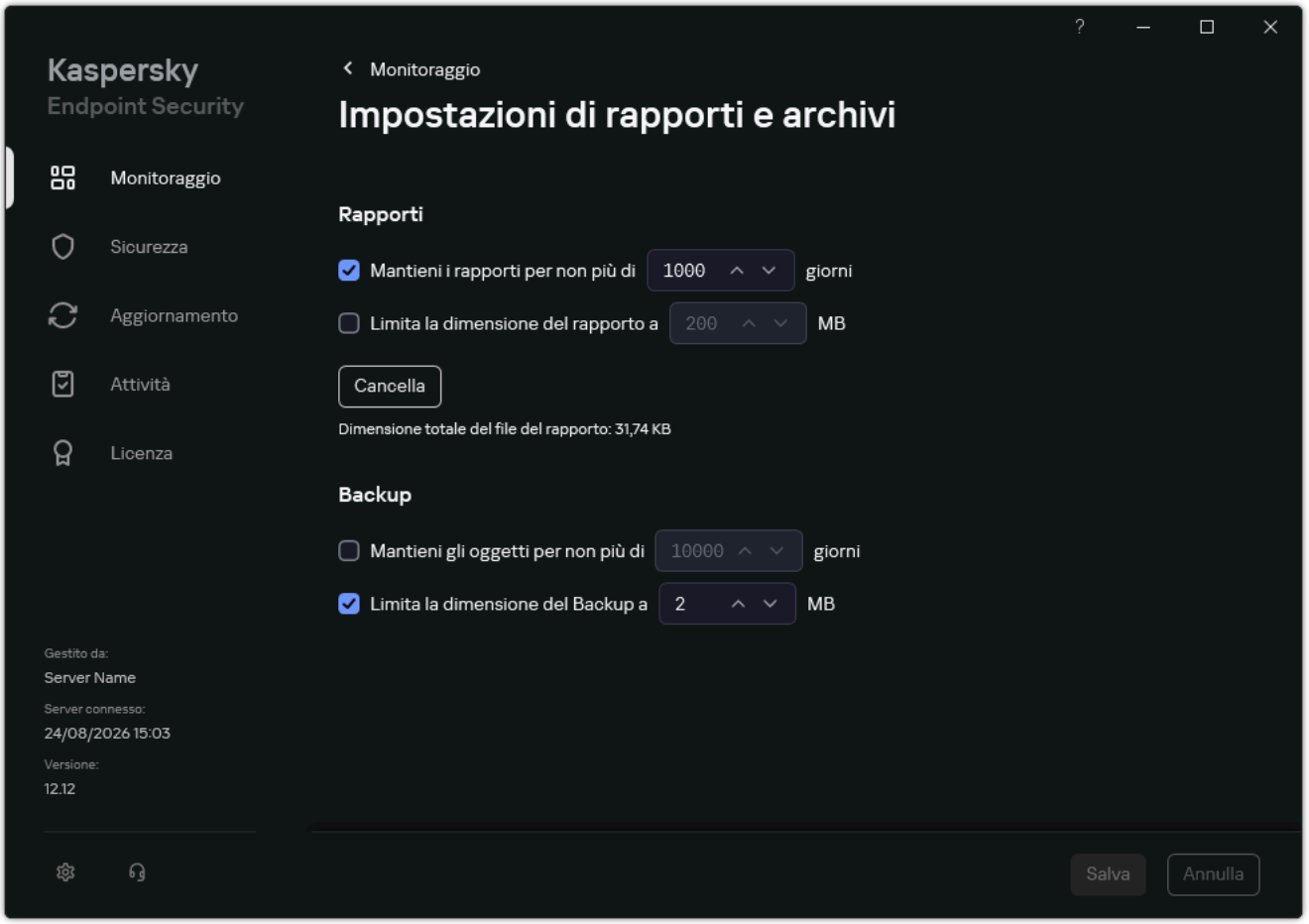
Configurazione del periodo massimo di archiviazione per i file in Backup

Per impostazione predefinita, il periodo massimo di archiviazione delle copie dei file in Backup è di 30 giorni. Al termine del periodo massimo di archiviazione, Kaspersky Endpoint Security elimina i file meno recenti da Backup.

Per configurare il periodo massimo di archiviazione per i file in Backup:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, in **Impostazioni generali**, fare clic sul riquadro **Rapporti e archivi**.



Impostazioni backup

3. Se si desidera limitare il periodo di archiviazione per le copie dei file in Backup, selezionare la casella di controllo **Mantieni gli oggetti per non più di N giorni** nella sezione **Backup**. Immettere la durata di archiviazione massima delle copie di file in Backup

4. Salvare le modifiche.

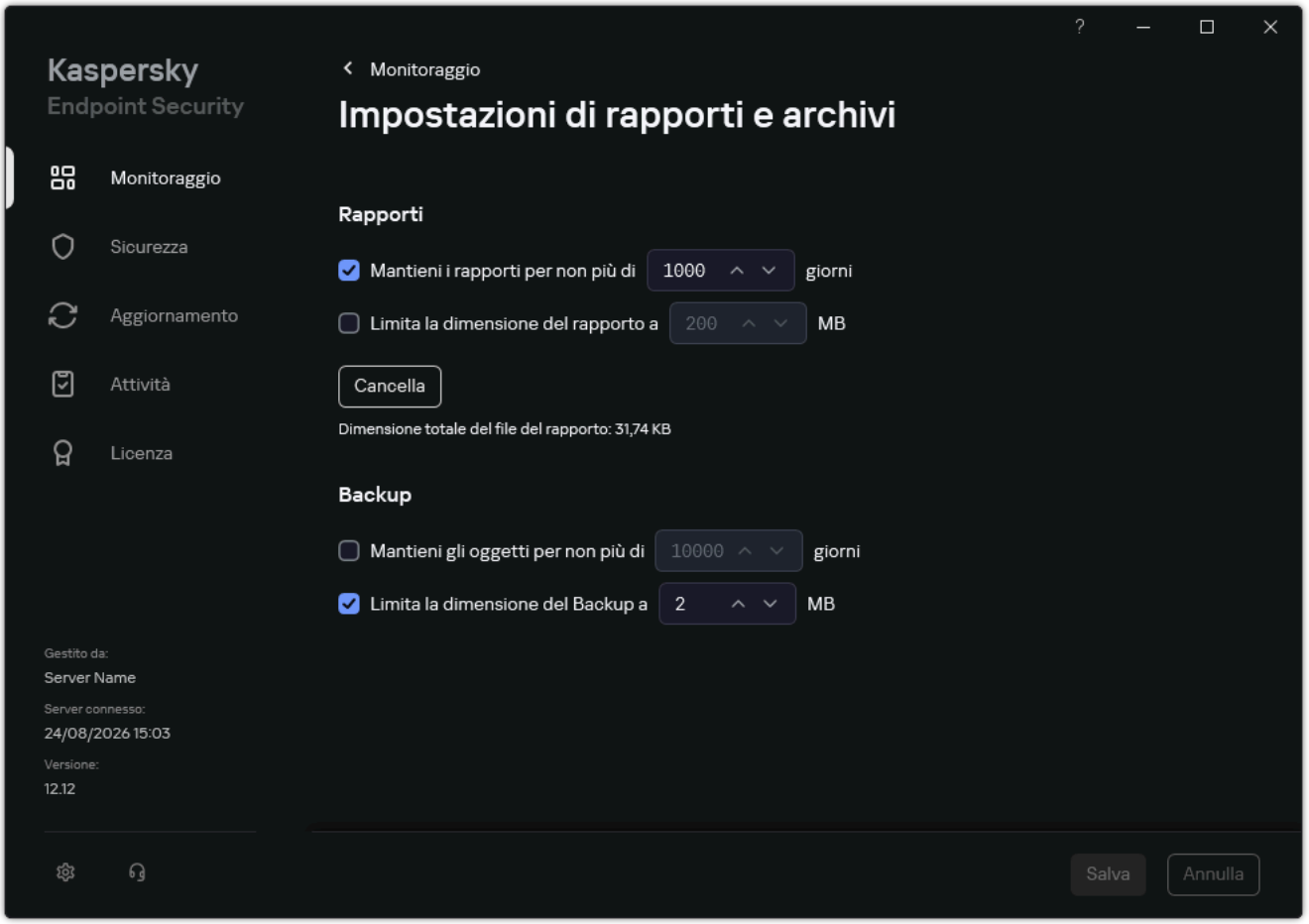
Configurazione della dimensione massima di Backup

È possibile specificare la dimensione massima di Backup. Le dimensioni di Backup sono illimitate per impostazione predefinita. Al raggiungimento della dimensione massima, Kaspersky Endpoint Security elimina automaticamente i file meno recenti da Backup.

Per configurare la dimensione massima di Backup:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, in **Impostazioni generali**, fare clic sul riquadro **Rapporti e archivi**.



Impostazioni backup

3. Nel blocco **Backup**, selezionare la casella di controllo **Limita la dimensione del Backup a N MB**. Se la casella di controllo è selezionata, le dimensioni di archiviazione massime si limitano al valore definito. Per impostazione predefinita, la dimensione massima è di 1024 MB. Per evitare il superamento delle dimensioni di archiviazione massime, Kaspersky Endpoint Security elimina automaticamente i file più vecchi dall'archivio al raggiungimento delle dimensioni massime di archiviazione.

4. Salvare le modifiche.

Ripristino di file da Backup

Se in un file viene rilevato codice dannoso, Kaspersky Endpoint Security blocca il file, assegna al file lo stato *Non disinfettata*, ne salva una copia in Backup e tenta di disinfettarlo. Se la disinfezione viene completata, lo stato della copia di backup del file diventa *Disinfettato*. Il file diventa disponibile nella cartella originale. Se un file non può essere disinfettato, Kaspersky Endpoint Security lo elimina dalla cartella originale. È possibile ripristinare il file dalla copia di backup nella cartella originale.

I file con lo stato *Da eliminare al riavvio del computer* non possono essere ripristinati. Dopo il riavvio del computer, lo stato del file diventerà *Disinfettato* o *Eliminata*. È inoltre possibile ripristinare il file dalla copia di backup nella cartella originale.

Se viene rilevato codice dannoso in un file appartenente all'applicazione Windows Store, Kaspersky Endpoint Security elimina immediatamente il file senza spostare una copia del file in Backup. È possibile ripristinare l'integrità dell'applicazione Windows Store utilizzando gli strumenti appropriati del sistema operativo (per informazioni dettagliate su come ripristinare un'applicazione Windows Store, consultare i file della Guida di Microsoft Windows).

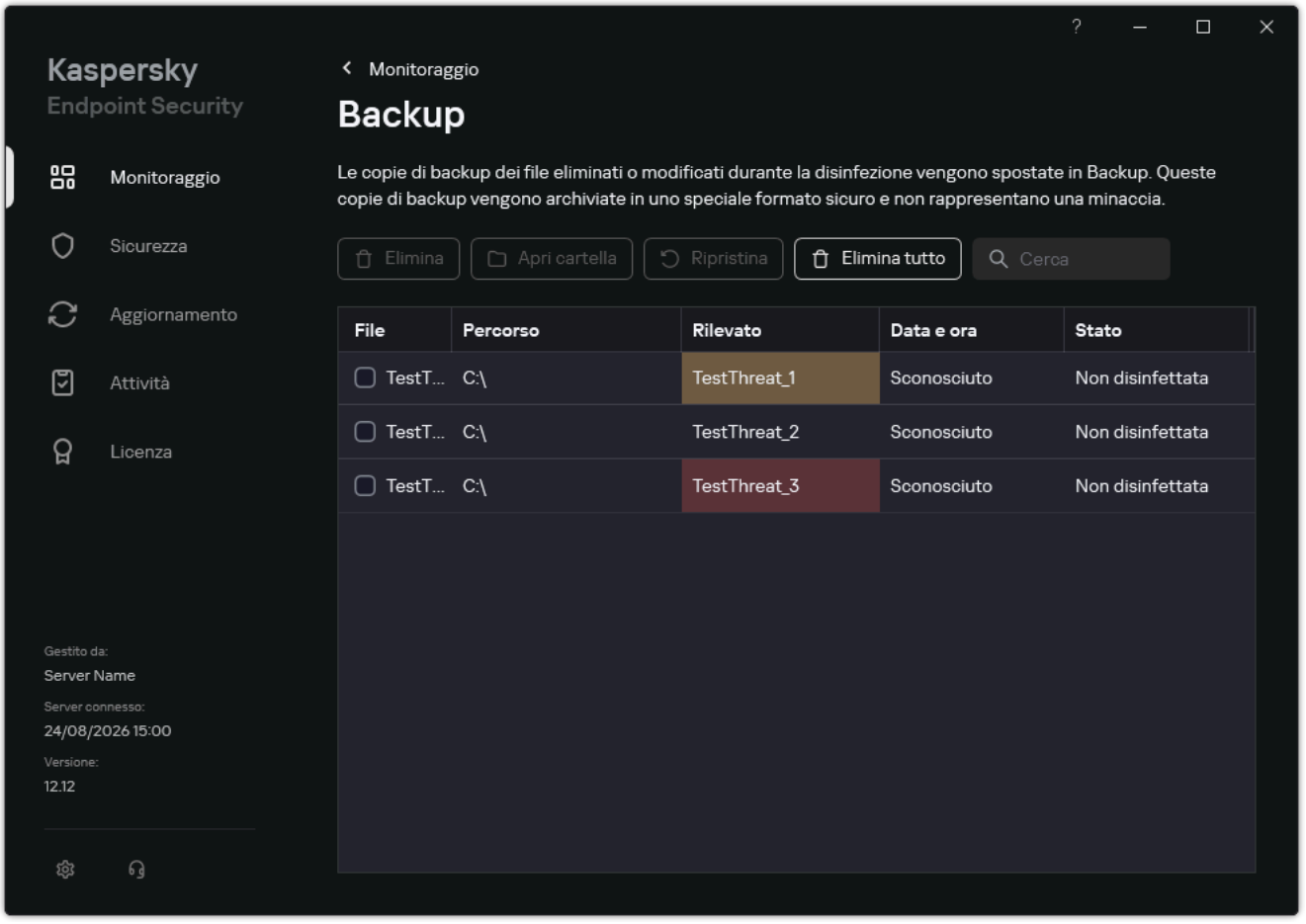
Il set di copie di backup dei file viene presentato sotto forma di tabella. Per la copia di backup di un file, viene visualizzato il percorso della cartella originale del file. Il percorso della cartella originale del file può contenere dati personali.

Se più file con nomi identici e contenuto diverso che si trovano nella stessa cartella vengono spostati in Backup, è possibile ripristinare solo il file che è stato inserito per ultimo in Backup.

Per ripristinare i file da Backup:

1. Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **Backup**.
2. Si apre l'elenco dei file in Backup; nell'elenco visualizzato, selezionare i file da ripristinare e fare clic su **Ripristina**.

I file verranno ripristinati nelle cartelle originali dalle copie di backup selezionate.



Backup

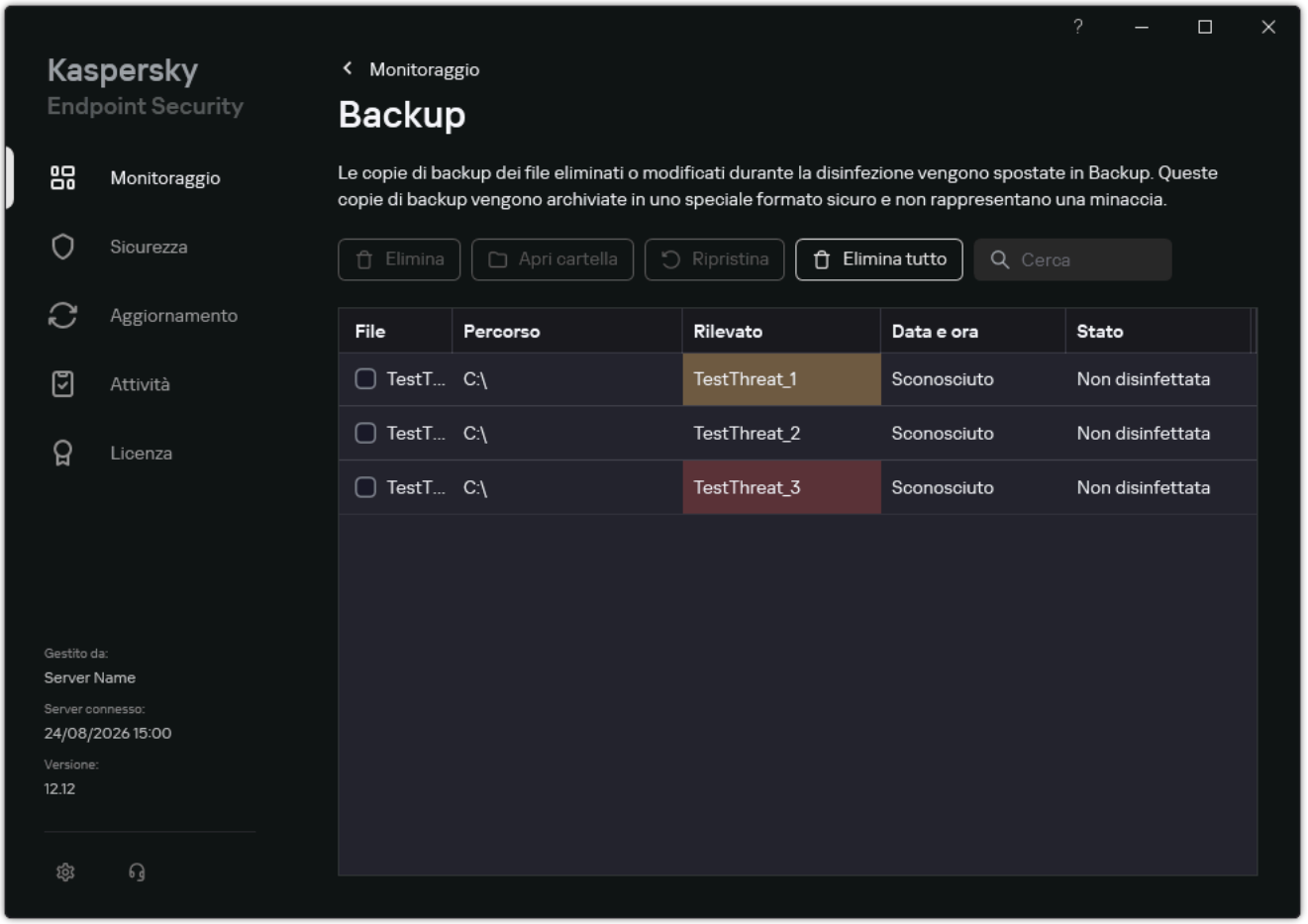
Eliminazione delle copie di backup dei file da Backup

Kaspersky Endpoint Security elimina automaticamente da Backup le copie di backup dei file con qualsiasi stato al termine del periodo di archiviazione configurato nelle impostazioni dell'applicazione. È anche possibile eliminare manualmente la copia di un file da Backup.

Per eliminare le copie di backup dei file da Backup:

1. Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **Backup**.
2. Si apre l'elenco dei file in Backup; nell'elenco visualizzato, selezionare i file da eliminare da Backup e fare clic su **Elimina**.

Kaspersky Endpoint Security eliminerà le copie di backup dei file selezionate da Backup.



Backup

Servizio di notifica

Durante l'esecuzione di Kaspersky Endpoint Security si verificano numerosi eventi. Le notifiche di questi eventi possono essere puramente informative o contenere informazioni critiche. Ad esempio, le notifiche possono segnalare il completamento di un aggiornamento dei database e dei moduli dell'applicazione o registrare errori dei componenti che devono essere corretti.

Kaspersky Endpoint Security supporta la registrazione delle informazioni sugli eventi nel registro delle applicazioni di Microsoft Windows e/o nel registro eventi di Kaspersky Endpoint Security.

Kaspersky Endpoint Security invia le notifiche nei seguenti modi:

- utilizzando messaggi a comparsa nell'area di notifica della barra delle applicazioni di Microsoft Windows;
- tramite e-mail.

È possibile configurare l'invio di notifiche sugli eventi. Il metodo di invio delle notifiche viene configurato per ogni tipo di evento.

Quando si utilizza la tabella degli eventi per configurare il servizio di notifica, è possibile eseguire le seguenti operazioni:

- Filtrare gli eventi del servizio di notifica in base ai valori delle colonne o alle condizioni di un filtro personalizzato.
- Utilizzare la funzione di ricerca degli eventi del servizio di notifica.
- Ordinare gli eventi del servizio di notifica.
- Modificare l'ordine e il set di colonne visualizzate nell'elenco degli eventi del servizio di notifica.

Configurazione delle impostazioni del registro eventi

Per configurare le impostazioni del registro eventi:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Interfaccia**.
3. Nel blocco **Notifiche**, fare clic sul pulsante **Configura notifiche**.

   I componenti e le attività di Kaspersky Endpoint Security sono visualizzati nella parte sinistra della finestra. Nella parte destra della finestra sono elencati gli eventi generati per l'attività o il componente selezionato.

   Gli eventi possono contenere i seguenti dati dell'utente:

   - Percorsi dei file esaminati da Kaspersky Endpoint Security.
   - Percorsi delle chiavi del Registro di sistema modificati durante l'esecuzione di Kaspersky Endpoint Security.
   - Nome utente di Microsoft Windows.
   - Indirizzi delle pagine Web aperte da parte dell'utente.

4. Nella parte sinistra della finestra selezionare il componente o l'attività per cui si desidera configurare le impostazioni del registro eventi.

5. Selezionare le caselle di controllo accanto agli eventi desiderati nelle colonne **Salva nel rapporto locale** e **Salva nel registro eventi di Windows**.

   Gli eventi per cui sono selezionate le caselle di controllo nella colonna **Salva nel rapporto locale** sono visualizzati nei registri dell'applicazione. Gli eventi per cui è selezionata la casella di controllo nella colonna **Salva nel registro eventi di Windows** sono visualizzati in Registri di Windows nel canale `Application`.

6. Salvare le modifiche.

Configurazione della visualizzazione e dell'invio delle notifiche

Per configurare la visualizzazione e l'invio delle notifiche:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Interfaccia**.

3. Nel blocco **Notifiche**, fare clic sul pulsante **Configura notifiche**.

   I componenti e le attività di Kaspersky Endpoint Security sono visualizzati nella parte sinistra della finestra. Nella parte destra della finestra sono elencati gli eventi generati per l'attività o il componente selezionato.

   Gli eventi possono contenere i seguenti dati dell'utente:

   - Percorsi dei file esaminati da Kaspersky Endpoint Security.
   - Percorsi delle chiavi del Registro di sistema modificati durante l'esecuzione di Kaspersky Endpoint Security.
   - Nome utente di Microsoft Windows.
   - Indirizzi delle pagine Web aperte da parte dell'utente.

4. Nella parte sinistra della finestra selezionare il componente o l'attività per cui si desidera configurare l'invio di notifiche.

5. Nella colonna **Notifica sullo schermo** selezionare le caselle di controllo accanto agli eventi pertinenti.

   Le informazioni sugli eventi selezionati vengono visualizzate tramite messaggi a comparsa nell'area di notifica della barra delle applicazioni di Microsoft Windows.

6. Nella colonna **Notifica tramite e-mail** selezionare le caselle di controllo accanto agli eventi pertinenti.

   Le informazioni sugli eventi selezionati vengono inviate tramite e-mail se sono configurate le impostazioni per l'invio delle notifiche tramite e-mail.

7. Fare clic su **OK**.

8. Se sono state abilitate le notifiche e-mail, configurare le impostazioni per l'invio dei messaggi e-mail:

   a. Fare clic su **Configura le notifiche via e-mail**.

   b. Selezionare la casella di controllo **Visualizza notifiche sugli eventi** per abilitare l'invio delle informazioni sugli eventi di Kaspersky Endpoint Security selezionati nella colonna **Notifica tramite e-mail**.

   c. Specificare le impostazioni per l'invio delle notifiche tramite e-mail.

   d. Fare clic su **OK**.

9. Salvare le modifiche.

Configurazione della visualizzazione degli avvisi sullo stato dell'applicazione nell'area di notifica

Per configurare la visualizzazione degli avvisi sullo stato dell'applicazione nell'area di notifica:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Interfaccia**.
3. Nel blocco **Mostra lo stato dell'applicazione nell'area di notifica**, selezionare le caselle di controllo accanto alle categorie di eventi per cui si desidera visualizzare le notifiche nell'area di notifica di Microsoft Windows.
4. Salvare le modifiche.

Quando si verificano eventi associati alle categorie selezionate, l'icona dell'applicazione nell'area di notifica cambia in o a seconda della gravità dell'avviso.

Invio di messaggi tra gli utenti e l'amministratore

I componenti Controllo Applicazioni, Controllo Dispositivi, Controllo Web e Controllo adattivo delle anomalie consentono agli utenti della rete LAN che utilizzano computer in cui è installato Kaspersky Endpoint Security di inviare messaggi all'amministratore.

Un utente può avere l'esigenza di inviare un messaggio all'amministratore della rete LAN nei seguenti casi:

- Controllo dispositivi ha bloccato l'accesso al dispositivo.

  Il modello del messaggio per una richiesta di accesso a un dispositivo bloccato è disponibile nell'interfaccia di Kaspersky Endpoint Security, nella sezione Controllo dispositivi.

- Controllo applicazioni ha bloccato l'avvio di un'applicazione.

  Il modello del messaggio per una richiesta di consenso dell'avvio di un'applicazione bloccata è disponibile nell'interfaccia di Kaspersky Endpoint Security, nella sezione Controllo applicazioni.

- Controllo Web ha bloccato l'accesso a una risorsa Web.

  Il modello del messaggio per una richiesta di accesso a una risorsa Web bloccata è disponibile nell'interfaccia di Kaspersky Endpoint Security, nella sezione Controllo Web.

Il metodo utilizzato per inviare i messaggi e la scelta del modello dipendono dal fatto che sia in esecuzione o meno un criterio attivo di Kaspersky Security Center nel computer in cui è installato Kaspersky Endpoint Security e che sia presente o meno una connessione con Kaspersky Security Center Administration Server. Gli scenari possibili sono i seguenti:

- Se nel computer in cui è installato Kaspersky Security Center non è in esecuzione un criterio di Kaspersky Endpoint Security, il messaggio di un utente viene inviato all'amministratore della rete locale tramite e-mail.

  Nel campo del messaggio vengono inseriti i valori dei campi del modello definito nell'interfaccia locale di Kaspersky Endpoint Security.

- Se nel computer in cui è installato Kaspersky Security Center è in esecuzione un criterio di Kaspersky Endpoint Security, viene inviato il messaggio standard a Kaspersky Security Center Administration Server.

  In questo caso, i messaggi dell'utente sono disponibili per la visualizzazione nell'archivio di eventi di Kaspersky Security Center (vedere le istruzioni di seguito). Nel campo del messaggio vengono inseriti i valori dei campi del modello definito nel criterio di Kaspersky Security Center.

- Se nel computer in cui è installato Kaspersky Endpoint Security è in esecuzione un criterio fuori sede di Kaspersky Security Center, il metodo utilizzato per inviare i messaggi dipende dal fatto che sia presente o meno una connessione con Kaspersky Security Center.

  - Se viene stabilita una connessione con Kaspersky Security Center, Kaspersky Endpoint Security invia il messaggio standard a Kaspersky Security Center Administration Server.

  - Se la connessione con Kaspersky Security Center è assente, il messaggio dell'utente viene inviato all'amministratore della rete locale tramite e-mail.

  In entrambi casi, nel campo del messaggio vengono inseriti i valori dei campi del modello definito nel criterio di Kaspersky Security Center.

Per visualizzare il messaggio di un utente nell'archivio di eventi di Kaspersky Security Center:

1. Aprire Kaspersky Security Center Administration Console.

2. Nel nodo **Administration Server** della struttura di Administration Console selezionare la scheda **Eventi**.

   L'area di lavoro di Kaspersky Security Center visualizza tutti gli eventi che si verificano durante l'esecuzione di Kaspersky Endpoint Security, inclusi i messaggi per l'amministratore ricevuti dagli utenti della rete LAN.

3. Per configurare il filtro per gli eventi, nell'elenco a discesa **Selezioni eventi**, selezionare **Richieste utente**.

4. Selezionare il messaggio inviato all'amministratore.

5. Fare clic sul pulsante **Apri la finestra delle proprietà dell'evento** nella parte destra dell'area di lavoro di Administration Console.

Gestione dei rapporti

Nei rapporti vengono registrate informazioni sull'esecuzione di ciascun componente di Kaspersky Endpoint Security, sugli eventi di criptaggio dei dati, sulle prestazioni di ogni attività di scansione, attività di aggiornamento e attività di Controllo integrità, nonché sull'esecuzione complessiva dell'applicazione.

I rapporti vengono archiviati nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.

I rapporti possono contenere i seguenti dati dell'utente:

- Percorsi dei file esaminati da Kaspersky Endpoint Security.
- Percorsi delle chiavi del Registro di sistema modificati durante l'esecuzione di Kaspersky Endpoint Security.
- Nome utente di Microsoft Windows.
- Indirizzi delle pagine Web aperte da parte dell'utente.

I dati nel rapporto sono presentati sotto forma di tabella. Ogni riga della tabella contiene informazioni su un evento distinto. Gli attributi degli eventi sono riportati nelle colonne della tabella. Alcune colonne sono composite, ovvero contengono colonne nidificate con ulteriori attributi. Per visualizzare gli attributi aggiuntivi, è necessario fare clic sul pulsante ⊞ accanto al nome della colonna. Gli eventi registrati durante l'esecuzione dei vari componenti o di varie attività hanno diversi set di attributi.

Sono disponibili i seguenti rapporti:

- Rapporto **Audit sistema**. Contiene informazioni sugli eventi che si verificano durante l'interazione tra l'utente e l'applicazione e nel corso dell'esecuzione dell'applicazione in generale, senza essere correlati a un particolare componente o attività di Kaspersky Endpoint Security.
- Rapporti sul funzionamento dei componenti di Kaspersky Endpoint Security.
- Rapporti sulle attività di Kaspersky Endpoint Security.
- Rapporto **Criptaggio dei dati**. Contiene informazioni sugli eventi che si verificano durante il criptaggio e il decriptaggio dei dati.

Nei rapporti vengono utilizzati i seguenti livelli di importanza degli eventi:

ⓘ **Messaggi informativi**. Eventi di riferimento che in genere non contengono informazioni importanti.

⚠ **Avvisi**. Eventi a cui è necessario prestare attenzione perché riflettono situazioni importanti nel funzionamento di Kaspersky Endpoint Security.

⓿ **Eventi critici**. Eventi di importanza critica che indicano problemi nel funzionamento di Kaspersky Endpoint Security o vulnerabilità nella protezione del computer dell'utente.

Per agevolare l'elaborazione dei rapporti, è possibile modificare la presentazione dei dati sullo schermo nei seguenti modi:

- Filtrare l'elenco degli eventi in base a vari criteri.
- Utilizzare la funzione di ricerca per trovare uno specifico evento.
- Visualizzare l'evento selezionato in una sezione distinta.
- Ordinare l'elenco degli eventi in base a ciascuna colonna del rapporto.
- Visualizzare e nascondere eventi raggruppati in base al filtro per gli eventi utilizzando il pulsante ⊞.
- Modificare l'ordine e la disposizione delle colonne visualizzate nel rapporto.

Se necessario, è possibile salvare il rapporto generato in un file di testo. È inoltre possibile eliminare le informazioni dei rapporti per componenti e attività di Kaspersky Endpoint Security combinati in gruppi.

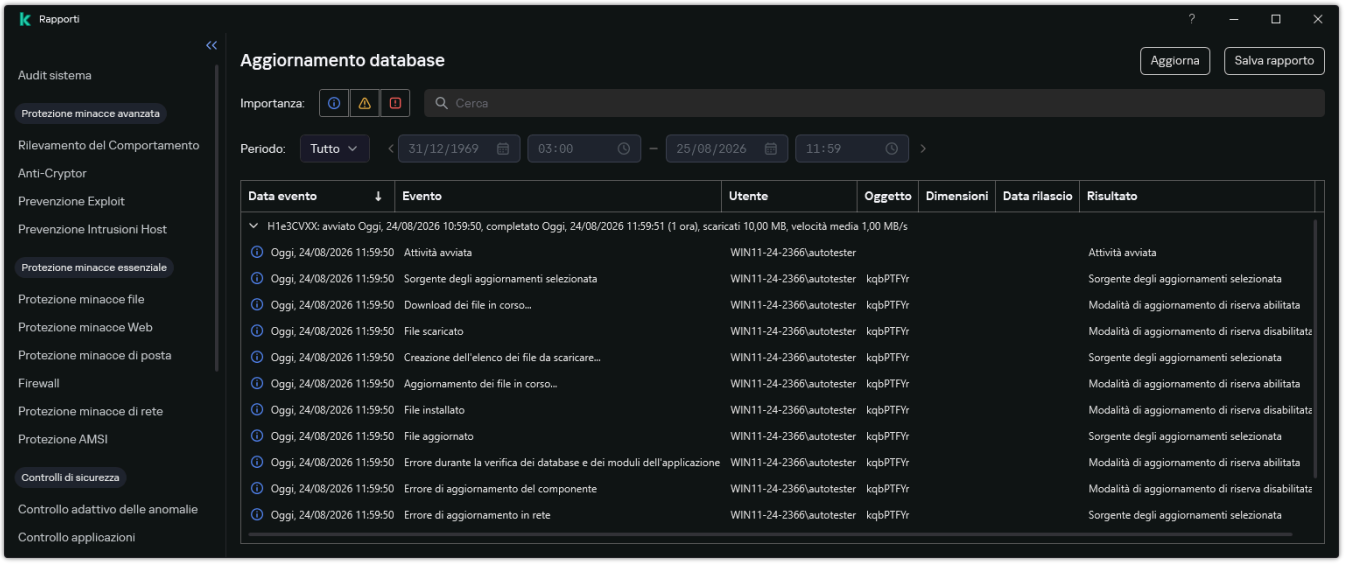
Se Kaspersky Endpoint Security è in esecuzione nell'ambito della gestione di Kaspersky Security Center, le informazioni sugli eventi possono essere trasmesse a Kaspersky Security Center Administration Server (per ulteriori dettagli, consultare la Guida di Kaspersky Security Center).

Visualizzazione dei rapporti

Se un utente può visualizzare i rapporti, l'utente può visualizzare anche tutti gli eventi presenti nei rapporti.

Per visualizzare i rapporti:

1. Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **Rapporti**.



Rapporti

2. Nell'elenco dei componenti e delle attività, selezionare un componente o un'attività.

   La parte destra della finestra visualizza un rapporto contenente un elenco degli eventi causati dall'esecuzione del componente selezionato o dell'attività selezionata di Kaspersky Endpoint Security. È possibile ordinare gli eventi nel rapporto in base ai valori nelle celle di una delle colonne.

3. Per visualizzare informazioni dettagliate su un evento, selezionare l'evento nel rapporto.

Un blocco con il riepilogo dell'evento viene visualizzato nella parte inferiore della finestra.

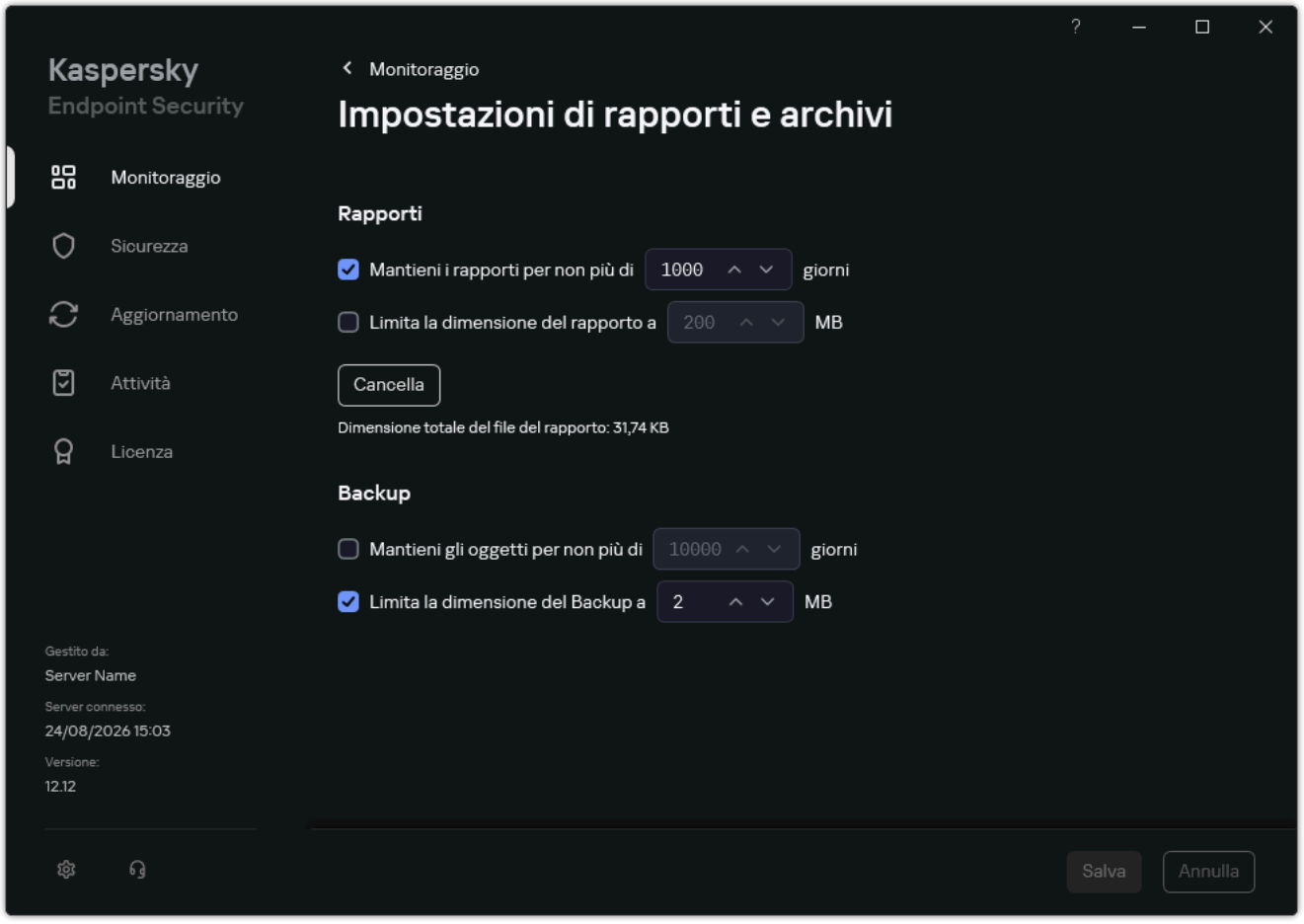
Configurazione del periodo massimo di archiviazione dei rapporti

Per impostazione predefinita, il periodo massimo di archiviazione dei rapporti sugli eventi registrati da Kaspersky Endpoint Security è di 30 giorni. Al termine di tale periodo di tempo, Kaspersky Endpoint Security elimina automaticamente le voci meno recenti dal file del rapporto.

Per modificare il periodo massimo di archiviazione dei rapporti:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, in **Impostazioni generali**, fare clic sul riquadro **Rapporti e archivi**.



Impostazioni rapporto

3. Se si desidera limitare il periodo di archiviazione dei rapporti, selezionare la casella di controllo **Mantieni i rapporti per non più di N giorni** nella sezione **Rapporti**. Definire il periodo massimo di archiviazione dei rapporti.

4. Salvare le modifiche.

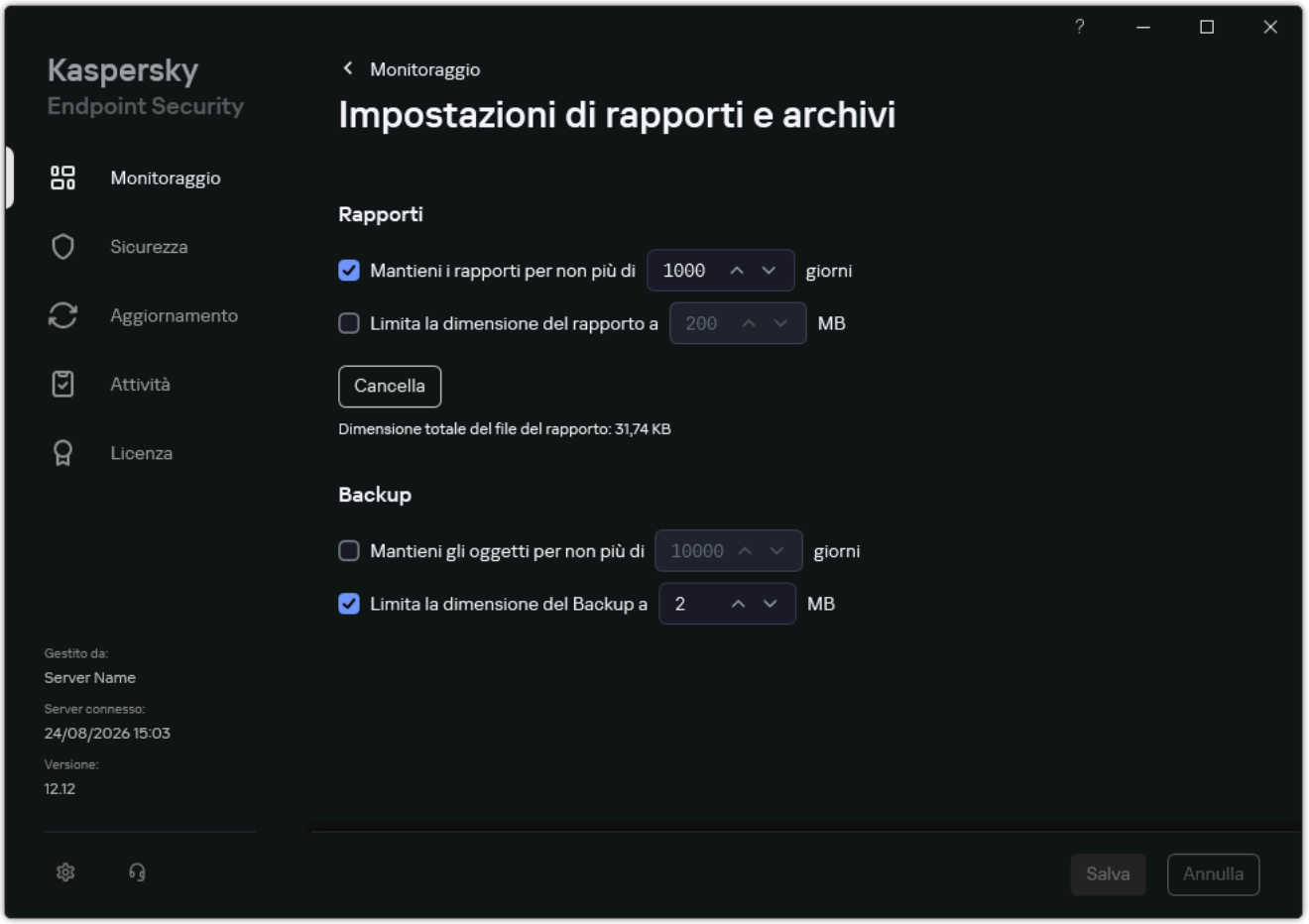
Configurazione della dimensione massima dei file del rapporto

È possibile specificare la dimensione massima dei file che contiene il rapporto. Per impostazione predefinita, la dimensione massima dei file del rapporto è di 1024 MB. Per evitare il superamento della dimensione massima dei file del rapporto, Kaspersky Endpoint Security elimina automaticamente le voci meno recenti dal file del rapporto quando viene raggiunta la dimensione massima dei file.

Per configurare la dimensione massima dei file dei rapporti:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, in **Impostazioni generali**, fare clic sul riquadro **Rapporti e archivi**.



Impostazioni rapporto

3. Nella sezione **Rapporti**, selezionare la casella di controllo **Limita la dimensione del rapporto a N MB** se si desidera limitare la dimensione di un file del rapporto. Definire la dimensione massima dei file del rapporto.

4. Salvare le modifiche.

Salvataggio di un rapporto in un file

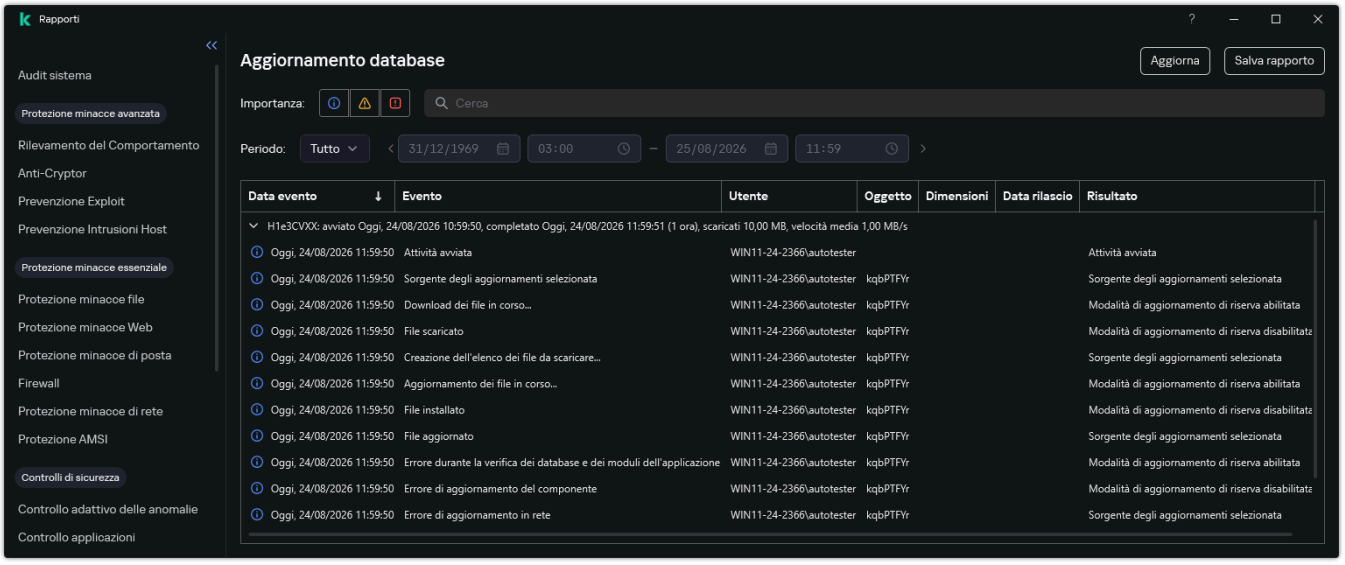
L'utente è personalmente responsabile della sicurezza delle informazioni di un rapporto salvato in un file e soprattuto del controllo e della limitazione dell'accesso a tali informazioni.

È possibile salvare il rapporto generato in un file in formato testo (TXT) o in un file CSV.

Kaspersky Endpoint Security registra gli eventi nel rapporto nello stesso modo in cui vengono visualizzati sullo schermo (con lo stesso set e la stessa sequenza di attributi evento).

Per salvare un rapporto in un file:

1. Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **Rapporti**.



Rapporti

2. Si apre una finestra; in questa finestra, selezionare il componente o l'attività.

   Nella parte destra della finestra viene visualizzato un rapporto, che contiene un elenco degli eventi che si sono verificati durante l'esecuzione del componente o dell'attività di Kaspersky Endpoint Security.

3. Se necessario, è possibile modificare la presentazione dai dati nel rapporto nei seguenti modi:

   - Filtrando gli eventi
   - Eseguendo la ricerca di un evento
   - Riorganizzando le colonne
   - Ordinando gli eventi

4. Fare clic sul pulsante **Salva rapporto** nella parte superiore destra della finestra.

5. Nella finestra visualizzata specificare la cartella di destinazione per il file del rapporto.

6. Immettere il nome del file del rapporto.

7. Selezionare il formato file del rapporto necessario: TXT o CSV.

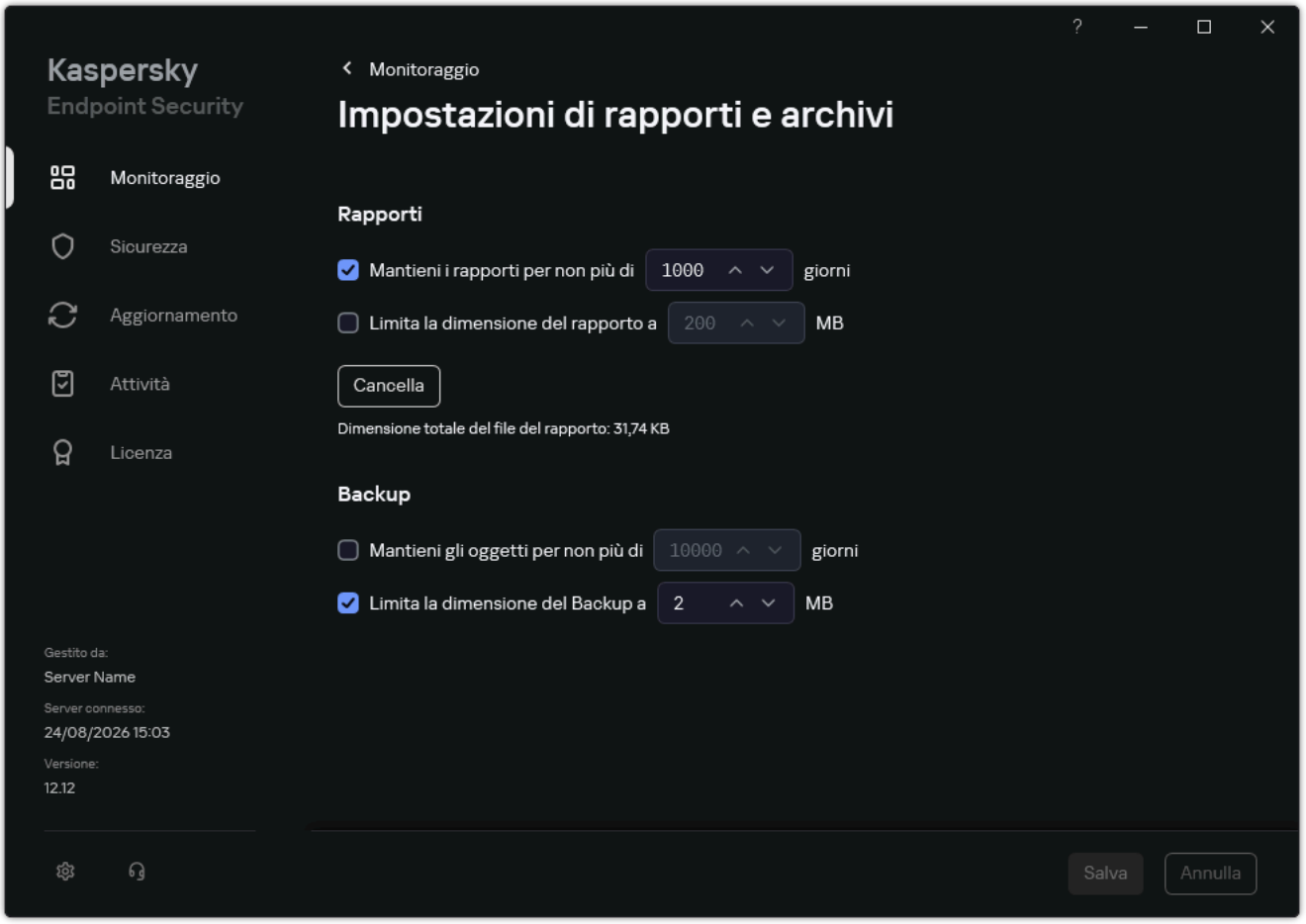
8. Salvare le modifiche.

Eliminazione dei rapporti

Per rimuovere le informazioni dai rapporti:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, in **Impostazioni generali**, fare clic sul riquadro **Rapporti e archivi**.



Impostazioni rapporto

3. Nel blocco **Rapporti**, fare clic sul pulsante **Cancella**.

4. Se la protezione tramite password è abilitata, Kaspersky Endpoint Security potrebbe richiedere le credenziali dell'account utente. L'applicazione richiede le credenziali dell'account se l'utente non dispone dell'autorizzazione necessaria.

Kaspersky Endpoint Security eliminerà tutti i rapporti per tutti i componenti e le attività dell'applicazione.

Auto-difesa di Kaspersky Endpoint Security

Auto-difesa impedisce ad altre applicazioni di eseguire azioni che possono interferire con il funzionamento di Kaspersky Endpoint Security e, ad esempio, rimuovere Kaspersky Endpoint Security dal computer. Il set di tecnologie di Auto-difesa disponibili per Kaspersky Endpoint Security varia in base al fatto che il sistema operativo sia a 32 bit o a 64 bit (consultare la tabella sottostante). Auto-difesa include anche la protezione tramite password e la protezione della connessione di Administration Server.

Protezione tramite password consente di limitare l'accesso degli utenti a Kaspersky Endpoint Security in base alle autorizzazioni concesse (ad esempio l'autorizzazione per la chiusura dell'applicazione).

Protezione della connessione ad Administration Server impedisce la riconnessione non autorizzata del computer a un server non attendibile.

Tecnologie Auto-difesa di Kaspersky Endpoint Security

Tecnologia	Descrizione	Computer x86	Computer x64
Meccanismo di Auto-difesa	La tecnologia blocca l'accesso ai seguenti componenti applicativi: • file nella cartella di installazione di Kaspersky Endpoint Security e altri file dell'applicazione; • chiavi del Registro di sistema con i record appartenenti all'applicazione; • processi eseguiti dall'applicazione.	✓	✓
AM-PPL (Antimalware Protected Process Light)	La tecnologia protegge i processi di Kaspersky Endpoint Security da azioni dannose. Per ulteriori informazioni sulla tecnologia AM-PPL, visitare il sito Web Microsoft. La tecnologia AM-PPL è disponibile per i sistemi operativi Windows 10 versione 1703 (RS2) o successiva e Windows Server 2019.	✓	✓
Meccanismo di difesa gestione esterna	Questa tecnologia impedisce alle altre applicazioni, ad esempio TeamViewer o RemotelyAnywhere, di accedere a Kaspersky Endpoint Security.	✓	– (ad eccezione di Windows 7)

Abilitazione e disabilitazione di Auto-difesa

Kaspersky Endpoint Security impedisce la modifica o l'eliminazione dei file dell'applicazione sul disco rigido, dei processi in memoria e delle voci del Registro di sistema.

La tecnologia blocca l'accesso ai seguenti componenti applicativi:

- file nella cartella di installazione di Kaspersky Endpoint Security e altri file dell'applicazione;
- chiavi del Registro di sistema con i record appartenenti all'applicazione;
- processi eseguiti dall'applicazione.

I meccanismi di autodifesa non si applicano ai processi di Kaspersky Endpoint Security avviati da processi padre non attendibili.

Il meccanismo Auto-Difesa di Kaspersky Endpoint Security è abilitato per impostazione predefinita.

Come abilitare o disabilitare Auto-difesa in Administration Console (MMC)

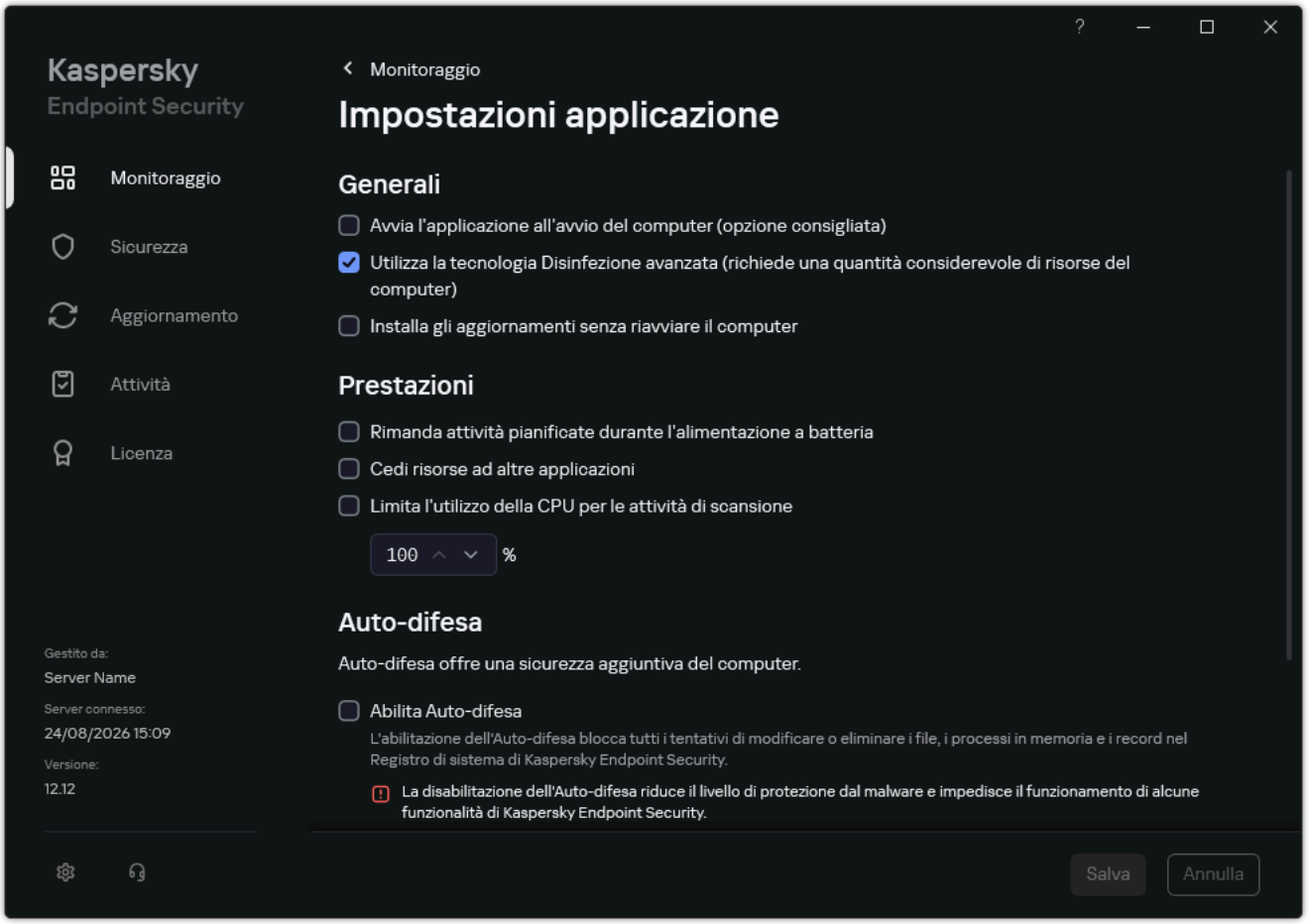
1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
4. Utilizzare la casella di controllo **Abilita Auto-difesa** per abilitare o disabilitare il meccanismo Auto-difesa.
5. Salvare le modifiche.

Come abilitare o disabilitare Auto-difesa in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Auto-difesa**.
5. Utilizzare l'interruttore **Auto-difesa ABILITATO** per abilitare o disabilitare il meccanismo Auto-difesa.
6. Salvare le modifiche.

Come abilitare o disabilitare Auto-difesa nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.



Impostazioni di Kaspersky Endpoint Security for Windows

3. Utilizzare la casella di controllo **Abilita Auto-difesa** per abilitare o disabilitare il meccanismo Auto-difesa.
4. Salvare le modifiche.

Abilitazione e disabilitazione del supporto AM-PPL

Kaspersky Endpoint Security supporta la tecnologia Antimalware Protected Process Light (di seguito denominata "AM-PPL") di Microsoft. AM-PPL protegge i processi di Kaspersky Endpoint Security dalle azioni dannose (ad esempio la chiusura dell'applicazione). AM-PPL consente esclusivamente l'esecuzione dei processi attendibili. I processi di Kaspersky Endpoint Security sono attendibili in quanto firmati in conformità con i requisiti di sicurezza Windows. Per ulteriori informazioni sulla tecnologia AM-PPL, visitare il sito Web Microsoft. La tecnologia AM-PPL è abilitata per impostazione predefinita.

Kaspersky Endpoint Security presenta inoltre meccanismi integrati per la protezione dei processi dell'applicazione. Il supporto AM-PPL consente di delegare le funzioni di sicurezza dei processi al sistema operativo. È quindi possibile aumentare la velocità dell'applicazione e ridurre il consumo di risorse del computer.

Utilizzare continuamente la tecnologia AM-PPL. AM-PPL è un componente importante della protezione del sistema operativo. La disabilitazione del supporto di AM-PPL può causare la mancata riuscita di alcune funzionalità di Kaspersky Endpoint Security (ad esempio l'integrazione dell'applicazione con Windows Security Center). La disabilitazione del supporto di AM-PPL è consentita solo in un ambiente di test separato a scopo di risoluzione dei problemi.

La tecnologia AM-PPL è disponibile per i sistemi operativi Windows 10 versione 1703 (RS2) o successiva e Windows Server 2019.

Per abilitare o disabilitare la tecnologia AM-PPL:

1. Disattivare il meccanismo di Auto-difesa dell'applicazione.

   Il meccanismo di Auto-difesa impedisce la modifica e l'eliminazione dei processi dell'applicazione nella memoria del computer, inclusa la modifica dello stato AM-PPL.

2. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.

3. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

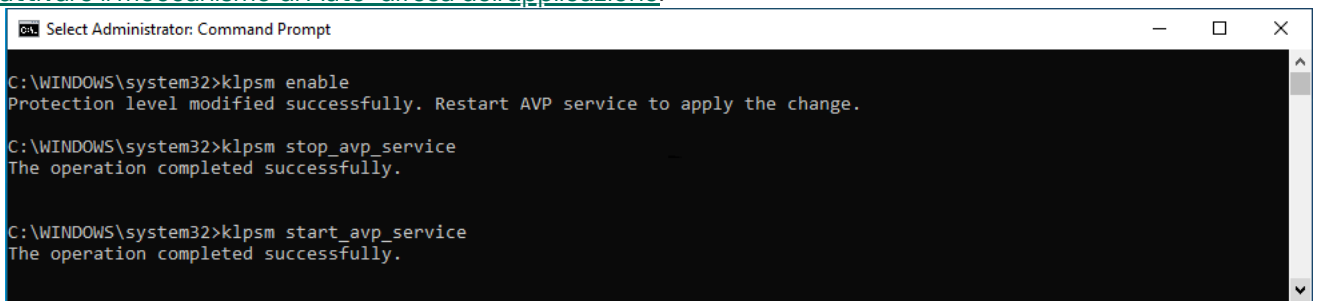
   È possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% durante l'installazione dell'applicazione.

4. Digitare quanto segue nella riga di comando:

   - `klpsm.exe enable` - consente di abilitare il supporto della tecnologia AM-PPL (vedere la figura seguente).
   - `klpsm.exe disable` - consente di disabilitare il supporto della tecnologia AM-PPL.

5. Riavviare Kaspersky Endpoint Security.

6. Riattivare il meccanismo di Auto-difesa dell'applicazione.



Abilitazione del supporto della tecnologia AM-PPL

Protezione dei servizi applicativi contro la gestione esterna

La protezione dei servizi applicativi contro la gestione esterna blocca i tentativi degli utenti e di altre applicazioni di arrestare i servizi di Kaspersky Endpoint Security. La protezione assicura il funzionamento dei seguenti servizi:

- Kaspersky Endpoint Security Service (AVP.KES.14.2)
- Servizio Kaspersky Seamless Update Service (AVPSUS.KES.14.2)

Per chiudere l'applicazione dalla riga di comando, disabilitare la protezione dei servizi di Kaspersky Endpoint Security dalla gestione esterna.

È possibile consentire la gestione esterna dei servizi applicativi solo nei computer che non supportano la tecnologia AM-PPL o nei computer in cui la tecnologia è disabilitata.

Come abilitare o disabilitare la protezione dei servizi applicativi con la gestione esterna in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
4. Utilizzare la casella di controllo **Blocca gestione esterna dei servizi applicativi** per abilitare o disabilitare la protezione dei servizi di Kaspersky Endpoint Security dalla gestione esterna.
5. Salvare le modifiche.

Come abilitare o disabilitare la protezione dei servizi applicativi con la gestione esterna in Web Console e Cloud Console

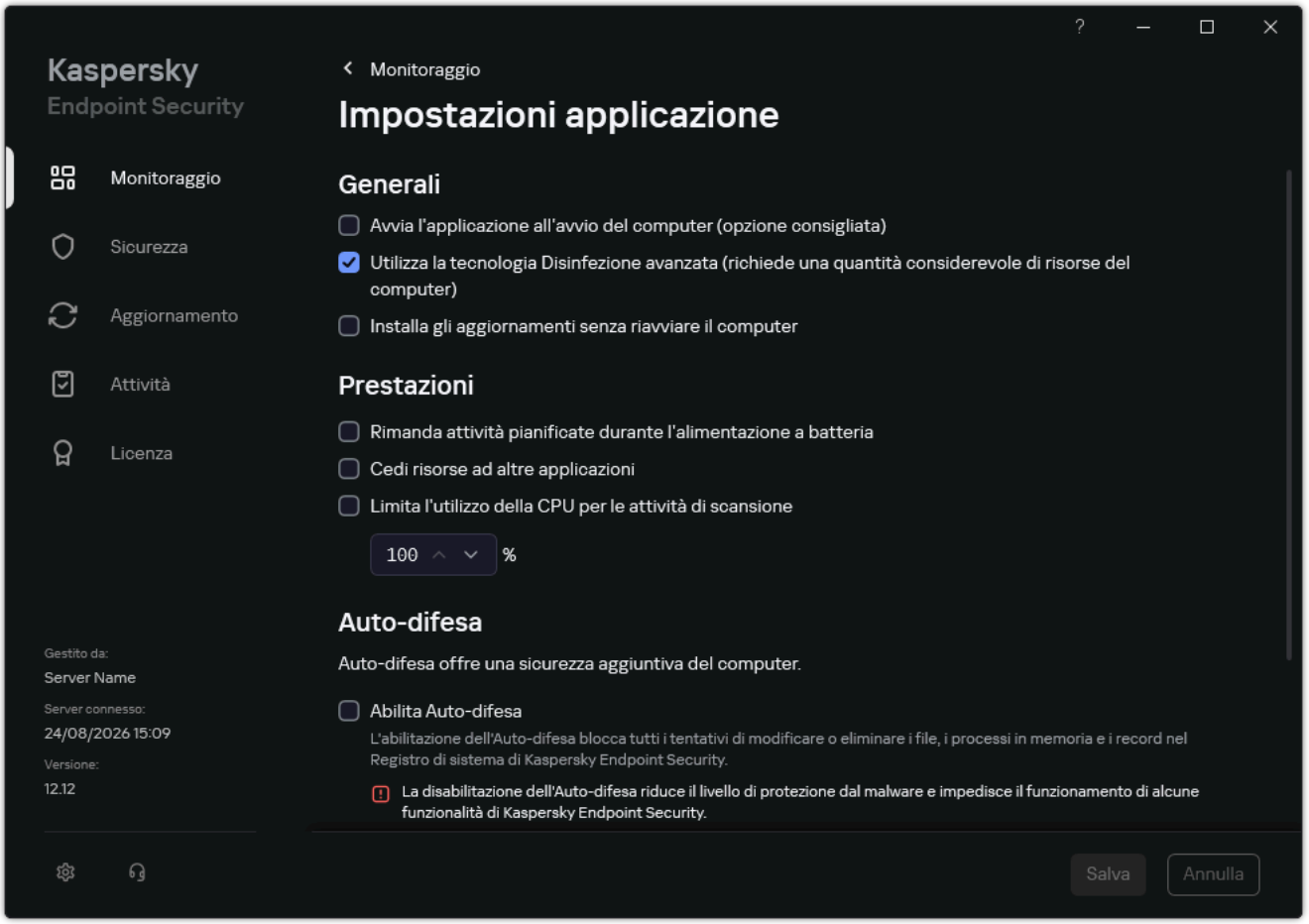
1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Auto-difesa**.
5. Utilizzare la casella di controllo **Blocca gestione esterna dei servizi applicativi** per abilitare o disabilitare la protezione dei servizi di Kaspersky Endpoint Security dalla gestione esterna.
6. Salvare le modifiche.

Come abilitare o disabilitare la protezione dei servizi applicativi con la gestione esterna nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.

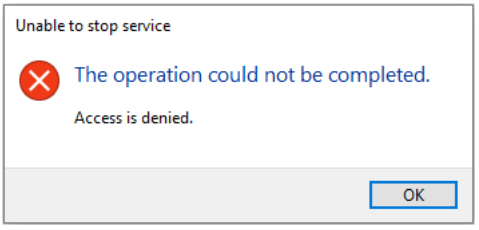


Impostazioni di Kaspersky Endpoint Security for Windows

3. Utilizzare la casella di controllo **Blocca gestione esterna dei servizi applicativi** per abilitare o disabilitare la protezione dei servizi di Kaspersky Endpoint Security dalla gestione esterna.

4. Salvare le modifiche.

Di conseguenza, quando un utente tenta di arrestare i servizi applicativi, viene visualizzata una finestra di sistema con un messaggio di errore. L'utente può gestire i servizi applicativi solo dall'interfaccia di Kaspersky Endpoint Security.



Errore di accesso ai servizi applicativi

Supporto delle applicazioni di amministrazione remota

Talvolta può essere necessario utilizzare un'applicazione di amministrazione remota mentre la difesa gestione esterna è abilitata.

Per consentire l'esecuzione di applicazioni di amministrazione remota:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti rilevati**.
3. Nella sezione **Esclusioni**, fare clic sul collegamento **Specifica applicazioni attendibili**.
4. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.
5. Selezionare il file eseguibile dell'applicazione di amministrazione remota.

   È inoltre possibile immettere il percorso manualmente. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.
6. Selezionare la casella di controllo **Consenti interazione con l'interfaccia di Kaspersky Endpoint Security**.
7. Salvare le modifiche.

Protezione tramite password

Più utenti con diversi livelli di esperienza possono condividere un computer. Se gli utenti dispongono di un accesso senza limitazioni a Kaspersky Endpoint Security e alle relative impostazioni, il livello complessivo di protezione del computer può risultare inferiore. Protezione tramite password consente di limitare l'accesso degli utenti a Kaspersky Endpoint Security in base alle autorizzazioni concesse (ad esempio l'autorizzazione per la chiusura dell'applicazione).

Se l'utente che ha avviato la sessione di Windows (*utente della sessione*) dispone dell'autorizzazione per eseguire l'azione, Kaspersky Endpoint Security non richiede il nome utente e la password o una password temporanea. L'utente riceve l'accesso a Kaspersky Endpoint Security in base alle autorizzazioni concesse.

Se un utente della sessione non dispone dell'autorizzazione per eseguire un'azione, l'utente può ottenere l'accesso all'applicazione nei seguenti modi:

- Inserire nome utente e password.

  Questo metodo è adatto per le operazioni quotidiane. Per eseguire un'azione protetta da password, è necessario immettere le credenziali dell'account di dominio dell'utente con l'autorizzazione richiesta. In questo caso, il computer deve trovarsi in tale dominio. Se il computer non si trova nel dominio, è possibile utilizzare l'account KLAdmin o un account aggiunto manualmente.

- Immettere una password provvisoria.

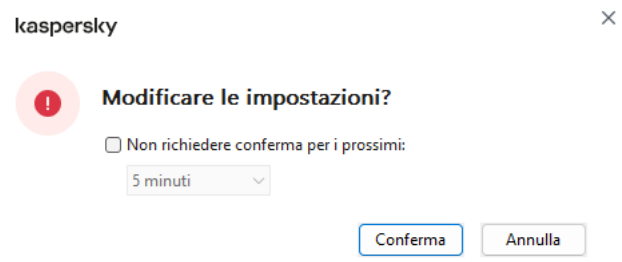
  Questo metodo è adatto per concedere autorizzazioni provvisorie per l'esecuzione di azioni bloccate (ad esempio la chiusura dell'applicazione) agli utenti esterni alla rete aziendale. Allo scadere di una password provvisoria o al termine di una sessione, Kaspersky Endpoint Security ripristina le relative impostazioni allo stato precedente.

- Token.

  Questo metodo è adatto agli utenti con privilegi, ad esempio il personale dell'Assistenza tecnica. L'autenticazione tramite token consente di utilizzare la modalità di accesso con smart card in Active Directory. Ciò migliora la sicurezza dell'infrastruttura dell'organizzazione.

Quando un utente tenta di eseguire un'azione protetta da password, Kaspersky Endpoint Security richiede all'utente nome utente e password, la password del token oppure una password temporanea (vedere la figura di seguito).

Nella finestra di immissione della password, è possibile cambiare la lingua: a tale scopo, è sufficiente premere **ALT+MAIUSC**. L'utilizzo di altri collegamenti, anche se configurati nel sistema operativo, non funziona per il cambio di lingua.



Richiesta della password di accesso a Kaspersky Endpoint Security

Nome utente e password

Per accedere a Kaspersky Endpoint Security, è necessario immettere le credenziali dell'account. Protezione tramite password supporta i seguenti account:

- **KLAdmin**. Account amministratore con accesso illimitato a Kaspersky Endpoint Security. L'account KLAdmin ha il diritto di eseguire qualsiasi azione protetta da password. Le autorizzazioni per l'account KLAdmin non possono essere revocate. Quando si abilita la protezione tramite password, Kaspersky Endpoint Security richiede di impostare una password per l'account KLAdmin.

- **Account aggiunto manualmente**. Un account esterno al dominio Active Directory. È possibile utilizzare questo account di servizio anziché KLAdmin se non si desidera condividere la password dell'amministratore. È possibile impostare qualsiasi nome utente e password e configurare autorizzazioni individuali.

- **Gruppo Everyone**. Gruppo di Windows integrato che include tutti gli utenti della rete aziendale. Gli utenti del gruppo Everyone possono accedere all'applicazione in base alle autorizzazioni concesse.

- **Singoli utenti o gruppi**. Account utente per cui è possibile configurare autorizzazioni individuali. Se ad esempio un'azione è bloccata per il gruppo Everyone, è possibile consentire tale azione per un singolo utente o gruppo.
- **Utente della sessione**. Account dell'utente che ha avviato la sessione Windows. È possibile passare a un altro utente della sessione quando viene richiesta la password (casella di controllo **Salva la password per la sessione corrente**). In questo caso Kaspersky Endpoint Security considera l'utente per cui sono state immesse le credenziali dell'account come utente della sessione anziché come utente che ha avviato la sessione di Windows.

Password provvisoria

È possibile utilizzare una password provvisoria per concedere l'accesso provvisorio a Kaspersky Endpoint Security per un singolo computer all'esterno della rete aziendale. L'amministratore genera una password provvisoria per un singolo computer nelle proprietà del computer in Kaspersky Security Center. L'amministratore seleziona le azioni che saranno protette dalla password provvisoria e specifica il periodo di validità della password provvisoria.

Token

Per accedere alle funzionalità di Kaspersky Endpoint Security, è necessario selezionare il certificato utente appropriato dall'elenco dei certificati archiviati nel token connesso e immettere il PIN. L'autenticazione tramite token è disponibile solo per gli utenti del dominio Active Directory. L'amministratore può configurare le autorizzazioni per un singolo utente o un gruppo. Per il corretto funzionamento dell'autenticazione tramite token, è necessario distribuire un'infrastruttura PKI attendibile e installare un software specifico per la gestione del token.

Abilitazione della protezione tramite password

Protezione tramite password consente di limitare l'accesso degli utenti a Kaspersky Endpoint Security in base alle autorizzazioni concesse (ad esempio l'autorizzazione per la chiusura dell'applicazione).

Come abilitare Protezione tramite password in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Interfaccia**.
4. Nel blocco **Protezione tramite password**, fare clic sul pulsante **Impostazioni**.

   Viene aperta una finestra con le impostazioni di Protezione tramite password.
5. Utilizzare la casella di controllo **Abilita protezione tramite password** per abilitare o disabilitare il componente.
6. In **Autorizzazioni** selezionare l'account KLAdmin.

7. Viene aperta una finestra; in quella finestra, fare clic su **Password** e impostare una password per l'account KLAdmin.

   L'account KLAdmin ha il diritto di eseguire qualsiasi azione protetta da password.

   > Se si dimentica la password dell'account KLAdmin, è possibile reimpostarla nelle proprietà dei criteri.

8. Tornare all'elenco degli account.

9. Impostare le autorizzazioni per tutti gli utenti nella rete aziendale:

   a. In **Autorizzazioni** selezionare il gruppo "Tutti".

      Il gruppo *Everyone* è un gruppo Windows integrato che include tutti gli utenti della rete aziendale.

   b. Nella finestra visualizzata selezionare le caselle di controllo accanto alle azioni che gli utenti potranno eseguire senza immettere la password.

      Se una casella di controllo è deselezionata, l'esecuzione dell'azione da parte degli utenti viene bloccata. Se ad esempio la casella di controllo accanto all'autorizzazione **Chiudi l'applicazione** è deselezionata, è possibile chiudere l'applicazione solo se è stato eseguito l'accesso come KLAdmin o come un singolo utente con l'autorizzazione richiesta oppure se si immette una password provvisoria.

      > Le autorizzazioni di protezione tramite password hanno alcuni aspetti importanti da tenere in considerazione. Verificare che tutte le condizioni per l'accesso a Kaspersky Endpoint Security siano soddisfatte.

10. Salvare le modifiche.

Come abilitare Protezione tramite password in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Auto-difesa**.

5. In **Protezione tramite password** utilizzare l'interruttore **Protezione tramite password ABILITATA** per abilitare o disabilitare il componente.

6. Specificare la password per l'account KLAdmin e confermarla.

   L'account KLAdmin ha il diritto di eseguire qualsiasi azione protetta da password.

   > Se si dimentica la password dell'account KLAdmin, è possibile reimpostarla nelle proprietà dei criteri.

7. Tornare all'elenco degli account.

8. Impostare le autorizzazioni per tutti gli utenti nella rete aziendale:

   a. Nella tabella degli account selezionare il gruppo "Tutti".

      Il gruppo *Everyone* è un gruppo Windows integrato che include tutti gli utenti della rete aziendale.

   b. Nella finestra visualizzata selezionare le caselle di controllo accanto alle azioni che gli utenti potranno eseguire senza immettere la password.

      Se una casella di controllo è deselezionata, l'esecuzione dell'azione da parte degli utenti viene bloccata. Se ad esempio la casella di controllo accanto all'autorizzazione **Chiudi l'applicazione** è deselezionata, è possibile chiudere l'applicazione solo se è stato eseguito l'accesso come KLAdmin o come un singolo utente con l'autorizzazione richiesta oppure se si immette una password provvisoria.

      Le autorizzazioni di protezione tramite password hanno alcuni aspetti importanti da tenere in considerazione. Verificare che tutte le condizioni per l'accesso a Kaspersky Endpoint Security siano soddisfatte.

9. Salvare le modifiche.

Come abilitare Protezione tramite password nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Interfaccia**.
3. Utilizzare l'interruttore **Protezione tramite password** per abilitare o disabilitare il componente.
4. Specificare la password per l'account KLAdmin e confermarla.

   L'account KLAdmin ha il diritto di eseguire qualsiasi azione protetta da password.

   Se un computer viene eseguito con un criterio, l'Amministratore può reimpostare la password per l'account KLAdmin nelle proprietà del criterio. Se il computer non è connesso a Kaspersky Security Center e si dimentica la password per l'account KLAdmin, non è possibile recuperare la password.

5. Impostare le autorizzazioni per tutti gli utenti nella rete aziendale:

   a. Nella tabella dell'account, fare clic su **Modifica** per aprire l'elenco delle autorizzazioni per il gruppo Everyone.

      Il gruppo *Everyone* è un gruppo Windows integrato che include tutti gli utenti della rete aziendale.

   b. Selezionare le caselle di controllo accanto alle azioni che gli utenti potranno eseguire senza immettere la password.

      Se una casella di controllo è deselezionata, l'esecuzione dell'azione da parte degli utenti viene bloccata. Se ad esempio la casella di controllo accanto all'autorizzazione **Chiudi l'applicazione** è deselezionata, è possibile chiudere l'applicazione solo se è stato eseguito l'accesso come KLAdmin o come un singolo utente con l'autorizzazione richiesta oppure se si immette una password provvisoria.

      Le autorizzazioni di protezione tramite password hanno alcuni aspetti importanti da tenere in considerazione. Verificare che tutte le condizioni per l'accesso a Kaspersky Endpoint Security siano soddisfatte.

6. Salvare le modifiche.

Quando la protezione tramite password è abilitata, l'applicazione limiterà l'accesso degli utenti a Kaspersky Endpoint Security in base alle autorizzazioni concesse al gruppo Everyone. È possibile eseguire le azioni bloccate per il gruppo Everyone solo se si utilizza l'account KLAdmin, un altro account a cui sono concesse le autorizzazioni richieste o se si immette una password provvisoria.

È possibile disabilitare Protezione tramite password solo se è stato eseguito l'accesso come KLAdmin. Non è possibile disabilitare la protezione tramite password se si utilizza un altro account utente o una password temporanea.

Durante il controllo della password è possibile selezionare la casella di controllo **Salva la password per la sessione corrente**. In questo caso Kaspersky Endpoint Security non richiederà una password quando un utente tenta di eseguire un'altra azione protetta da password per tutta la durata della sessione.

Concessione delle autorizzazioni a singoli utenti o gruppi

La protezione tramite password consente di concedere a Kaspersky Endpoint Security l'accesso a singoli account utente di Active Directory e ad account utente aggiunti manualmente.

Account utente di Active Directory

È possibile concedere a Kaspersky Endpoint Security l'accesso a singoli utenti o gruppi all'interno del dominio Active Directory. Se ad esempio la chiusura dell'applicazione è bloccata per il gruppo Everyone, è possibile concedere l'autorizzazione **Chiudi l'applicazione**. In seguito a questa operazione, è possibile chiudere l'applicazione solo se è stato eseguito l'accesso come tale utente o KLAdmin.

È possibile utilizzare le credenziali dell'account per accedere all'applicazione solo se il computer si trova nel dominio. Se il computer non si trova nel dominio, è possibile utilizzare l'account KLAdmin o una password temporanea.

Account utente aggiunti manualmente

È possibile creare un account utente non presente in Active Directory e assegnare autorizzazioni individuali a tale account utente. In altre parole, è possibile creare un *account utente di servizio* e utilizzarlo al posto di KLAdmin. In questo modo, non è necessario condividere la password di KLAdmin con altri utenti o creare nuovi account utente di Active Directory. È possibile specificare qualsiasi nome utente e password. Ad esempio, è possibile concedere l'autorizzazione **Visualizza rapporti** all'account utente di servizio. Di conseguenza, se la visualizzazione dei rapporti è vietata al gruppo "Tutti", è possibile aprire i rapporti utilizzando l'account utente di servizio o l'account utente di KLAdmin.

Concessione delle autorizzazioni a singoli utenti o gruppi

Come concedere autorizzazioni a singoli utenti o gruppi in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Interfaccia**.
4. Nel blocco **Protezione tramite password**, fare clic sul pulsante **Impostazioni**.

   Viene aperta una finestra con le impostazioni di Protezione tramite password.
5. Nella tabella dell'account, fare clic su **Aggiungi**.
6. Selezionare il tipo di account utente che si desidera aggiungere:

   - **Seleziona un utente/gruppo da Active Directory** - Account utente di Active Directory.

     Per selezionare un account utente, fare clic su **Seleziona**. Selezionare un utente o un gruppo in Active Directory e confermare la selezione.

   - **Aggiungi un utente/gruppo di utenti manualmente** per un account utente del servizio aggiunto manualmente.

     Per aggiungere un account utente di servizio, immettere un nome utente e una password (ad esempio, SecureAdmin).

     È possibile reimpostare la password di un account utente del servizio nelle impostazioni dei criteri. La password dell'account utente del servizio deve essere reimpostata allo stesso modo della password di KLAdmin. Se la modifica delle impostazioni di Protezione tramite password è consentita (il "lucchetto" è aperto) o non è applicato alcun criterio al computer, è possibile reimpostare la password dell'account utente del servizio nell'interfaccia dell'applicazione. A tale scopo, confermare le modifiche delle informazioni dell'account utente del servizio utilizzando la password di KLAdmin.
7. Nell'elenco **Autorizzazioni** selezionare le caselle di controllo accanto alle azioni che l'utente o il gruppo selezionato potrà eseguire senza dover specificare una password.

   Se una casella di controllo è deselezionata, l'esecuzione dell'azione da parte degli utenti viene bloccata. Se ad esempio la casella di controllo accanto all'autorizzazione **Chiudi l'applicazione** è deselezionata, è possibile chiudere l'applicazione solo se è stato eseguito l'accesso come KLAdmin o come un singolo utente con l'autorizzazione richiesta oppure se si immette una password provvisoria.

   Le autorizzazioni di protezione tramite password hanno alcuni aspetti importanti da tenere in considerazione. Verificare che tutte le condizioni per l'accesso a Kaspersky Endpoint Security siano soddisfatte.
8. Salvare le modifiche.

Come concedere autorizzazioni a singoli utenti o gruppi in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Auto-difesa**.
5. Nella sezione **Protezione tramite password**, fare clic sul collegamento **Autorizzazioni utente**.

   Verrà aperto il modulo per la concessione delle autorizzazioni di abilitazione della password.
6. Fare clic su **Aggiungi**.
7. Selezionare il tipo di account utente che si desidera aggiungere:

   - **Selezionare da Active Directory** - Account utente di Active Directory.

     Per selezionare un account utente, fare clic su **Modifica**. Selezionare un utente o un gruppo in Active Directory e confermare la selezione.
   - **Aggiungi manualmente** per un account utente del servizio aggiunto manualmente.

     Per aggiungere un account utente di servizio, immettere un nome utente e una password (ad esempio, SecureAdmin).

     È possibile reimpostare la password di un account utente del servizio nelle impostazioni dei criteri. La password dell'account utente del servizio deve essere reimpostata allo stesso modo della password di KLAdmin. Se la modifica delle impostazioni di Protezione tramite password è consentita (il "lucchetto" è aperto) o non è applicato alcun criterio al computer, è possibile reimpostare la password dell'account utente del servizio nell'interfaccia dell'applicazione. A tale scopo, confermare le modifiche delle informazioni dell'account utente del servizio utilizzando la password di KLAdmin.
8. Nell'elenco **Autorizzazioni** selezionare le caselle di controllo accanto alle azioni che l'utente o il gruppo selezionato potrà eseguire senza dover specificare una password.

   Se una casella di controllo è deselezionata, l'esecuzione dell'azione da parte degli utenti viene bloccata. Se ad esempio la casella di controllo accanto all'autorizzazione **Chiudi l'applicazione** è deselezionata, è possibile chiudere l'applicazione solo se è stato eseguito l'accesso come KLAdmin o come un singolo utente con l'autorizzazione richiesta oppure se si immette una password provvisoria.

   Le autorizzazioni di protezione tramite password hanno alcuni aspetti importanti da tenere in considerazione. Verificare che tutte le condizioni per l'accesso a Kaspersky Endpoint Security siano soddisfatte.
9. Fare clic su **Aggiungi**.
10. Salvare le modifiche.

Come concedere autorizzazioni a singoli utenti o gruppi nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Interfaccia**.
3. Nella tabella dell'account, fare clic su **Aggiungi**.
4. Selezionare il tipo di account utente che si desidera aggiungere:
   - **Seleziona un utente/gruppo da Active Directory** - Account utente di Active Directory.

     Per selezionare un account utente, fare clic su **Seleziona utente o gruppo**. Selezionare un utente o un gruppo in Active Directory e confermare la selezione.
   - **Aggiungi un utente manualmente** per un account utente del servizio aggiunto manualmente.

     Per aggiungere un account utente di servizio, immettere un nome utente e una password (ad esempio, SecureAdmin).

     > È possibile reimpostare la password di un account utente del servizio nelle impostazioni dei criteri. La password dell'account utente del servizio deve essere reimpostata allo stesso modo della password di KLAdmin. Se la modifica delle impostazioni di Protezione tramite password è consentita (il "lucchetto" è aperto) o non è applicato alcun criterio al computer, è possibile reimpostare la password dell'account utente del servizio nell'interfaccia dell'applicazione. A tale scopo, confermare le modifiche delle informazioni dell'account utente del servizio utilizzando la password di KLAdmin.
5. Nell'elenco **Autorizzazioni** selezionare le caselle di controllo accanto alle azioni che l'utente o il gruppo selezionato potrà eseguire senza dover specificare una password.

   Se una casella di controllo è deselezionata, l'esecuzione dell'azione da parte degli utenti viene bloccata. Se ad esempio la casella di controllo accanto all'autorizzazione **Chiudi l'applicazione** è deselezionata, è possibile chiudere l'applicazione solo se è stato eseguito l'accesso come KLAdmin o come un singolo utente con l'autorizzazione richiesta oppure se si immette una password provvisoria.

   > Le autorizzazioni di protezione tramite password hanno alcuni aspetti importanti da tenere in considerazione. Verificare che tutte le condizioni per l'accesso a Kaspersky Endpoint Security siano soddisfatte.
6. Salvare le modifiche.

Di conseguenza, se l'accesso all'applicazione è limitato per il gruppo Everyone, agli utenti verranno concesse le autorizzazioni per l'accesso a Kaspersky Endpoint Security in base alle singole autorizzazioni dell'utente.

Utilizzo di una password provvisoria per concedere le autorizzazioni

È possibile utilizzare una password provvisoria per concedere l'accesso provvisorio a Kaspersky Endpoint Security per un singolo computer all'esterno della rete aziendale. Questo è necessario per consentire all'utente di eseguire un'azione bloccata senza ottenere le credenziali dell'account KLAdmin. Per utilizzare una password provvisoria, il computer deve essere aggiunto a Kaspersky Security Center.

Come consentire a un utente di eseguire un'azione bloccata utilizzando una password provvisoria tramite Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, aprire la cartella con il nome del gruppo di amministrazione a cui appartengono i computer client desiderati.
3. Nell'area di lavoro, selezionare la scheda **Dispositivi**.
4. Fare doppio clic per aprire la finestra delle proprietà del computer.
5. Nella finestra delle proprietà del computer, selezionare la sezione **Applicazioni**.
6. Nell'elenco delle applicazioni Kaspersky installate nel computer selezionare **Kaspersky Endpoint Security for Windows (14.2)** e fare doppio clic per aprire le proprietà dell'applicazione.
7. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali → Interfaccia**.
8. Nel blocco **Protezione tramite password**, fare clic sul pulsante **Impostazioni**.
9. Nella finestra visualizzata, nel blocco **Password provvisoria**, fare clic sul pulsante **Elenco delle password provvisorie**.

   Verrà visualizzata la finestra Gestione delle password provvisorie.
10. Fare clic su **Aggiungi**.
11. Nel campo **Data di scadenza** specificare la data di scadenza della password provvisoria.
12. Nella tabella **Ambito della password provvisoria** selezionare le caselle di controllo accanto alle azioni che saranno disponibili per l'utente dopo l'immissione della password provvisoria.
13. Fare clic su **Genera**.

    Verrà visualizzata una finestra contenente la password provvisoria (vedere la figura seguente).
14. Copiare la password e fornirla all'utente.

Come consentire a un utente di eseguire un'azione bloccata utilizzando una password provvisoria tramite Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Risorse (dispositivi)**.
2. Fare clic sul nome del computer sul quale si desidera consentire a un utente di eseguire un'azione bloccata.
3. Selezionare la scheda **Applicazioni**.
4. Fare clic su **Kaspersky Endpoint Security for Windows**.

   Verranno visualizzate le impostazioni locali dell'applicazione.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali → Interfaccia**.
7. Nel blocco **Password provvisorie**, fare clic sul pulsante **Aggiungi**.

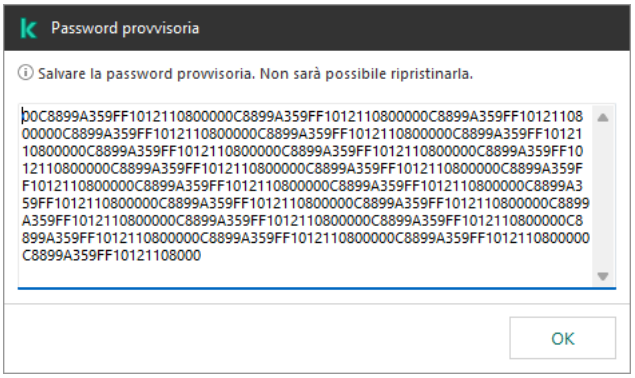
8. Nel campo **Data di scadenza** specificare la data di scadenza della password provvisoria.

9. Nella tabella **Ambito della password provvisoria** selezionare le caselle di controllo accanto alle azioni che saranno disponibili per l'utente dopo l'immissione della password provvisoria.

10. Fare clic su **Genera**.

    Viene visualizzata una finestra contenente la password provvisoria.

11. Copiare la password e fornirla all'utente.



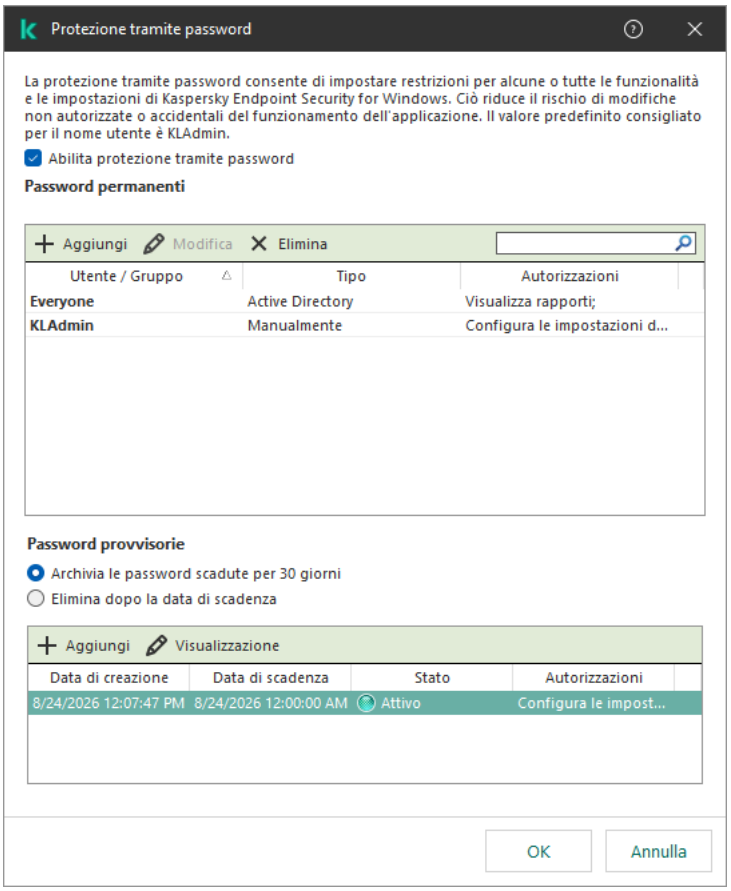
Password provvisoria

Revoca delle password provvisorie

A partire dalla versione 12.9, Kaspersky Endpoint Security for Windows include la funzionalità *Gestione delle password provvisorie*. La gestione delle password provvisorie consente di eseguire le seguenti azioni:

- Salvare la cronologia delle password (fino a 30 giorni).
- Monitorare lo stato delle password provvisorie: *Attivo*, *Scaduto*, *Revocato*.

- Revocare le password provvisorie.



Gestione delle password provvisorie

La gestione delle password provvisorie aggiorna lo stato della password e revoca la password solo dopo la sincronizzazione del computer con Kaspersky Security Center.

Come revocare una password provvisoria utilizzando Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, aprire la cartella con il nome del gruppo di amministrazione a cui appartengono i computer client desiderati.
3. Nell'area di lavoro, selezionare la scheda **Dispositivi**.
4. Fare doppio clic per aprire la finestra delle proprietà del computer.
5. Nella finestra delle proprietà del computer, selezionare la sezione **Applicazioni**.
6. Nell'elenco delle applicazioni Kaspersky installate nel computer selezionare **Kaspersky Endpoint Security for Windows (14.2)** e fare doppio clic per aprire le proprietà dell'applicazione.
7. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Interfaccia**.
8. Nel blocco **Protezione tramite password**, fare clic sul pulsante **Impostazioni**.
9. Questo apre una finestra; in tale finestra sotto **Password provvisoria**, configurare le impostazioni di archiviazione per le password scadute.

10. Fare clic su **Elenco delle password provvisorie**.

    Verrà visualizzata la finestra Gestione delle password provvisorie. Gestione delle password provvisorie consente di visualizzare la data di scadenza della password, lo stato della password e l'elenco delle autorizzazioni.

11. Selezionare la password provvisoria attiva che si desidera revocare e fare doppio clic sulla password per aprirne le proprietà.

12. Nella finestra visualizzata, fare clic sul pulsante **Revoca**.

13. Salvare le modifiche. Per applicare il criterio nei computer, chiudere i lucchetti .

Come revocare la password provvisoria in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Risorse (dispositivi)**.

2. Fare clic sul nome del computer sul quale si desidera consentire a un utente di eseguire un'azione bloccata.

3. Selezionare la scheda **Applicazioni**.

4. Fare clic su **Kaspersky Endpoint Security for Windows**.

    Verranno visualizzate le impostazioni locali dell'applicazione.

5. Selezionare la scheda **Impostazioni applicazione**.

6. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali → Interfaccia**.

7. In **Password provvisorie**, configurare l'archiviazione delle password scadute.

8. Fare clic sul collegamento **Password provvisoria**.

    Verrà visualizzata la finestra Gestione delle password provvisorie. Gestione delle password provvisorie consente di visualizzare la data di scadenza della password, lo stato della password e l'elenco delle autorizzazioni.

9. Selezionare la password provvisoria attiva che si desidera revocare.

10. Nella finestra visualizzata, fare clic sul pulsante **Revoca password**.

11. Salvare le modifiche. Per applicare il criterio nei computer, chiudere i lucchetti .

Di conseguenza, Gestione delle password provvisorie imposta lo stato della password su *Revoca in corso (sincronizzazione con un host)*. Dopo la sincronizzazione del computer con Kaspersky Security Center, l'applicazione revoca la password provvisoria e blocca immediatamente le autorizzazioni concesse.

Caratteristiche speciali delle autorizzazioni di Protezione tramite password

Le autorizzazioni di protezione tramite password hanno alcuni aspetti e limitazioni importanti da tenere in considerazione.

Configura le impostazioni dell'applicazione

Se il computer di un utente è in esecuzione con un criterio, verificare che tutte le impostazioni necessarie nel criterio siano disponibili per la modifica (gli attributi sono aperti).

Chiudi l'applicazione

Non sono presenti considerazioni o limitazioni speciali.

Disabilita componenti della protezione

- Non è possibile concedere l'autorizzazione per disabilitare i componenti della protezione per il gruppo Tutti. Per consentire agli utenti al di fuori di KL Admin di disabilitare i componenti di controllo, aggiungere un utente o un gruppo con l'autorizzazione **Disabilita componenti della protezione** nelle impostazioni di Protezione tramite password.
- Se il computer di un utente è in esecuzione con un criterio, verificare che tutte le impostazioni necessarie nel criterio siano disponibili per la modifica (gli attributi sono aperti).
- Per disabilitare i componenti della protezione nelle impostazioni dell'applicazione, un utente deve disporre dell'autorizzazione **Configura le impostazioni dell'applicazione**.
- Per disabilitare i componenti della protezione dal menu di scelta rapida (utilizzando la voce del menu **Sospendi la protezione**), un utente deve disporre dell'autorizzazione **Disabilita componenti della protezione** oltre all'autorizzazione **Disabilita componenti di controllo**.

Disabilita componenti di controllo

- Non è possibile concedere l'autorizzazione per disabilitare i componenti di controllo per il gruppo Tutti. Per consentire agli utenti al di fuori di KL Admin di disabilitare i componenti di controllo, aggiungere un utente o un gruppo con l'autorizzazione **Disabilita componenti di controllo** nelle impostazioni di Protezione tramite password.
- Se il computer di un utente è in esecuzione con un criterio, verificare che tutte le impostazioni necessarie nel criterio siano disponibili per la modifica (gli attributi sono aperti).
- Per disabilitare i componenti di controllo nelle impostazioni dell'applicazione, un utente deve disporre dell'autorizzazione **Configura le impostazioni dell'applicazione**.
- Per disabilitare i componenti di controllo dal menu di scelta rapida (utilizzando la voce del menu **Sospendi la protezione**), un utente deve disporre dell'autorizzazione **Disabilita componenti di controllo** oltre all'autorizzazione **Disabilita componenti della protezione**.

Disabilita il criterio di Kaspersky Security Center

Non è possibile concedere al gruppo "Tutti" l'autorizzazione per disabilitare i criteri di Kaspersky Security Center. Per consentire agli utenti al di fuori di KLAdmin di disabilitare il criterio, aggiungere un utente o un gruppo con l'autorizzazione **Disabilita il criterio di Kaspersky Security Center** nelle impostazioni di protezione tramite password.

Rimuovi chiave

Non sono presenti considerazioni o limitazioni speciali.

Rimuovi/modifica/ripristina l'applicazione

Se la rimozione, la modifica e il ripristino dell'applicazione per il gruppo "Tutti" sono state consentiti, Kaspersky Endpoint Security non richiede una password quando l'utente tenta di eseguire queste operazioni. Pertanto, qualsiasi utente, inclusi gli utenti esterni al dominio, può installare, modificare o ripristinare l'applicazione.

Ripristina l'accesso ai dati nell'unità criptata

È possibile ripristinare l'accesso ai dati sulle unità criptate solo se è stato eseguito l'accesso come KLAdmin. L'autorizzazione per l'esecuzione di questa azione non può essere concessa a nessun altro utente.

Visualizza rapporti

Non sono presenti considerazioni o limitazioni speciali.

Ripristina da Backup

Non sono presenti considerazioni o limitazioni speciali.

Esporta impostazioni

Per impostazione predefinita, l'esportazione delle impostazioni dell'applicazione è negata al gruppo "Tutti". È possibile esportare le impostazioni dell'applicazione utilizzando l'account utente KLAdmin. L'esportazione delle impostazioni dell'applicazione include solo la creazione di un file di configurazione con le impostazioni di Kaspersky Endpoint Security nell'interfaccia dell'applicazione. L'autorizzazione non limita l'esportazione di elenchi di esclusioni dalla scansione, indirizzi Web attendibili, dispositivi attendibili o altri elenchi gestiti dai componenti dell'applicazione.

Reimpostazione della password KLAdmin

Se si dimentica la password dell'account KLAdmin, è possibile reimpostarla nelle proprietà dei criteri. Non è possibile reimpostare la password nell'interfaccia dell'applicazione.

È possibile eseguire azioni protette da password utilizzando una password provvisoria. In questo caso, non è necessario immettere le credenziali di KLAdmin.

Se il computer non è connesso a Kaspersky Security Center e si dimentica la password per l'account KLAdmin, non è possibile recuperare la password.

Come reimpostare la password dell'account KLAdmin utilizzando Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Interfaccia**.
4. Nel blocco **Protezione tramite password**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, deselezionare la casella di controllo **Abilita protezione tramite password**.
6. Salvare le modifiche.
7. Selezionare di nuovo la casella di controllo **Abilita protezione tramite password**.
8. Fare clic su **OK**.
   Viene verrà visualizzata la finestra Password amministratore.
9. Specificare la nuova password dell'account KLAdmin e confermarla.
10. Salvare le modifiche.

Come reimpostare la password dell'account KLAdmin in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Selezionare il computer per cui si desidera configurare le impostazioni locali dell'applicazione.
   Verranno visualizzate le proprietà del computer.
3. Selezionare la scheda **Applicazioni**.
4. Fare clic su **Kaspersky Endpoint Security for Windows 14.2**.
   Verranno visualizzate le impostazioni locali dell'applicazione.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Passare a **Impostazioni generali** → **Auto-difesa**.

7. In **Protezione tramite password**, disattivare l'interruttore **Protezione tramite password**.
8. Salvare le modifiche.
9. Riattivare l'interruttore **Protezione tramite password**.
10. Specificare la nuova password dell'account KLAdmin e confermarla.
11. Salvare le modifiche.

Di conseguenza, la password dell'account KLAdmin viene aggiornata dopo l'applicazione del criterio.

Protezione della connessione ad Administration Server

La connessione del computer ad Administration Server viene effettuata utilizzando il componente *Network Agent* di Kaspersky Security Center. Se un intruso dispone di diritti sufficienti per modificare le impostazioni di connessione del server, esiste il rischio che il computer venga connesso a un server non attendibile. In questo modo, si consente all'intruso di applicare i propri criteri di gruppo e, ad esempio, disabilitare l'autodifesa dell'applicazione. Kaspersky Endpoint Security può impedire la riconnessione non autorizzata di un computer a un server diverso. Per proteggere la connessione al server, l'applicazione suggerisce di impostare una password e di utilizzare la funzione Password-Based key Derivation Function (PBKDF2). Di conseguenza, l'accesso all'applicazione senza password è impossibile.

Per garantire la protezione completa di Kaspersky Endpoint Security e Network Agent da accessi non autorizzati, si consiglia di abilitare una protezione aggiuntiva. Per Kaspersky Endpoint Security, si consiglia di abilitare Protezione tramite password. Per proteggere Network Agent, si consiglia di impostare una password di disinstallazione. Per informazioni sulla protezione di Network Agent dalla rimozione, consultare la Guida di Kaspersky Security Center.

La gestione della connessione del computer ad Administration Server viene effettuata utilizzando l'attività *Protezione della connessione ad Administration Server*. L'attività consente di eseguire le seguenti azioni:

- Impostare una password per proteggere la connessione al server.
- Modificare la password.
- Riconnettere il computer a un server diverso.
- Disabilitare la protezione della connessione al server.

Autenticazione del computer durante la connessione ad Administration Server

Dopo aver impostato una password, l'applicazione crea un array di dati utilizzando la trasformazione PBKDF2 della password. L'applicazione cripta quindi questo array di dati utilizzando la chiave di Network Agent. L'applicazione utilizza l'array di dati criptati per verificare i diritti e i privilegi di Administration Server per le connessioni successive.

Successivamente, ogni volta che si tenta di riconnettere il computer ad Administration Server, l'applicazione decripta l'array di dati con la chiave di Network Agent e lo confronta con la copia locale. Se non corrispondono, l'accesso all'applicazione è limitato.

Protezione della connessione ad Administration Server

Come impostare una password per la protezione della connessione al server in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Protezione della connessione ad Administration Server**.

Passaggio 2. Protezione della connessione ad Administration Server

Impostare una password per proteggere la connessione ad Administration Server:

1. In **Protezione della connessione ad Administration Server**, selezionare **Proteggi con una password**.

2. Nell'elenco a discesa **Administration Server**, selezionare **Nuovo server**.

3. Nel campo **Password per la connessione ad Administration Server**, impostare una password per la connessione ad Administration Server e confermarla.

   Se si dimentica la password, è possibile modificarla utilizzando un'attività.

4. Se è distribuito Kaspersky Endpoint Security 12.7 o una versione precedente dell'applicazione, selezionare la casella di controllo **Abilita la compatibilità del criptaggio della password per le versioni precedenti dell'applicazione (12.7 e precedenti)**.

   A partire da Kaspersky Endpoint Security 12.8 for Windows, l'applicazione utilizza un criptaggio delle password più avanzato. Se è distribuito Kaspersky Endpoint Security 12.8 o versioni successive, è consigliabile deselezionare questa casella di controllo e utilizzare il criptaggio delle password più avanzato. Le versioni precedenti dell'applicazione non supportano il criptaggio delle password avanzato. Per eseguire l'attività, è necessario selezionare la casella di controllo.

Passaggio 3. Selezione dell'account per eseguire l'attività

Selezionare **Account predefinito**. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

Passaggio 4. Configurazione di una pianificazione di avvio dell'attività

In **Avvio pianificato**, selezionare **Manualmente**.

Passaggio 5. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Password di connessione al server principale*.

Passaggio 6. Completamento della creazione dell'attività

Terminare la procedura guidata. Selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata** o eseguire l'attività manualmente. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come impostare una password per la protezione della connessione al server in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Protezione della connessione ad Administration Server**.

   c. Nel campo **Nome attività**, immettere una breve descrizione, ad esempio *Password di connessione al server principale*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Selezionare un account utente predefinito. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

6. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Fare clic sull'attività **Protezione della connessione ad Administration Server** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

8. Selezionare la scheda **Impostazioni applicazione**.

9. In **Protezione della connessione ad Administration Server**, selezionare **Proteggi con una password**.

10. Nell'elenco a discesa **Connessione all'Administration Server**, selezionare **Nuova password**.

11. Nel campo **Password per la connessione ad Administration Server**, impostare una password per la connessione ad Administration Server e confermarla.

    Se si dimentica la password, è possibile modificarla utilizzando un'attività.

12. Se è distribuito Kaspersky Endpoint Security 12.7 o una versione precedente dell'applicazione, selezionare la casella di controllo **Abilita la compatibilità del criptaggio delle password per le versioni precedenti dell'applicazione (12.7 e inferiori)**.

    A partire da Kaspersky Endpoint Security 12.8 for Windows, l'applicazione utilizza un criptaggio delle password più avanzato. Se è distribuito Kaspersky Endpoint Security 12.8 o versioni successive, è consigliabile deselezionare questa casella di controllo e utilizzare il criptaggio delle password più avanzato. Le versioni precedenti dell'applicazione non supportano il criptaggio delle password avanzato. Per eseguire l'attività, è necessario selezionare la casella di controllo.

13. Salvare le modifiche.

14. Selezionare la casella di controllo accanto all'attività.

15. Fare clic su **Avvia**.

È possibile monitorare lo stato dell'attività e il numero di dispositivi in cui l'attività è stata completata o è stata completata con un errore.

Riconnessione del computer a un Administration Server diverso

La riconnessione del computer a un Administration Server diverso prevede i seguenti passaggi:

1. Nella console del server `[KSC1]` corrente, eseguire l'attività *Cambia Administration Server* per Network Agent.

   Dopo aver eseguito l'attività, il computer viene ricollegato al nuovo server `[KSC2]`.

   Il computer verrà visualizzato nella console del server `[KSC1]` con lo stato *Critico*  . È impossibile configurare l'applicazione utilizzando criteri o eseguendo attività da remoto sul computer.

2. Nella console del nuovo server `[KSC2]`, creare una nuova attività *Protezione della connessione ad Administration Server* per Kaspersky Endpoint Security. Nelle proprietà dell'attività, immettere la password del server precedente e impostare una password per il nuovo server.

   Come impostare una nuova password per riconnettersi a un nuovo server in Administration Console (MMC)

   1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

      Viene aperto l'elenco delle attività.

   2. Fare clic su **Nuova attività**.

   Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Protezione della connessione ad Administration Server**.

Passaggio 2. Protezione della connessione ad Administration Server

Impostare una password per proteggere la connessione al nuovo Administration Server:

1. In **Protezione della connessione ad Administration Server**, selezionare **Proteggi con una password**.
2. Nell'elenco a discesa **Administration Server**, selezionare **Riconnetti da un altro server**.
3. Nel campo **Password corrente**, immettere la password impostata per la connessione al server attendibile utilizzato in precedenza.
4. Nel campo **Nuova password**, impostare una password per la connessione al nuovo Administration Server e confermarla.

   Se si dimentica la password, è possibile modificarla utilizzando un'attività.
5. Se è distribuito Kaspersky Endpoint Security 12.7 o una versione precedente dell'applicazione, selezionare la casella di controllo **Abilita la compatibilità del criptaggio della password per le versioni precedenti dell'applicazione (12.7 e precedenti)**.

   A partire da Kaspersky Endpoint Security 12.8 for Windows, l'applicazione utilizza un criptaggio delle password più avanzato. Se è distribuito Kaspersky Endpoint Security 12.8 o versioni successive, è consigliabile deselezionare questa casella di controllo e utilizzare il criptaggio delle password più avanzato. Le versioni precedenti dell'applicazione non supportano il criptaggio delle password avanzato. Per eseguire l'attività, è necessario selezionare la casella di controllo.

Passaggio 3. Selezione dell'account per eseguire l'attività

Selezionare **Account predefinito**. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

Passaggio 4. Configurazione di una pianificazione di avvio dell'attività

In **Avvio pianificato**, selezionare **Manualmente**.

Passaggio 5. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Password di connessione al server principale*.

Passaggio 6. Completamento della creazione dell'attività

Terminare la procedura guidata. Selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata** o eseguire l'attività manualmente. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come impostare una nuova password per riconnettersi a un nuovo server in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Protezione della connessione ad Administration Server**.

   c. Nel campo **Nome attività**, immettere una breve descrizione, ad esempio *Password di connessione al server principale*.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Selezionare un account utente predefinito. Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

6. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Fare clic sull'attività **Protezione della connessione ad Administration Server** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

8. Selezionare la scheda **Impostazioni applicazione**.

9. In **Protezione della connessione ad Administration Server**, selezionare **Proteggi con una password**.

10. Nell'elenco a discesa **Connessione all'Administration Server**, selezionare **Riconnetti da un altro server**.

11. Nel campo **Password corrente**, immettere la password impostata per la connessione al server attendibile utilizzato in precedenza.

12. Nel campo **Nuova password**, impostare una password per la connessione al nuovo Administration Server e confermarla.

    Se si dimentica la password, è possibile modificarla utilizzando un'attività.

13. Se è distribuito Kaspersky Endpoint Security 12.7 o una versione precedente dell'applicazione, selezionare la casella di controllo **Abilita la compatibilità del criptaggio delle password per le versioni precedenti dell'applicazione (12.7 e inferiori)**.

    A partire da Kaspersky Endpoint Security 12.8 for Windows, l'applicazione utilizza un criptaggio delle password più avanzato. Se è distribuito Kaspersky Endpoint Security 12.8 o versioni successive, è consigliabile deselezionare questa casella di controllo e utilizzare il criptaggio delle password più avanzato. Le versioni precedenti dell'applicazione non supportano il criptaggio delle password avanzato. Per eseguire l'attività, è necessario selezionare la casella di controllo.

14. Salvare le modifiche.

15. Selezionare la casella di controllo accanto all'attività.

16. Fare clic su **Avvia**.

    È possibile monitorare lo stato dell'attività e il numero di dispositivi in cui l'attività è stata completata o è stata completata con un errore.

Dopo aver completato l'attività, assicurarsi che nella console del nuovo server `[KSC2]` al computer sia associato lo stato *OK*. Verificare se è possibile eseguire attività da remoto e configurare l'applicazione utilizzando i criteri.

Reimpostazione della password di connessione di Administration Server

Se si dimentica la password di connessione di Administration Server o la password è compromessa, è possibile reimpostarla nelle proprietà dell'attività. È inoltre possibile reimpostare la password e impostarne una nuova per un gruppo di computer con stati di protezione della connessione di Administration Server diversi. In altre parole, se su alcuni computer la protezione è abilitata e su altri è disabilitata, l'attività imposta una password per tutti i computer.

> È possibile reimpostare la password di connessione di Administration Server solo nella console del server attendibile a cui è connesso il computer.

Come reimpostare la password della connessione di Administration Server utilizzando Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella struttura della console, selezionare **Attività**.

3. Selezionare l'attività **Protezione della connessione ad Administration Server** e fare doppio clic per aprire le proprietà dell'attività.

4. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.

5. In **Protezione della connessione ad Administration Server**, selezionare **Proteggi e cambia password**.

6. Nel campo **Password per la connessione ad Administration Server**, impostare una nuova password per la connessione al server attendibile corrente e confermarla.

7. Salvare le modifiche.

8. Eseguire l'attività.

Come reimpostare la password della connessione di Administration Server in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Protezione della connessione ad Administration Server** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Selezionare la scheda **Impostazioni applicazione**.

4. In **Protezione della connessione ad Administration Server**, selezionare **Proteggi e cambia password**.

5. Nel campo **Password per la connessione ad Administration Server**, impostare una nuova password per la connessione al server attendibile corrente e confermarla.

6. Salvare le modifiche.

7. Selezionare la casella di controllo accanto all'attività.

8. Fare clic su **Avvia**.

Di conseguenza, la password di connessione di Administration Server viene reimpostata al termine dell'attività.

Disabilitazione della protezione della connessione ad Administration Server

È possibile disabilitare la protezione della connessione di Administration Server da remoto solo nella console del server attendibile a cui è connesso il computer. È inoltre possibile disabilitare la protezione in locale tramite la riga di comando.

Come disabilitare la protezione della connessione al server in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella struttura della console, selezionare **Attività**.

3. Selezionare l'attività **Protezione della connessione ad Administration Server** e fare doppio clic per aprire le proprietà dell'attività.

4. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.

5. In **Protezione della connessione ad Administration Server**, selezionare **Non proteggere**.

6. Salvare le modifiche.

7. Eseguire l'attività.

   È possibile monitorare lo stato dell'attività e il numero di dispositivi in cui l'attività è stata completata o è stata completata con un errore.

Come disabilitare la protezione della connessione al server in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Protezione della connessione ad Administration Server** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Selezionare la scheda **Impostazioni applicazione**.

4. In **Protezione della connessione ad Administration Server**, selezionare **Non proteggere con una password**.

5. Salvare le modifiche.

6. Selezionare la casella di controllo accanto all'attività.

7. Fare clic su **Avvia**.

   È possibile monitorare lo stato dell'attività e il numero di dispositivi in cui l'attività è stata completata o è stata completata con un errore.

Come disabilitare la protezione della connessione al server tramite la riga di comando

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.

2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

3. Eseguire il seguente comando:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   dove `<password>` è la password dell'account utente di KL Admin o la password dall'attività *Protezione della connessione ad Administration Server*. Se il parametro non è specificato, Kaspersky Endpoint Security richiede di immettere una password nella riga successiva.

   Per eseguire questo comando, Protezione tramite password deve essere abilitato.

Esempio

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Criptaggio dei dati

Kaspersky Endpoint Security consente di criptare file e cartelle archiviati in unità locali e rimovibili o interi dischi rigidi e unità rimovibili. Il criptaggio dei dati riduce al minimo il rischio di diffusione di informazioni che può verificarsi in seguito al furto o allo smarrimento di computer portatili, unità rimovibili o dischi rigidi oppure in caso di accesso ai dati da parte di utenti o applicazioni non autorizzati. Kaspersky Endpoint Security utilizza l'algoritmo di criptaggio AES Advanced Encryption Standard.

Se la licenza è scaduta, l'applicazione non cripta i nuovi dati e i dati criptati precedenti restano criptati e disponibili per l'utilizzo. In questo caso, il criptaggio dei nuovi dati richiede l'attivazione dell'applicazione con una nuova licenza che consente l'utilizzo del criptaggio.

Se Kaspersky Endpoint Security è installato in un computer basato su Arm, è disponibile solo Criptaggio unità BitLocker. L'applicazione non supporta altri componenti di criptaggio dei dati.

Se la licenza è scaduta, si è verificata una violazione del Contratto di licenza con l'utente finale oppure la chiave di licenza, Kaspersky Endpoint Security o i componenti di criptaggio sono stati rimossi, lo stato di criptaggio dei file criptati in precedenza non è garantito. Questo è dovuto al fatto che alcune applicazioni, come Microsoft Office Word, creano una copia temporanea dei file durante la modifica. Quando il file originale viene salvato, la copia temporanea sostituisce il file originale. Di conseguenza, in un computer privo di funzionalità di criptaggio o in cui tali funzionalità non sono accessibili, il file rimane non criptato.

Kaspersky Endpoint Security offre le seguenti caratteristiche per la protezione dei dati:

- **Criptaggio a livello di file nelle unità locali del computer**. È possibile compilare elenchi di file (per estensione o gruppi di estensioni) e cartelle nelle unità locali del computer, nonché creare regole per il criptaggio dei file creati da applicazioni specifiche. Dopo l'applicazione di un criterio, Kaspersky Endpoint Security cripta e decripta i seguenti file:
  - file aggiunti singolarmente agli elenchi per il criptaggio e il decriptaggio;
  - file memorizzati in cartelle aggiunte agli elenchi per il criptaggio e il decriptaggio;
  - File creati da applicazioni distinte.
- **Criptaggio unità rimovibili**. È possibile specificare una regola di criptaggio predefinita in base alla quale l'applicazione applica la stessa azione a tutte le unità rimovibili oppure specificare diverse regole di criptaggio per le singole unità rimovibili.

  La regola di criptaggio predefinita ha una priorità inferiore rispetto alle regole di criptaggio create per le singole unità rimovibili. Le regole di criptaggio create per le unità rimovibili con il modello di dispositivo specificato hanno una priorità inferiore rispetto alle regole di criptaggio create per le unità rimovibili con l'ID dispositivo specificato.

  Per selezionare una regola di criptaggio per i file in un'unità rimovibile, Kaspersky Endpoint Security verifica se il modello e l'ID del dispositivo sono noti o meno. L'applicazione esegue quindi una delle seguenti operazioni:
  - Se è noto solo il modello di dispositivo, l'applicazione utilizza l'eventuale regola di criptaggio creata per le unità rimovibili con lo specifico modello di dispositivo.
  - Se è noto solo l'ID del dispositivo, l'applicazione utilizza l'eventuale regola di criptaggio creata per le unità rimovibili con lo specifico ID di dispositivo.

- Se il modello e l'ID del dispositivo sono noti, l'applicazione utilizza l'eventuale regola di criptaggio creata per le unità rimovibili con lo specifico ID di dispositivo. Se non esiste una regola di questo tipo, ma è stata creata una regola di criptaggio per le unità rimovibili con lo specifico modello di dispositivo, viene applicata questa regola. Se non è specificata alcuna regola di criptaggio per l'ID di dispositivo specifico né per il modello di dispositivo specifico, viene applicata la regola di criptaggio predefinita.

- Se non sono noti né il modello né l'ID del dispositivo, l'applicazione utilizza la regola di criptaggio predefinita.

L'applicazione consente di preparare un'unità rimovibile per l'utilizzo dei dati criptati che contiene in modalità portatile. Dopo avere abilitato la modalità portatile, è possibile accedere ai file criptati nelle unità rimovibili connesse a un computer in cui non è installata la funzionalità di criptaggio.

- **Gestione delle regole di accesso delle applicazioni ai file criptati**. Per qualsiasi applicazione, è possibile creare una regola di accesso ai file criptati che blocca l'accesso ai file criptati o consente l'accesso ai file criptati solo come testo criptato (una sequenza di caratteri ottenuti quando viene applicato il criptaggio).

- **Creazione di pacchetti criptati**. È possibile creare archivi criptati e proteggere l'accesso a tali archivi tramite una password. Il contenuto degli archivi criptati è accessibile solo immettendo le password utilizzate per proteggere l'accesso agli archivi. Tali archivi possono essere trasferiti in modo sicuro in rete o su unità rimovibili.

- **Criptaggio dell'intero disco**. È possibile selezionare una tecnologia di criptaggio: Criptaggio disco Kaspersky o Crittografia unità BitLocker (di seguito denominato semplicemente "BitLocker").

  BitLocker è una tecnologia inclusa nel sistema operativo Windows. Se un computer è dotato di un TPM Trusted Platform Module, BitLocker lo utilizza per archiviare le chiavi di ripristino che forniscono l'accesso a un disco rigido criptato. All'avvio del computer, BitLocker richiede al Trusted Platform Module le chiavi di ripristino del disco rigido e sblocca l'unità. È possibile configurare l'utilizzo di una password e/o un codice PIN per l'accesso alle chiavi di ripristino.

  È possibile specificare la regola predefinita per il criptaggio dell'intero disco e creare un elenco di dischi rigidi da escludere dal criptaggio. Kaspersky Endpoint Security esegue il criptaggio dell'intero disco a livello di settore dopo l'applicazione del criterio di Kaspersky Security Center. L'applicazione cripta tutte le partizioni dei dischi rigidi contemporaneamente.

  Una volta criptati i dischi rigidi di sistema, al successivo avvio del computer l'utente deve eseguire l'autenticazione utilizzando l'Agente di Autenticazione prima di poter accedere ai dischi rigidi e caricare il sistema operativo. Questo richiede l'immissione della password del token o della smart card connessa al computer oppure il nome utente e la password dell'account per l'Agente di Autenticazione creato dall'amministratore della rete LAN tramite l'attività *Gestisci account dell'Agente di Autenticazione*. Questi account sono basati sugli account di Microsoft Windows con cui gli utenti eseguono l'accesso al sistema operativo. È inoltre possibile utilizzare la tecnologia SSO Single Sign-On, che consente di accedere automaticamente al sistema operativo utilizzando il nome utente e la password dell'account dell'Agente di Autenticazione.

  Se si esegue il backup di un computer, si criptano i dati nel computer e quindi si esegue il ripristino della copia di backup del computer e si criptano nuovamente i dati nel computer, Kaspersky Endpoint Security crea duplicati degli account per l'Agente di Autenticazione. Per rimuovere gli account duplicati, è necessario utilizzare l'utilità klmover con il parametro `dupfix`. L'utilità klmover è inclusa nella build di Kaspersky Security Center. Ulteriori informazioni sul relativo utilizzo sono disponibili nella Guida di Kaspersky Security Center.

L'accesso alle unità criptate è possibile solo dai computer in cui è installato Kaspersky Endpoint Security con la funzionalità di criptaggio dell'intero disco. Questa precauzione riduce al minimo il rischio di diffusione dei dati da un'unità criptata quando viene effettuato un tentativo di accedervi all'esterno della rete LAN aziendale.

Per criptare i dischi rigidi e le unità rimovibili, è possibile utilizzare la funzione Cripta solo lo spazio su disco utilizzato. È consigliabile utilizzare questa funzione solo per i nuovi dispositivi che non sono stati utilizzati in precedenza. Se si applica il criptaggio a un dispositivo già in uso, è consigliabile criptare l'intero dispositivo. Questo garantisce che tutti i dati siano protetti, anche i dati eliminati che potrebbero ancora contenere informazioni recuperabili.

Prima di avviare il criptaggio, Kaspersky Endpoint Security ottiene la mappa dei settori del file system. Il primo passaggio di criptaggio include i settori che sono occupati da file al momento dell'avvio del criptaggio. Il secondo passaggio di criptaggio include i settori che sono stati scritti dopo l'avvio del criptaggio. Al termine del criptaggio, tutti i settori che contengono dati sono criptati.

Una volta completato il criptaggio, se un utente elimina un file, i settori in cui era memorizzato il file eliminato diventano disponibili per la memorizzazione di nuove informazioni a livello di file system, ma rimangono criptati. Dal momento che i file vengono scritti in un nuovo dispositivo e il dispositivo viene regolarmente criptato con la funzione **Cripta solo lo spazio su disco utilizzato** abilitata, tutti i settori verranno criptati dopo un determinato periodo di tempo.

I dati necessari per decriptare i file vengono forniti dal sistema Kaspersky Security Center Administration Server che controllava il computer al momento del criptaggio. Se per qualche motivo il computer con oggetti criptati era gestito da un Administration Server diverso, è possibile ottenere l'accesso ai dati criptati in uno dei seguenti modi:

- Administration Server nella stessa gerarchia:
  - Non è necessario eseguire azioni aggiuntive. L'utente manterrà l'accesso agli oggetti criptati. Le chiavi di criptaggio vengono distribuite a tutti gli Administration Server.
- Administration Server separati:
  - Richiedere l'accesso agli oggetti criptati all'amministratore della LAN.
  - Ripristinare i dati nei dispositivi criptati utilizzando l'utilità di ripristino.
  - Ripristinare la configurazione del sistema Kaspersky Security Center Administration Server che controllava il computer al momento del criptaggio da una copia di backup e utilizzare questa configurazione sull'Administration Server che ora controlla il computer con gli oggetti criptati.

Se non è disponibile l'accesso ai dati criptati, seguire le istruzioni speciali per l'utilizzo dei dati criptati (Ripristino dell'accesso ai file criptati, Utilizzo dei dispositivi criptati quando non è possibile accedervi).

Limitazioni della funzionalità di criptaggio

Il criptaggio dei dati presenta le seguenti limitazioni:

- L'applicazione crea file di servizio durante il criptaggio. Per archiviarli è necessario circa lo 0,5% dello spazio non frammentato disponibile sul disco rigido. Se nel disco rigido non è disponibile spazio libero non frammentato, il criptaggio non verrà avviato fino a quando non verrà liberato spazio sufficiente.
- È possibile gestire tutti i componenti di criptaggio dei dati in Kaspersky Security Center Administration Console e in Kaspersky Security Center Web Console. In Kaspersky Security Center Cloud Console è possibile gestire solo Bitlocker.
- Il criptaggio dei dati è disponibile solo quando si utilizza Kaspersky Endpoint Security con il sistema di amministrazione Kaspersky Security Center o Kaspersky Security Center Cloud Console (solo BitLocker). Non è possibile utilizzare il criptaggio dei dati quando si utilizza Kaspersky Endpoint Security in modalità offline poiché Kaspersky Endpoint Security archivia le chiavi di criptaggio in Kaspersky Security Center.

- Se Kaspersky Endpoint Security è installato in un computer che esegue Microsoft Windows for Servers, è disponibile solo il criptaggio dell'intero disco con la tecnologia Crittografia unità BitLocker. Se Kaspersky Endpoint Security è installato in un computer che esegue Windows per workstation, la funzionalità di criptaggio dei dati è completamente disponibile.

- Se Kaspersky Endpoint Security è installato in un computer basato su Arm, è disponibile solo il Criptaggio dell'intero disco che utilizza la tecnologia Crittografia unità BitLocker, mentre gli altri componenti di criptaggio non sono supportati.

Il criptaggio dell'intero disco con la tecnologia Criptaggio disco Kaspersky non è disponibile per i dischi rigidi che non soddisfano i requisiti hardware e software.

La compatibilità tra la funzionalità Criptaggio dell'intero disco di Kaspersky Endpoint Security e Kaspersky Anti-Virus for UEFI non è supportata. Kaspersky Anti-Virus for UEFI viene avviato prima del caricamento del sistema operativo. Quando si utilizza il criptaggio dell'intero disco, l'applicazione rileverà l'assenza di un sistema operativo installato nel computer. Di conseguenza, il funzionamento di Kaspersky Anti-Virus for UEFI terminerà con un errore. Criptaggio a livello di file (FLE) non influisce sul funzionamento di Kaspersky Anti-Virus for UEFI.

Kaspersky Endpoint Security supporta le seguenti configurazioni:

- Unità HDD, SSD e USB.

  La tecnologia Criptaggio disco Kaspersky (FDE) supporta l'utilizzo di unità SSD preservando le prestazioni e la durata delle unità SSD.

- Unità collegate tramite bus: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.

- Unità non rimovibili collegate tramite bus MMC o SD.

- Unità con settori da 512 byte.

- Unità con settori da 4096 byte che emulano 512 byte.

- Unità con il seguente tipo di partizioni: GPT, MBR e VBR (unità rimovibili).

- Software integrato dello standard UEFI 64 e Legacy BIOS.

- Software integrato dello standard UEFI con supporto Secure Boot.

  Secure Boot è una tecnologia progettata per verificare le firme digitali per applicazioni e driver del caricatore UEFI. Secure Boot blocca l'avvio di applicazioni e driver UEFI non firmati o firmati da autori sconosciuti. Criptaggio disco Kaspersky (FDE) supporta completamente Secure Boot. L'Agente di Autenticazione è firmato da un certificato Microsoft Windows UEFI Driver Publisher.

  In alcuni dispositivi (ad esempio Microsoft Surface Pro e Microsoft Surface Pro 2), potrebbe essere installato per impostazione predefinita un elenco obsoleto di certificati di verifica della firma digitale. Prima di criptare l'unità è necessario aggiornare l'elenco dei certificati.

- Software integrato dello standard UEFI con supporto Fast Boot.

  Fast Boot è una tecnologia che consente un avvio più rapido del computer. Quando la tecnologia Fast Boot è abilitata, normalmente il computer carica solo il set minimo di driver UEFI necessari per l'avvio del sistema operativo. Quando la tecnologia Fast Boot è abilitata, tastiere USB, mouse, token USB, touchpad e touchscreen potrebbero non funzionare mentre l'Agente di Autenticazione è in esecuzione.

Per utilizzare Criptaggio disco Kaspersky (FDE), è consigliabile disabilitare la tecnologia Fast Boot. È possibile utilizzare l'utilità di test FDE per testare il funzionamento di Criptaggio disco Kaspersky (FDE).

Kaspersky Endpoint Security non supporta le seguenti configurazioni:

- Il caricatore di avvio è in un'unità mentre il sistema operativo è in un'unità diversa.
- Il sistema contiene software incorporato conforme allo standard UEFI 32.
- Il sistema dispone di Intel® Rapid Start Technology e unità con una partizione di ibernazione, anche quando Intel® Rapid Start Technology è disabilitato.
- Unità in formato MBR con più di 10 partizioni estese.
- Il sistema dispone di un file di scambio situato su un'unità non di sistema.
- Sistema ad avvio multiplo con diversi sistemi operativi installati contemporaneamente.
- Partizioni dinamiche (sono supportate solo le partizioni principali).
- Unità con meno del 0,5% di spazio libero su disco non frammentato.
- Unità con dimensioni dei settori diverse da 512 byte o 4096 byte che emulano 512 byte.
- Unità ibride.
- Il sistema dispone di caricatori di terze parti.
- Unità con directory NTFS compresse.
- La tecnologia Criptaggio disco Kaspersky (FDE) non è compatibile con altre tecnologie di criptaggio dell'intero disco (come BitLocker, McAfee Drive Encryption e WinMagic SecureDoc).
- La tecnologia Criptaggio disco Kaspersky (FDE) non è compatibile con la tecnologia ExpressCache.
- La creazione, l'eliminazione e la modifica di partizioni su un'unità criptata non sono supportate. I dati potrebbero essere persi.
- La formattazione del file system non è supportata. I dati potrebbero essere persi.

  Se è necessario formattare un'unità criptata con la tecnologia Criptaggio disco Kaspersky (FDE), formattare l'unità in un computer che non dispone di Kaspersky Endpoint Security for Windows e utilizzare solo il criptaggio dell'intero disco.

  Un'unità criptata formattata con l'opzione di formattazione rapida potrebbe essere erroneamente identificata come criptata la volta successiva che viene collegata a un computer in cui è installato Kaspersky Endpoint Security for Windows. I dati dell'utente non saranno disponibili.
- L'Agente di Autenticazione supporta non più di 100 account.
- La tecnologia Single Sign-On non è compatibile con altre tecnologie di sviluppatori di terze parti.

- La tecnologia Criptaggio disco Kaspersky (FDE) non è supportata nei seguenti modelli di dispositivi:
  - Dell Latitude E6410 (modalità UEFI)
  - HP Compaq nc8430 (modalità Legacy BIOS)
  - Lenovo ThinkCentre 8811 (modalità Legacy BIOS)
- L'Agente di Autenticazione non supporta l'utilizzo di token USB quando è abilitato il supporto Legacy USB. Nel computer sarà possibile solo l'autenticazione basata su password.
- Quando si cripta un'unità in modalità Legacy BIOS, è consigliabile abilitare il supporto Legacy USB nei seguenti modelli di dispositivi:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 Microtower PC
  - Lenovo G550
  - Lenovo ThinkPad L530

- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (scheda madre)

Modifica della lunghezza della chiave di criptaggio (AES56 / AES256)

Kaspersky Endpoint Security utilizza l'algoritmo di criptaggio AES (Advanced Encryption Standard). Kaspersky Endpoint Security supporta l'algoritmo di criptaggio AES con una lunghezza della chiave effettiva di 256 o 56 bit. L'algoritmo di criptaggio dei dati dipende dalla libreria di criptaggio AES inclusa nel pacchetto di distribuzione: *Criptaggio avanzato (AES256)* o *Criptaggio superficiale (AES56)*. La libreria di criptaggio AES viene installata insieme all'applicazione.

La modifica della lunghezza della chiave di criptaggio è disponibile solo per Kaspersky Endpoint Security 11.2.0 o versioni successive.

La modifica della lunghezza della chiave di criptaggio prevede i seguenti passaggi:

1. Decriptare gli oggetti criptati da Kaspersky Endpoint Security prima di iniziare a modificare la lunghezza della chiave di criptaggio:
   a. Decriptare i dischi rigidi.
   b. Decriptare i file nelle unità locali.
   c. Decriptare le unità rimovibili.

   Dopo avere modificato la lunghezza della chiave di criptaggio, gli oggetti precedentemente criptati diventano non disponibili.
2. Rimuovere Kaspersky Endpoint Security.
3. Installare Kaspersky Endpoint Security dal pacchetto di distribuzione di Kaspersky Endpoint Security che contiene un'altra libreria di criptaggio.

È inoltre possibile modificare la lunghezza della chiave di criptaggio eseguendo l'upgrade dell'applicazione. La lunghezza della chiave può essere modificata tramite un upgrade dell'applicazione solo se vengono soddisfatte le seguenti condizioni:

- Kaspersky Endpoint Security versione 10 Service Pack 2 o successiva è installato nel computer.
- I componenti di criptaggio dei dati (Criptaggio a livello di file, Criptaggio dell'intero disco) non sono installati nel computer.

  Per impostazione predefinita, i componenti di criptaggio dei dati non sono inclusi in Kaspersky Endpoint Security. Il componente BitLocker Management non influisce sulla modifica della lunghezza della chiave di criptaggio.

Per modificare la lunghezza della chiave di criptaggio, eseguire il file kes_win.msi o setup_kes.exe dal pacchetto di distribuzione contenente la libreria di criptaggio necessaria. È inoltre possibile eseguire in remoto l'upgrade dell'applicazione utilizzando il pacchetto di installazione.

È impossibile modificare la lunghezza della chiave di criptaggio utilizzando il pacchetto di distribuzione della stessa versione dell'applicazione installata nel computer senza prima disinstallare l'applicazione.

Criptaggio disco Kaspersky

Criptaggio disco Kaspersky non è supportato nei computer basati su Arm.

Criptaggio disco Kaspersky è disponibile solo per i computer che eseguono un sistema operativo Windows per workstation. Per i computer che eseguono un sistema operativo Windows per server, utilizzare la tecnologia Crittografia unità BitLocker.

Kaspersky Endpoint Security supporta il criptaggio dell'intero disco nei file system FAT32, NTFS ed exFat.

Prima di avviare il criptaggio dell'intero disco, l'applicazione esegue una serie di controlli per stabilire se il dispositivo può essere criptato. I controlli includono la verifica della compatibilità del disco rigido del sistema con l'Agente di Autenticazione o con i componenti di criptaggio di BitLocker. Per verificare la compatibilità, è necessario riavviare il computer. Dopo aver riavviato il computer, l'applicazione esegue automaticamente tutti i controlli necessari. Se il controllo della compatibilità ha esito positivo, ha inizio il criptaggio dell'intero disco dopo il caricamento del sistema operativo e l'avvio dell'applicazione. Se i dischi rigidi del sistema risultano incompatibili con l'Agente di Autenticazione o con i componenti di criptaggio di BitLocker, è necessario riavviare il computer premendo il pulsante di reimpostazione dell'hardware. Kaspersky Endpoint Security registra le informazioni sull'incompatibilità. In base a queste informazioni, l'applicazione non avvia il criptaggio dell'intero disco all'avvio del sistema operativo. Le informazioni su questo evento vengono registrate nei rapporti di Kaspersky Security Center.

Se la configurazione hardware del computer è stata modificata, le informazioni sull'incompatibilità registrate dall'applicazione durante il controllo precedente devono essere eliminate per verificare la compatibilità dei dischi rigidi del sistema con l'Agente di Autenticazione e con i componenti di criptaggio di BitLocker. A tale scopo, prima del criptaggio dell'intero disco è necessario digitare `avp pbatestreset` nella riga di comando. Se si verificano errori nel caricamento del sistema operativo in seguito alla verifica della compatibilità dei dischi rigidi del sistema con l'Agente di Autenticazione, è necessario rimuovere gli oggetti e i dati rimanenti in seguito all'operazione di verifica dell'Agente di Autenticazione tramite l'utilità di ripristino, avviare Kaspersky Endpoint Security ed eseguire nuovamente il comando `avp pbatestreset`.

In seguito all'avvio del criptaggio dell'intero disco, Kaspersky Endpoint Security cripta tutti i dati presenti nei dischi.

Se l'utente arresta o riavvia il computer durante il criptaggio dell'intero disco, l'Agente di Autenticazione viene caricato prima del successivo avvio del sistema operativo. Kaspersky Endpoint Security riprende il criptaggio dell'intero disco dopo l'autenticazione tramite l'agente di autenticazione e l'avvio del sistema operativo.

Se il sistema operativo entra in modalità di ibernazione durante il criptaggio dell'intero disco, l'Agente di Autenticazione viene caricato all'uscita del sistema operativo dalla modalità di ibernazione. Kaspersky Endpoint Security riprende il criptaggio dell'intero disco dopo l'autenticazione tramite l'agente di autenticazione e l'avvio del sistema operativo.

Se il sistema operativo entra in modalità di sospensione durante il criptaggio dell'intero disco, Kaspersky Endpoint Security riprende il criptaggio dell'intero disco quando il sistema operativo esce dalla modalità di sospensione, senza caricare l'Agente di Autenticazione.

L'autenticazione dell'utente nell'Agente di Autenticazione può essere eseguita in due modi:

- Immettere il nome e la password dell'account per l'Agente di Autenticazione creato dall'amministratore della rete LAN utilizzando gli strumenti di Kaspersky Security Center.
- Immettere la password di un token o di una smart card connessa al computer.

  L'utilizzo di un token o di una smart card è disponibile solo se i dischi rigidi del computer sono stati criptati utilizzando l'algoritmo di criptaggio AES256. Se i dischi rigidi del computer sono stati criptati utilizzando l'algoritmo di criptaggio AES56, l'aggiunta del file del certificato elettronico al comando verrà negata.

L'Agente di Autenticazione supporta i layout di tastiera per le seguenti lingue:

- Inglese (Regno Unito)
- Inglese (Stati Uniti)
- Arabo (Algeria, Marocco, Tunisia; layout AZERTY)
- Spagnolo (America latina)
- Italiano
- Tedesco (Germania e Austria)
- Tedesco (Svizzera)
- Portoghese (Brasile, layout ABNT2)
- Russo (per tastiere IBM/WINDOWS a 105 tasti con layout QWERTY)
- Turco (layout QWERTY)
- Francese (Francia)
- Francese (Svizzera)

- Francese (Belgio, layout AZERTY)
- Giapponese (per tastiere a 106 tasti con layout QWERTY)

Un layout di tastiera diventa disponibile nell'Agente di Autenticazione se il layout è stato aggiunto nelle impostazioni della lingua e delle impostazioni internazionali del sistema operativo e risulta disponibile nella schermata di accesso a Microsoft Windows.

Se il nome dell'account per l'Agente di Autenticazione contiene simboli che non possono essere immessi utilizzando i layout di tastiera disponibili nell'Agente di Autenticazione, è possibile accedere ai dischi rigidi criptati solo dopo che ne è stato eseguito il ripristino tramite l'utilità di ripristino o dopo avere eseguito il ripristino del nome e della password dell'account per l'Agente di Autenticazione.

Funzionalità speciali di criptaggio dell'unità SSD

L'applicazione supporta il criptaggio di unità SSD, unità SSHD ibride e unità con la funzionalità Intel Smart Response. L'applicazione non supporta il criptaggio delle unità con la funzionalità Intel Rapid Start. Disabilitare la funzionalità Intel Rapid Start prima di criptare tale unità.

Il criptaggio delle unità SSD prevede le seguenti funzionalità speciali:

- Se un'unità SSD è nuova e non contiene dati riservati, abilitare il criptaggio solo dello spazio occupato. Ciò consente di sovrascrivere i settori delle unità pertinenti.
- Se è in uso un'unità SSD e contiene dati riservati, selezionare una delle seguenti opzioni:
  - Cancellare completamente l'unità SSD (Secure Erase), installare il sistema operativo ed eseguire il criptaggio dell'unità SSD con l'opzione per criptare solo lo spazio occupato abilitata.
  - Eseguire il criptaggio dell'unità SSD con l'opzione per criptare solo lo spazio occupato disabilitata.

Il criptaggio di un'unità SSD richiede 5-10 GB di spazio libero. I requisiti di spazio per l'archiviazione dei dati di amministrazione di criptaggio sono elencati nella tabella seguente.

Requisiti di spazio per l'archiviazione dei dati di amministrazione di criptaggio

Dimensioni unità SSD (GB)	Spazio libero sulla partizione primaria dell'unità SSD (MB)	Spazio libero sulla partizione secondaria dell'unità SSD (MB)
128	250	64
256	250	640
512	300	128

Avvio di Criptaggio disco Kaspersky

Prima di avviare il criptaggio dell'intero disco, è consigliabile verificare che il computer non sia infetto. A tale scopo, avviare l'attività Scansione completa o Scansione delle aree critiche. L'esecuzione del criptaggio dell'intero disco in un computer infetto da un rootkit può rendere inutilizzabile il computer.

Prima di avviare il criptaggio del disco, è necessario verificare le impostazioni degli account dell'Agente di Autenticazione. L'Agente di Autenticazione è necessario per utilizzare unità protette mediante la tecnologia Criptaggio disco Kaspersky. Prima del caricamento del sistema operativo, l'utente deve completare l'autenticazione con l'Agente. Kaspersky Endpoint Security consente di creare automaticamente account dell'Agente di Autenticazione prima di criptare un'unità. È possibile abilitare la creazione automatica degli account dell'Agente di Autenticazione nelle impostazioni dei criteri di Criptaggio dell'intero disco (vedere le istruzioni riportate di seguito). È inoltre possibile utilizzare la tecnologia SSO (Single Sign-On).

Kaspersky Endpoint Security consente di creare automaticamente l'Agente di Autenticazione per i seguenti gruppi di utenti.

- **Tutti gli account nel computer**. Tutti gli account nel computer che sono stati attivi in qualsiasi momento.
- **Tutti gli account di dominio nel computer**. Tutti gli account nel computer che appartengono a qualche dominio e che sono stati attivi in qualsiasi momento.
- **Tutti gli account locali nel computer**. Tutti gli account locali nel computer che sono stati attivi in qualsiasi momento.
- **Account di servizio con una password monouso**. L'account di servizio è necessario per accedere al computer, ad esempio quando l'utente dimentica la password. È inoltre possibile utilizzare l'account di servizio come account di riserva. È necessario inserire il nome dell'account (per impostazione predefinita, `ServiceAccount`). Kaspersky Endpoint Security crea automaticamente una password. È possibile trovare la password nella console di Kaspersky Security Center.
- **Amministratore locale**. Kaspersky Endpoint Security crea un account utente dell'Agente di Autenticazione per l'amministratore locale del computer.
- **Responsabile computer**. Kaspersky Endpoint Security crea un account utente dell'Agente di Autenticazione per l'account del responsabile del computer. È possibile vedere quale account ha il ruolo di responsabile del computer nelle proprietà del computer in Active Directory. Per impostazione predefinita, il ruolo di responsabile del computer non è definito, ovvero non corrisponde ad alcun account.
- **Account attivo**. Kaspersky Endpoint Security crea automaticamente un account dell'Agente di Autenticazione per l'account attivo al momento del criptaggio del disco.

L'attività *Gestisci account dell'Agente di Autenticazione* è progettata per la configurazione delle impostazioni di autenticazione degli utenti. È possibile utilizzare questa attività per aggiungere nuovi account, modificare le impostazioni degli account correnti o rimuovere account se necessario. È possibile utilizzare attività locali per singoli computer, nonché attività di gruppo per computer di gruppi di amministrazione separati o una selezione di computer.

Come eseguire Criptaggio disco Kaspersky tramite Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
4. Nell'elenco a discesa **Tecnologia di criptaggio**, selezionare **Criptaggio disco Kaspersky**.

   La tecnologia Criptaggio disco Kaspersky non può essere utilizzata se il computer dispone di dischi rigidi criptati tramite BitLocker.

5. Nell'elenco a discesa **Modalità di criptaggio**, selezionare **Cripta tutti i dischi rigidi**.

Se nel computer sono installati diversi sistemi operativi, dopo il criptaggio di tutti i dischi rigidi sarà possibile caricare solo il sistema operativo in cui è installata l'applicazione.

Se è necessario escludere alcuni dischi rigidi dal criptaggio, creare un elenco di tali dischi rigidi.

6. Configurare le opzioni avanzate di Criptaggio disco Kaspersky (vedere la tabella seguente).

7. Salvare le modifiche.

Come eseguire Criptaggio disco Kaspersky tramite Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Criptaggio dei dati** → **Criptaggio dell'intero disco**.

5. Selezionare la tecnologia **Criptaggio disco Kaspersky**.

La tecnologia Criptaggio disco Kaspersky non può essere utilizzata se il computer dispone di dischi rigidi criptati tramite BitLocker.

6. Nel blocco **Azione sui dispositivi**, selezionare **Cripta tutti i dischi rigidi**.

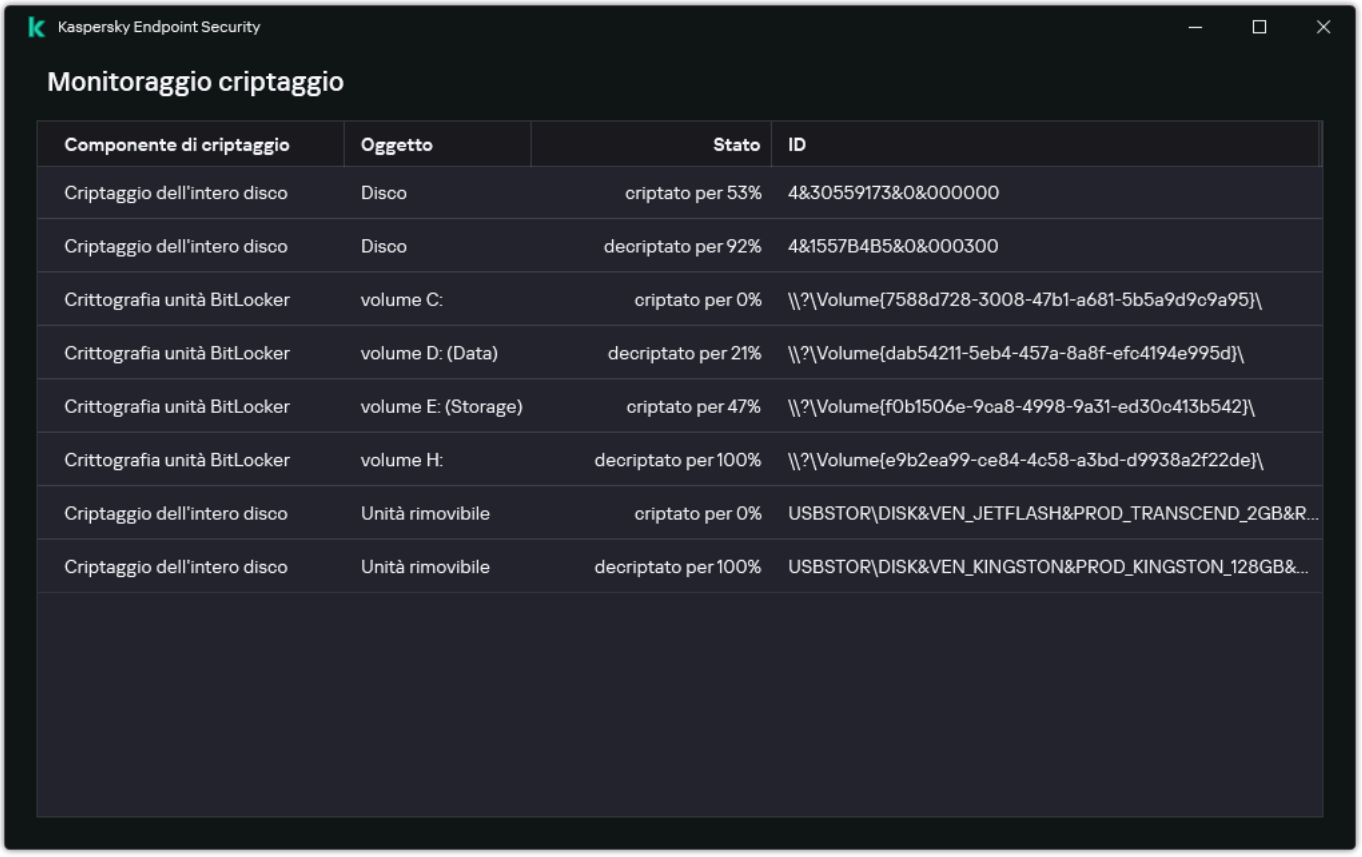
Se nel computer sono installati diversi sistemi operativi, dopo il criptaggio sarà possibile caricare solo il sistema operativo in cui è stato eseguito il criptaggio.

Se è necessario escludere alcuni dischi rigidi dal criptaggio, creare un elenco di tali dischi rigidi.

7. Configurare le opzioni avanzate di Criptaggio disco Kaspersky (vedere la tabella seguente).

8. Salvare le modifiche.

È possibile utilizzare lo strumento Monitoraggio criptaggio per controllare il processo di criptaggio o decriptaggio del disco nel computer di un utente. È possibile eseguire lo strumento Monitoraggio criptaggio dalla finestra principale dell'applicazione.



Monitoraggio criptaggio

Se i dischi rigidi di sistema sono criptati, l'agente di autenticazione viene caricato prima dell'avvio del sistema operativo. Utilizzare l'agente di autenticazione per eseguire l'autenticazione in modo da ottenere l'accesso ai dischi rigidi di sistema criptati e caricare il sistema operativo. Dopo il completamento della procedura di autenticazione, viene caricato il sistema operativo. Il processo di autenticazione viene ripetuto a ogni riavvio del sistema operativo.

Impostazioni del componente Criptaggio disco Kaspersky

Parametro	Descrizione
Crea automaticamente gli account dell'Agente di Autenticazione per utenti durante il criptaggio.	Se questa casella di controllo è selezionata, l'applicazione crea gli account dell'Agente di Autenticazione in base all'elenco degli account utente di Windows nel computer. Per impostazione predefinita, Kaspersky Endpoint Security utilizza tutti gli account locali e di dominio con i quali l'utente ha effettuato l'accesso al sistema operativo negli ultimi 30 giorni.
Crea automaticamente gli account dell'Agente di Autenticazione per tutti gli utenti di questo computer al momento dell'accesso	Se questa casella di controllo è selezionata, l'applicazione controlla le informazioni sugli account utente di Windows nel computer prima di avviare l'Agente di Autenticazione. Se Kaspersky Endpoint Security rileva un account utente Windows che non dispone di un account dell'Agente di Autenticazione, l'applicazione creerà un nuovo account per accedere alle unità criptate. Il nuovo account dell'Agente di Autenticazione avrà le seguenti impostazioni predefinite: solo accesso protetto da password e modifica della password alla prima autenticazione. Pertanto, non è necessario aggiungere manualmente gli account dell'Agente di Autenticazione utilizzando l'attività *Gestisci account dell'Agente di Autenticazione* per i computer con unità già criptate.
Salva il nome utente immesso nell'Agente di Autenticazione	Se la casella di controllo è selezionata, l'applicazione salva il nome dell'account Agente di Autenticazione. Non verrà richiesto di immettere il nome dell'account durante il successivo tentativo di eseguire l'autenticazione nell'Agente di Autenticazione con lo stesso account.

Parametro	Descrizione
Cripta solo lo spazio su disco utilizzato (riduce i tempi di criptaggio)	Questa casella di controllo consente di abilitare o disabilitare l'opzione che limita l'area di criptaggio ai soli settori occupati del disco rigido. Questo limite consente di ridurre il tempo di criptaggio. L'abilitazione o la disabilitazione della funzionalità **Cripta solo lo spazio su disco utilizzato (riduce i tempi di criptaggio)** dopo l'avvio del criptaggio non comporta la modifica di questa impostazione finché i dischi rigidi non vengono decriptati. È necessario selezionare o deselezionare la casella di controllo prima di avviare il criptaggio. Se la casella di controllo è selezionata, vengono criptate solo le parti del disco rigido che sono occupate da file. Kaspersky Endpoint Security cripta automaticamente i nuovi dati man mano che vengono aggiunti. Se la casella di controllo è deselezionata, viene criptato l'intero disco rigido, inclusi i frammenti residui dei file precedentemente eliminati e modificati. Questa opzione è consigliata per i nuovi dischi rigidi in cui non sono stati modificati o eliminati dati. Se si applica il criptaggio a un disco rigido già in uso, è consigliabile criptare l'intero disco rigido. Questo garantisce la protezione di tutti i dati, anche dei dati eliminati potenzialmente ripristinabili. Per impostazione predefinita, la casella di controllo è deselezionata.
Usa Legacy USB Support (opzione non consigliata)	Questa casella di controllo abilita o disabilita la funzionalità Legacy USB Support. *Legacy USB Support* **è** una funzione BIOS/UEFI che consente di utilizzare i dispositivi USB (ad esempio un token di sicurezza) durante la fase di avvio del computer prima dell'avvio del sistema operativo (modalità BIOS). Legacy USB Support non influisce sul supporto dei dispositivi USB dopo l'avvio del sistema operativo. Se la casella di controllo è selezionata, il supporto dei dispositivi USB durante l'avvio iniziale del computer sarà abilitato. Quando la funzione Legacy USB Support è abilitata, l'Agente di Autenticazione in modalità BIOS non supporta l'utilizzo dei token tramite USB. È consigliabile utilizzare questa opzione solo se si verifica un problema di compatibilità hardware e solo per i computer in cui si è verificato il problema.

Creazione di un elenco di dischi rigidi esclusi dal criptaggio

È possibile creare un elenco di esclusioni dal criptaggio solo per tecnologia Criptaggio disco Kaspersky.

Per creare un elenco di dischi rigidi esclusi dal criptaggio:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
4. Nell'elenco a discesa **Tecnologia di criptaggio**, selezionare **Criptaggio disco Kaspersky**.

   Le voci corrispondenti ai dischi rigidi esclusi dal criptaggio vengono visualizzate nella tabella **Non criptare i seguenti dischi rigidi**. Se non è stato creato in precedenza un elenco di dischi rigidi esclusi dal criptaggio, la tabella è vuota.

5. Per aggiungere dischi rigidi all'elenco dei dischi rigidi esclusi dal criptaggio:

   a. Fare clic su **Aggiungi**.

   b. Nella finestra visualizzata, specificare i valori per **Nome dispositivo**, **Computer**, **Tipo di disco**, **Criptaggio disco Kaspersky**.

   c. Fare clic su **Aggiorna**.

   d. Nella colonna **Nome** selezionare le caselle di controllo nelle righe della tabella corrispondenti ai dischi rigidi che si desidera aggiungere all'elenco dei dischi rigidi esclusi dal criptaggio.

   e. Fare clic su **OK**.

   I dischi rigidi selezionati vengono visualizzati nella tabella **Non criptare i seguenti dischi rigidi**.

6. Salvare le modifiche.

Esportazione e importazione di un elenco di dischi rigidi esclusi dal criptaggio

È possibile esportare l'elenco delle esclusioni di criptaggio dei dischi rigidi in un file XML. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di esclusioni dello stesso tipo. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco delle esclusioni o per eseguire la migrazione delle esclusioni in un server diverso.

Come esportare e importare un elenco di esclusioni di criptaggio dei dischi rigidi in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.

4. Nell'elenco a discesa **Tecnologia di criptaggio**, selezionare **Criptaggio disco Kaspersky**.

   Le voci corrispondenti ai dischi rigidi esclusi dal criptaggio vengono visualizzate nella tabella **Non criptare i seguenti dischi rigidi**.

5. Per esportare l'elenco delle esclusioni:

   a. Selezionare le esclusioni che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.

   Se non è stata selezionata alcuna esclusione, Kaspersky Endpoint Security esporterà tutte le esclusioni.

   b. Fare clic sul pulsante → **Esporta**.

   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle esclusioni e selezionare la cartella in cui si desidera salvare il file.

   d. Salvare il file.

   Kaspersky Endpoint Security esporta l'intero elenco di esclusioni nel file XML.

6. Per importare l'elenco delle regole:

    a. Fare clic sul pulsante → **Importa**.

    b. Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle esclusioni.

    c. Aprire il file.

    Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

7. Salvare le modifiche.

Come esportare e importare un elenco di esclusioni di criptaggio dei dischi rigidi in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

    Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Criptaggio dei dati** → **Criptaggio dell'intero disco**.

    Selezionare la tecnologia **Criptaggio disco Kaspersky**.

5. Fare clic sul collegamento **Esclusioni**.

    Verrà visualizzato l'elenco delle esclusioni.

6. Per esportare l'elenco delle regole:

    a. Selezionare le esclusioni che si desidera esportare.

    b. Fare clic sul pulsante → **Esporta**.

    Kaspersky Endpoint Security esporta l'elenco delle esclusioni in un file JSON nella cartella dei download predefinita.

7. Per importare l'elenco delle esclusioni:

    a. Fare clic sul pulsante → **Importa**.

    Nella finestra visualizzata selezionare il file JSON da cui si desidera importare l'elenco delle esclusioni.

    b. Aprire il file.

    Se il computer dispone già di un elenco di esclusioni, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file JSON.

8. Salvare le modifiche.

Abilitazione della tecnologia Single Sign-On (SSO)

La tecnologia SSO (Single Sign-On) consente di accedere automaticamente al sistema operativo utilizzando le credenziali dell'Agente di Autenticazione. Ciò significa che un utente deve immettere una password solo una volta quando accede a Windows (password dell'account di Agente di autenticazione). La tecnologia Single Sign-On consente inoltre di aggiornare automaticamente la password dell'account di Agente di autenticazione quando viene modificata la password dell'account Windows.

Quando si utilizza la tecnologia Single Sign-On, l'Agente di Autenticazione ignora i requisiti di sicurezza della password specificati in Kaspersky Security Center. È possibile impostare i requisiti di sicurezza della password nelle impostazioni del sistema operativo.

Abilitazione della tecnologia Single Sign-On

Come abilitare l'uso della tecnologia Single Sign-On in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Impostazioni di criptaggio generali**.
4. Nel blocco **Impostazioni password**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Agente di autenticazione**, selezionare la casella di controllo **Utilizza la tecnologia SSO (Single Sign-On)**.
6. Se si utilizza un provider di credenziali di terzi, selezionare la casella di controllo **Esegui il wrapping dei fornitori di credenziali di terzi**.
7. Salvare le modifiche.

Successivamente, l'utente deve completare la procedura di autenticazione una sola volta con l'Agente. La procedura di autenticazione non è richiesta per il caricamento del sistema operativo. Il sistema operativo viene caricato automaticamente.

Come abilitare l'utilizzo di Single Sign-On in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
5. Selezionare la tecnologia **Criptaggio disco Kaspersky**.

6. Nella sezione **Impostazioni password** selezionare la casella di controllo **Utilizza la tecnologia SSO (Single Sign-On)**.

7. Se si utilizza un provider di credenziali di terzi, selezionare la casella di controllo **Esegui il wrapping dei fornitori di credenziali di terzi**.

8. Salvare le modifiche.

   Successivamente, l'utente deve completare la procedura di autenticazione una sola volta con l'Agente. La procedura di autenticazione non è richiesta per il caricamento del sistema operativo. Il sistema operativo viene caricato automaticamente.

Affinché la tecnologia Single Sign-On funzioni, la password dell'account Windows e la password per l'account dell'Agente di Autenticazione devono corrispondere. Se le password non corrispondono, l'utente deve eseguire la procedura di autenticazione due volte: nell'interfaccia dell'Agente di Autenticazione e prima di caricare il sistema operativo. Queste azioni devono essere eseguite una sola volta per sincronizzare le password. Successivamente, Kaspersky Endpoint Security sostituisce la password dell'account Agente di Autenticazione con la password dell'account Windows. Quando la password dell'account Windows viene modificata, l'applicazione aggiorna automaticamente la password dell'account di Agente di autenticazione.

Provider di credenziali di terzi

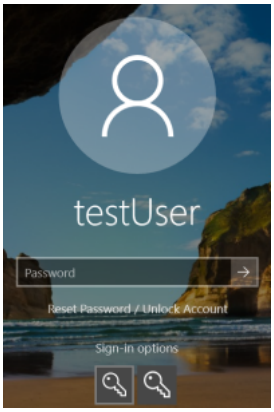
Kaspersky Endpoint Security supporta il provider di credenziali di terzi ADSelfService Plus.

Quando si utilizzano provider di credenziali di terzi, Agente di autenticazione intercetta la password prima del caricamento del sistema operativo. Ciò significa che un utente deve immettere una password solo una volta quando accede a Windows. Dopo aver effettuato l'accesso a Windows, l'utente può utilizzare le funzionalità di un provider di credenziali di terzi, ad esempio per l'autenticazione nei servizi aziendali. I provider di credenziali di terzi consentono inoltre agli utenti di reimpostare in modo indipendente la propria password. In questo caso, Kaspersky Endpoint Security aggiorna automaticamente la password per Agente di autenticazione.

Se si utilizza un provider di credenziali di terzi non supportato dall'applicazione, è possibile che si verifichino alcune limitazioni nel funzionamento della tecnologia Single Sign-On. Quando si effettua l'accesso a Windows, saranno disponibili due profili: il provider di credenziali interno al sistema e il provider di credenziali di terzi. Le icone di questi profili saranno identiche (vedere la figura seguente). All'utente saranno presentate le seguenti opzioni per continuare:

- Se l'utente seleziona il *provider di credenziali di terzi*, Agente di autenticazione non sarà in grado di sincronizzare la password con l'account Windows. Pertanto, se l'utente ha modificato la password dell'account Windows, Kaspersky Endpoint Security non può aggiornare la password dell'account di Agente di autenticazione. Di conseguenza, l'utente deve eseguire la procedura di autenticazione due volte: nell'interfaccia dell'Agente di Autenticazione e prima di caricare il sistema operativo. In questo caso, l'utente può utilizzare le funzionalità di un provider di credenziali di terzi, ad esempio per l'autenticazione nei servizi aziendali.

- Se l'utente seleziona il *provider di credenziali interno al sistema*, Agente di autenticazione sincronizzerà le password con l'account Windows. In questo caso, l'utente non può utilizzare le funzionalità di un provider di terzi, ad esempio per l'autenticazione nei servizi aziendali.



Profilo di autenticazione di sistema e profilo di autenticazione di terzi per l'accesso a Windows

Gestisci account dell'Agente di Autenticazione

L'Agente di Autenticazione è necessario per utilizzare unità protette mediante la tecnologia Criptaggio disco Kaspersky. Prima del caricamento del sistema operativo, l'utente deve completare l'autenticazione con l'Agente. L'attività *Gestisci account di Agente di Autenticazione* è progettata per la configurazione delle impostazioni di autenticazione degli utenti. È possibile utilizzare attività locali per singoli computer, nonché attività di gruppo per computer di gruppi di amministrazione separati o una selezione di computer.

Non è possibile configurare una pianificazione per l'avvio dell'attività *Gestisci account di Agente di Autenticazione*. È inoltre impossibile interrompere forzatamente un'attività.

Come creare l'attività Gestisci account dell'Agente di Autenticazione in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Gestisci account dell'Agente di Autenticazione**.

Passaggio 2. Selezione di un comando di gestione degli account per l'Agente di Autenticazione

Generare un elenco di comandi di gestione degli account dell'Agente di Autenticazione. I comandi di gestione consentono di aggiungere, modificare ed eliminare gli account dell'Agente di Autenticazione (vedere le istruzioni di seguito). Solo gli utenti che dispongono di un account dell'Agente di Autenticazione possono completare la procedura di autenticazione, caricare il sistema operativo e ottenere l'accesso all'unità criptata.

Passaggio 3. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 4. Definizione del nome dell'attività

Immettere un nome per l'attività, ad esempio *Account amministratore*.

Passaggio 5. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Di conseguenza, dopo il completamento dell'attività al successivo avvio del computer, il nuovo utente può completare la procedura di autenticazione, caricare il sistema operativo e ottenere l'accesso all'unità criptata.

Come creare l'attività Gestisci gli account per l'Agente di Autenticazione in Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.
   Viene aperto l'elenco delle attività.
2. Fare clic su **Aggiungi**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Configurazione delle impostazioni generali dell'attività

Configurare le impostazioni generali dell'attività:

1. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.
2. Nell'elenco a discesa **Tipo di attività**, selezionare **Gestisci account di Agente di Autenticazione**.
3. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Account amministratore*.
4. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

Passaggio 2. Gestione dell'account dell'Agente di Autenticazione

Generare un elenco di comandi di gestione degli account dell'Agente di Autenticazione. I comandi di gestione consentono di aggiungere, modificare ed eliminare gli account dell'Agente di Autenticazione (vedere le istruzioni di seguito). Solo gli utenti che dispongono di un account dell'Agente di Autenticazione possono completare la procedura di autenticazione, caricare il sistema operativo e ottenere l'accesso all'unità criptata.

Passaggio 3. Completamento della creazione dell'attività

Terminare la procedura guidata. Verrà visualizzata una nuova attività nell'elenco delle attività.

Per eseguire un'attività, selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**.

Di conseguenza, dopo il completamento dell'attività al successivo avvio del computer, il nuovo utente può completare la procedura di autenticazione, caricare il sistema operativo e ottenere l'accesso all'unità criptata.

Per aggiungere un account dell'Agente di Autenticazione, è necessario aggiungere un comando speciale all'attività *Gestisci account di Agente di Autenticazione*. Utilizzare un'attività di gruppo è ad esempio utile per aggiungere un account amministratore a tutti i computer.

Kaspersky Endpoint Security consente di creare automaticamente account dell'Agente di Autenticazione prima di criptare un'unità. È possibile abilitare la creazione automatica degli account dell'Agente di Autenticazione nelle impostazioni dei criteri di Criptaggio dell'intero disco. È inoltre possibile utilizzare la tecnologia SSO (Single Sign-On).

Come aggiungere un account dell'Agente di Autenticazione tramite Administration Console (MMC)

1. Aprire le proprietà dell'attività *Gestisci account dell'Agente di Autenticazione*.
2. Nelle proprietà dell'attività, selezionare la sezione **Impostazioni**.
3. Fare clic su **Aggiungi → Comando di aggiunta account**.
4. Nella finestra visualizzata, nel campo **Account di Windows**, specificare il nome dell'account Microsoft Windows che verrà utilizzato per creare l'account dell'Agente di Autenticazione.
5. Se è stato inserito manualmente il nome dell'account Windows, fare clic sul pulsante **Consenti** per definire l'identificatore di sicurezza dell'account (SID).

   Se si sceglie di non determinare il SID facendo clic sul pulsante **Consenti**, il SID verrà determinato al momento dell'esecuzione dell'attività nel computer.

   > Definire un identificatore di sicurezza dell'account Windows è necessario per verificare che il nome dell'account Windows sia stato inserito correttamente. Se l'account Windows non esiste nel computer o nel dominio attendibile, l'attività *Gestisci account dell'Agente di Autenticazione* terminerà con un errore.

6. Selezionare la casella di controllo **Sostituisci account esistente** se si desidera che l'account esistente creato in precedenza per l'Agente di Autenticazione venga sostituito dall'account in fase di creazione.

   > Questo passaggio è disponibile durante l'aggiunta di un comando per la creazione di un account per l'Agente di Autenticazione nelle proprietà di un'attività di gruppo per la gestione degli account per l'Agente di Autenticazione. Questo passaggio è disponibile durante l'aggiunta di un comando per la creazione di un account per l'Agente di Autenticazione nelle proprietà dell'attività locale *Gestisci account dell'Agente di Autenticazione*.

7. Nel campo **Nome utente** digitare il nome dell'account per l'Agente di Autenticazione che deve essere immesso durante l'autenticazione per l'accesso ai dischi rigidi criptati.
8. Selezionare la casella di controllo **Consenti l'autenticazione basata sulla password** se si desidera che l'applicazione richieda all'utente di immettere la password dell'account per l'agente di autenticazione durante l'autenticazione per l'accesso ai dischi rigidi criptati. Impostare una password per l'account dell'Agente di Autenticazione. Se necessario, è possibile richiedere una nuova password all'utente dopo la prima autenticazione.
9. Selezionare la casella di controllo **Consenti l'autenticazione basata sul certificato** se si desidera che l'applicazione richieda all'utente di connettere al computer un token o una smart card durante l'autenticazione per l'accesso ai dischi rigidi criptati. Selezionare un file di certificato per l'autenticazione con una smart card o un token.
10. Se necessario, nel campo **Descrizione del comando** immettere i dettagli sull'account per l'Agente di Autenticazione necessario per la gestione del comando.
11. Nel blocco **Accesso all'autenticazione nell'Agente di Autenticazione**, configurare l'accesso all'autenticazione nell'Agente di Autenticazione per l'utente che utilizza l'account specificato nel comando.
12. Salvare le modifiche.

Come aggiungere un account dell'Agente di Autenticazione tramite Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Gestisci account di Agente di Autenticazione** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Nell'elenco degli account per l'Agente di autenticazione, fare clic sul pulsante **Aggiungi** e selezionare il tipo di comando **Aggiungi account**.

5. Selezionare un account utente. È possibile selezionare un account dall'elenco degli account di dominio o inserire manualmente il nome dell'account. Procedere con il passaggio successivo.

   Kaspersky Endpoint Security determina l'identificatore di sicurezza dell'account (Security Identifier, SID). Questa operazione è necessaria per verificare l'account. Se il nome utente è stato inserito in modo errato, Kaspersky Endpoint Security terminerà l'attività con un errore.

6. Configurare le impostazioni degli account dell'Agente di Autenticazione.

   - **Crea un nuovo account di Agente di Autenticazione per sostituire l'account esistente**. Kaspersky Endpoint Security esamina gli account esistenti nel computer. Se gli ID di sicurezza dell'utente nel computer e nell'attività corrispondono, Kaspersky Endpoint Security modificherà le impostazioni dell'account utente in base all'attività.

   - **Nome utente**. Il nome utente predefinito dell'account dell'Agente di Autenticazione corrisponde al nome di dominio dell'utente.

   - **Consenti autenticazione basata su password**. Impostare una password per l'account dell'Agente di Autenticazione. Se necessario, è possibile richiedere una nuova password all'utente dopo la prima autenticazione. In questo modo, ogni utente avrà una password unica. È inoltre possibile impostare i requisiti di complessità della password per l'account dell'Agente di Autenticazione nel criterio.

   - **Consenti autenticazione basata su certificato**. Selezionare un file di certificato per l'autenticazione con una smart card o un token. In questo modo, l'utente dovrà inserire la password per la smart card o il token.

   - **Accesso dell'account ai dati criptati**. Configurare l'accesso dell'utente all'unità criptata. È ad esempio possibile disabilitare temporaneamente l'autenticazione dell'utente anziché eliminare l'account dell'Agente di Autenticazione.

   - **Commento**. Immettere una descrizione dell'account, se necessario.

7. Salvare le modifiche.

8. Selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**.

   Di conseguenza, dopo il completamento dell'attività al successivo avvio del computer, il nuovo utente può completare la procedura di autenticazione, caricare il sistema operativo e ottenere l'accesso all'unità criptata.

Per modificare la password e altre impostazioni dell'account dell'Agente di Autenticazione, è necessario aggiungere un comando speciale all'attività *Gestisci account di Agente di Autenticazione*. Utilizzare un'attività di gruppo è ad esempio utile per sostituire il certificato token dell'amministratore in tutti i computer.

Come modificare l'account dell'Agente di Autenticazione tramite Administration Console (MMC)

1. Aprire le proprietà dell'attività *Gestisci account dell'Agente di Autenticazione*.
2. Nelle proprietà dell'attività, selezionare la sezione **Impostazioni**.
3. Fare clic su **Aggiungi → Comando di modifica account**.
4. Nella finestra visualizzata, nel campo **Account di Windows**, specificare il nome dell'account utente Microsoft Windows che si desidera modificare.
5. Se è stato inserito manualmente il nome dell'account Windows, fare clic sul pulsante **Consenti** per definire l'identificatore di sicurezza dell'account (SID).

   Se si sceglie di non determinare il SID facendo clic sul pulsante **Consenti**, il SID verrà determinato al momento dell'esecuzione dell'attività nel computer.

   > Definire un identificatore di sicurezza dell'account Windows è necessario per verificare che il nome dell'account Windows sia stato inserito correttamente. Se l'account Windows non esiste nel computer o nel dominio attendibile, l'attività *Gestisci account dell'Agente di Autenticazione* terminerà con un errore.

6. Selezionare la casella di controllo **Cambia nome utente** e immettere un nuovo nome per l'account per l'Agente di Autenticazione se si desidera che Kaspersky Endpoint Security utilizzi il nome digitato nel campo sottostante come nome utente per tutti gli account per l'Agente di Autenticazione creati utilizzando l'account di Microsoft Windows con il nome indicato nel campo **Account di Windows**.
7. Selezionare la casella di controllo **Modifica le impostazioni per l'autenticazione basata sulla password** per rendere modificabili le impostazioni dell'autenticazione basata sulla password.
8. Selezionare la casella di controllo **Consenti l'autenticazione basata sulla password** se si desidera che l'applicazione richieda all'utente di immettere la password dell'account per l'agente di autenticazione durante l'autenticazione per l'accesso ai dischi rigidi criptati. Impostare una password per l'account dell'Agente di Autenticazione.
9. Selezionare la casella di controllo **Modifica la regola di modifica della password al momento dell'autenticazione nell'Agente di Autenticazione** se si desidera che Kaspersky Endpoint Security modifichi il valore dell'impostazione di modifica della password con il valore dell'impostazione specificato di seguito per tutti gli account per l'Agente di Autenticazione creati utilizzando l'account di Microsoft Windows con il nome indicato nel campo **Account di Windows**.
10. Specificare il valore dell'impostazione di modifica della password al momento dell'autenticazione nell'Agente di Autenticazione.
11. Selezionare la casella di controllo **Modifica le impostazioni per l'autenticazione basata sul certificato** per rendere modificabili le impostazioni dell'autenticazione basata sul certificato elettronico di un token o una smart card.
12. Selezionare la casella di controllo **Consenti l'autenticazione basata sul certificato** se si desidera che l'applicazione richieda all'utente di immettere la password nel token o nella smart card connessa al computer durante il processo di autenticazione per l'accesso ai dischi rigidi criptati. Selezionare un file di certificato per l'autenticazione con una smart card o un token.
13. Selezionare la casella di controllo **Modifica la descrizione del comando** e modificare la descrizione del comando se si desidera che Kaspersky Endpoint Security modifichi la descrizione del comando per tutti gli account per l'Agente di Autenticazione creati utilizzando l'account di Microsoft Windows con il nome indicato nel campo **Account di Windows**.

14. Selezionare la casella di controllo **Modifica la regola di accesso all'autenticazione nell'Agente di Autenticazione** se si desidera che Kaspersky Endpoint Security modifichi la regola per l'accesso dell'utente alla finestra di dialogo di autenticazione nell'Agente di Autenticazione con il valore specificato di seguito per tutti gli account per l'Agente di Autenticazione creati utilizzando l'account di Microsoft Windows con il nome indicato nel campo **Account di Windows**.

15. Specificare la regola per l'accesso alla finestra di dialogo di autenticazione nell'Agente di Autenticazione.

16. Salvare le modifiche.

Come modificare l'account dell'Agente di Autenticazione tramite Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Gestisci account di Agente di Autenticazione** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Nell'elenco degli account per l'Agente di autenticazione, fare clic sul pulsante **Aggiungi** e selezionare il tipo di comando **Modifica account**.

5. Selezionare un account utente. È possibile selezionare un account dall'elenco degli account di dominio o inserire manualmente il nome dell'account. Procedere con il passaggio successivo.

   Kaspersky Endpoint Security determina l'identificatore di sicurezza dell'account (Security Identifier, SID). Questa operazione è necessaria per verificare l'account. Se il nome utente è stato inserito in modo errato, Kaspersky Endpoint Security terminerà l'attività con un errore.

6. Selezionare le caselle di controllo accanto alle impostazioni che si desidera modificare.

7. Configurare le impostazioni degli account dell'Agente di Autenticazione.

   - **Crea un nuovo account di Agente di Autenticazione per sostituire l'account esistente**. Kaspersky Endpoint Security esamina gli account esistenti nel computer. Se gli ID di sicurezza dell'utente nel computer e nell'attività corrispondono, Kaspersky Endpoint Security modificherà le impostazioni dell'account utente in base all'attività.

   - **Nome utente**. Il nome utente predefinito dell'account dell'Agente di Autenticazione corrisponde al nome di dominio dell'utente.

   - **Consenti autenticazione basata su password**. Impostare una password per l'account dell'Agente di Autenticazione. Se necessario, è possibile richiedere una nuova password all'utente dopo la prima autenticazione. In questo modo, ogni utente avrà una password unica. È inoltre possibile impostare i requisiti di complessità della password per l'account dell'Agente di Autenticazione nel criterio.

   - **Consenti autenticazione basata su certificato**. Selezionare un file di certificato per l'autenticazione con una smart card o un token. In questo modo, l'utente dovrà inserire la password per la smart card o il token.

   - **Accesso dell'account ai dati criptati**. Configurare l'accesso dell'utente all'unità criptata. È ad esempio possibile disabilitare temporaneamente l'autenticazione dell'utente anziché eliminare l'account dell'Agente di Autenticazione.

   - **Commento**. Immettere una descrizione dell'account, se necessario.

8. Salvare le modifiche.

9. Selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**.

Per eliminare un account dell'Agente di Autenticazione, è necessario aggiungere un comando speciale all'attività *Gestisci account di Agente di Autenticazione*. Utilizzare un'attività di gruppo è ad esempio utile per eliminare l'account di un ex dipendente.

Come eliminare un account dell'Agente di Autenticazione tramite Administration Console (MMC)

1. Aprire le proprietà dell'attività *Gestisci account dell'Agente di Autenticazione*.

2. Nelle proprietà dell'attività, selezionare la sezione **Impostazioni**.

3. Fare clic su **Aggiungi** → **Comando di eliminazione account**.

4. Nel campo **Account di Windows** della finestra visualizzata specificare il nome dell'account utente Windows utilizzato per creare l'account per l'Agente di Autenticazione che si desidera eliminare.

5. Se è stato inserito manualmente il nome dell'account Windows, fare clic sul pulsante **Consenti** per definire l'identificatore di sicurezza dell'account (SID).

   Se si sceglie di non determinare il SID facendo clic sul pulsante **Consenti**, il SID verrà determinato al momento dell'esecuzione dell'attività nel computer.

   > Definire un identificatore di sicurezza dell'account Windows è necessario per verificare che il nome dell'account Windows sia stato inserito correttamente. Se l'account Windows non esiste nel computer o nel dominio attendibile, l'attività *Gestisci account dell'Agente di Autenticazione* terminerà con un errore.

6. Salvare le modifiche.

Come eliminare un account dell'Agente di Autenticazione tramite Web Console

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Gestisci account di Agente di Autenticazione** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Nell'elenco degli account per l'Agente di autenticazione, fare clic sul pulsante **Aggiungi** e selezionare il tipo di comando **Rimuovi account**.

5. Selezionare un account utente. È possibile selezionare un account dall'elenco degli account di dominio o inserire manualmente il nome dell'account.

6. Salvare le modifiche.

7. Selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**.

Di conseguenza, dopo il completamento dell'attività al successivo avvio del computer, l'utente non sarà in grado di completare la procedura di autenticazione e caricare il sistema operativo. Kaspersky Endpoint Security negherà l'accesso ai dati criptati.

Per visualizzare l'elenco degli utenti che possono completare l'autenticazione con l'Agente e caricare il sistema operativo, è necessario accedere alle proprietà del computer gestito.

Come visualizzare l'elenco degli account dell'Agente di Autenticazione tramite Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi**.
3. Fare doppio clic per aprire la finestra delle proprietà del computer.
4. Nella finestra delle proprietà del computer, selezionare la sezione **Attività**.
5. Nell'elenco delle attività, selezionare **Gestisci account dell'Agente di Autenticazione** e aprire le proprietà dell'attività facendo doppio clic.
6. Nelle proprietà dell'attività, selezionare la sezione **Impostazioni**.

Di conseguenza, sarà possibile accedere a un elenco di account dell'Agente di Autenticazione in questo computer. Solo gli utenti dell'elenco possono completare l'autenticazione con l'Agente e caricare il sistema operativo.

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Risorse (dispositivi)**.
2. Fare clic sul nome del computer in cui si desidera visualizzare l'elenco degli account dell'Agente di Autenticazione.
3. Nelle proprietà del computer, selezionare la scheda **Attività**.
4. Nelle proprietà dell'attività, selezionare **Gestisci account di Agente di Autenticazione**.
5. Nelle proprietà dell'attività, selezionare la scheda **Impostazioni applicazione**.

Di conseguenza, sarà possibile accedere a un elenco di account dell'Agente di Autenticazione in questo computer. Solo gli utenti dell'elenco possono completare l'autenticazione con l'Agente e caricare il sistema operativo.

Utilizzo di un token o una smart card con l'agente di autenticazione

È possibile utilizzare un token o una smart card per l'autenticazione durante l'accesso ai dischi rigidi criptati. A tale scopo, è necessario aggiungere il file di certificato elettronico di un token o di una smart card all'attività *Gestisci account dell'Agente di Autenticazione*.

L'utilizzo di un token o di una smart card è disponibile solo se i dischi rigidi del computer sono stati criptati utilizzando l'algoritmo di criptaggio AES256. Se i dischi rigidi del computer sono stati criptati utilizzando l'algoritmo di criptaggio AES56, l'aggiunta del file del certificato elettronico al comando verrà negata.

Kaspersky Endpoint Security supporta i seguenti token, lettori di smart card e smart card:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

Per aggiungere il file del certificato elettronico di un token o di una smart card al comando per la creazione di un account per l'Agente di Autenticazione, è prima necessario salvare il file utilizzando un software di terzi per la gestione dei certificati.

Il certificato del token o della smart card deve avere le seguenti proprietà:

- Il certificato deve essere conforme allo standard X.509 e il file del certificato deve disporre della codifica DER.
- Il certificato contiene una chiave RSA con una lunghezza di almeno 1024 bit.

Se il certificato elettronico del token o della smart card non soddisfa questi requisiti, non è possibile caricare il file del certificato nel comando per la creazione di un account dell'Agente di Autenticazione.

Il parametro `KeyUsage` del certificato deve avere il valore `keyEncipherment` o `dataEncipherment`. Il parametro `KeyUsage` determina lo scopo del certificato. Se il parametro ha un valore diverso, Kaspersky Security Center scaricherà il file del certificato ma visualizzerà un avviso.

Se un utente ha smarrito un token o una smart card, l'amministratore deve aggiungere il file di un token o il certificato elettronico di una smart card al comando per creare un account dell'agente di autenticazione. L'utente deve quindi completare la procedura per l'ottenimento dell'accesso ai dispositivi criptati o il ripristino dei dati nei dispositivi criptati.

Decriptaggio dei dischi rigidi

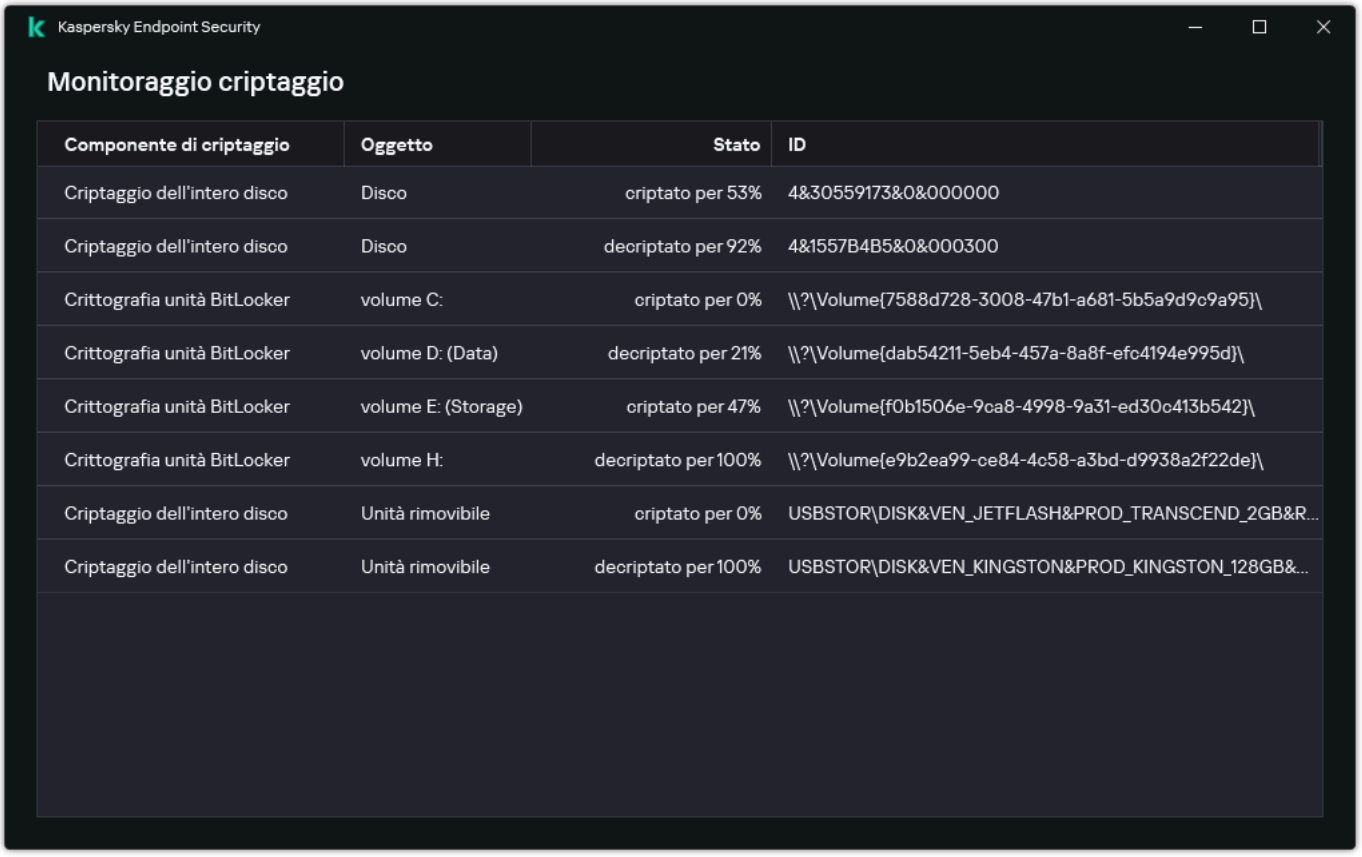
È possibile decriptare i dischi rigidi anche se non è presente una licenza corrente che consente il criptaggio dei dati.

Per decriptare i dischi rigidi:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
4. Nell'elenco a discesa **Tecnologia di criptaggio** selezionare la tecnologia con cui sono stati criptati i dischi rigidi.
5. Eseguire una delle seguenti operazioni:
   - Nell'elenco a discesa **Modalità di criptaggio** selezionare l'opzione **Decripta tutti i dischi rigidi** per decriptare tutti i dischi rigidi.
   - Aggiungere i dischi rigidi criptati che si desidera decriptare alla tabella **Non criptare i seguenti dischi rigidi**.

     Questa opzione è disponibile solo per la tecnologia Criptaggio disco Kaspersky.
6. Salvare le modifiche.

È possibile utilizzare lo strumento Monitoraggio criptaggio per controllare il processo di criptaggio o decriptaggio del disco nel computer di un utente. È possibile eseguire lo strumento Monitoraggio criptaggio dalla finestra principale dell'applicazione.



Monitoraggio criptaggio

Se l'utente arresta o riavvia il computer durante il decriptaggio dei dischi rigidi criptati tramite la tecnologia Criptaggio disco Kaspersky, l'Agente di Autenticazione viene caricato prima del successivo avvio del sistema operativo. Kaspersky Endpoint Security riprende il decriptaggio dei dischi rigidi dopo l'autenticazione tramite l'Agente di Autenticazione e l'avvio del sistema operativo.

Se il sistema operativo entra in modalità di ibernazione durante il decriptaggio dei dischi rigidi criptati tramite la tecnologia Criptaggio disco Kaspersky, l'Agente di Autenticazione viene caricato all'uscita del sistema operativo dalla modalità di ibernazione. Kaspersky Endpoint Security riprende il decriptaggio dei dischi rigidi dopo l'autenticazione tramite l'Agente di Autenticazione e l'avvio del sistema operativo. Dopo il decriptaggio del disco rigido, la modalità di ibernazione non è disponibile fino al primo riavvio del sistema operativo.

Se il sistema operativo entra in modalità di sospensione durante il decriptaggio dei dischi rigidi, Kaspersky Endpoint Security riprende il decriptaggio dei dischi rigidi quando il sistema operativo esce dalla modalità di sospensione, senza caricare l'Agente di Autenticazione.

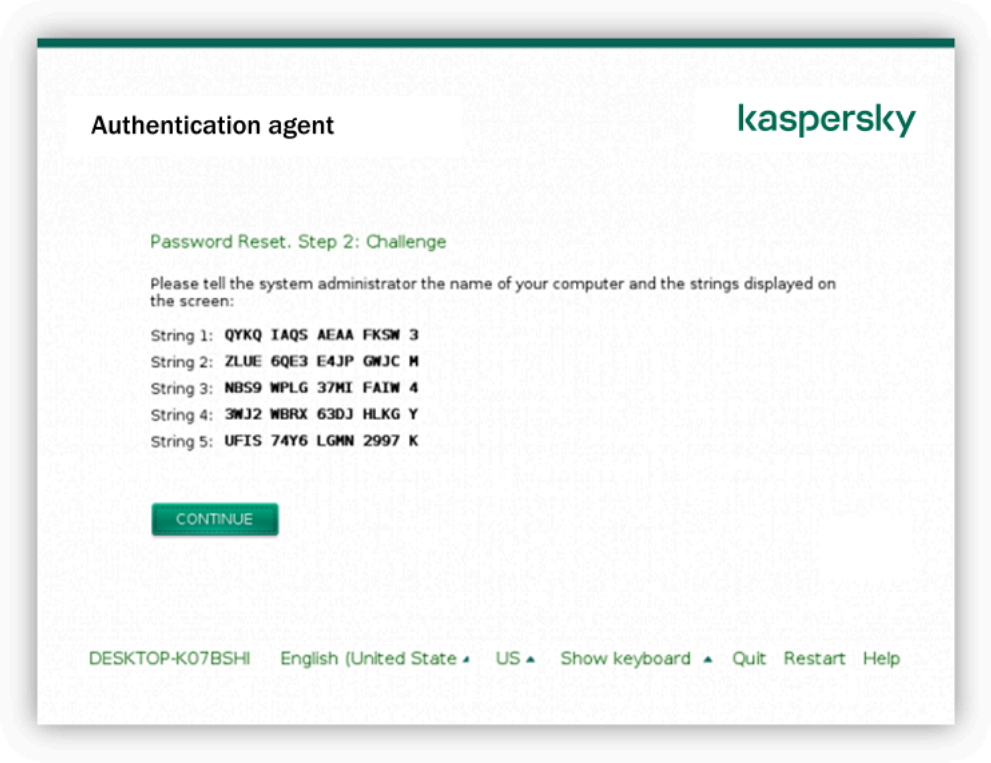
Ripristino dell'accesso a un'unità protetta dalla tecnologia Criptaggio disco Kaspersky

Se un utente ha dimenticato la password per l'accesso a un disco rigido protetto dalla tecnologia Criptaggio disco Kaspersky, è necessario avviare la procedura di ripristino (richiesta-risposta). È inoltre possibile utilizzare l'account di servizio per accedere al disco rigido se questa funzionalità è abilitata nelle impostazioni di criptaggio del disco.

Ripristino dell'accesso al disco rigido di sistema

Il ripristino dell'accesso a un disco rigido di sistema protetto dalla tecnologia Criptaggio disco Kaspersky prevede i seguenti passaggi:

1. L'utente segnala i blocchi della richiesta all'amministratore (vedere la figura seguente).
2. L'amministratore immette i blocchi della richiesta in Kaspersky Security Center, riceve i blocchi della risposta e inoltra i blocchi della risposta all'utente.
3. L'utente immette i blocchi della risposta nell'interfaccia dell'Agente di Autenticazione e ottiene l'accesso al disco rigido.



Ripristino dell'accesso a un disco rigido di sistema protetto dalla tecnologia Criptaggio disco Kaspersky

Per avviare la procedura di ripristino, l'utente deve fare clic sul pulsante **Forgot your password** nell'interfaccia dell'Agente di Autenticazione.

Come ottenere i blocchi della risposta per un disco rigido di sistema protetto dalla tecnologia Criptaggio disco Kaspersky in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi**.
3. Nella scheda **Dispositivi** selezionare il computer dell'utente che richiede l'accesso ai dati criptati, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
4. Nel menu di scelta rapida, selezionare **Concedi l'accesso in modalità offline**.
5. Viene visualizzata una finestra, che consente di selezionare la scheda **Agente di autenticazione**.

6. Nel blocco **Algoritmo di criptaggio in uso**, selezionare un algoritmo di criptaggio: **AES56** o **AES256**.

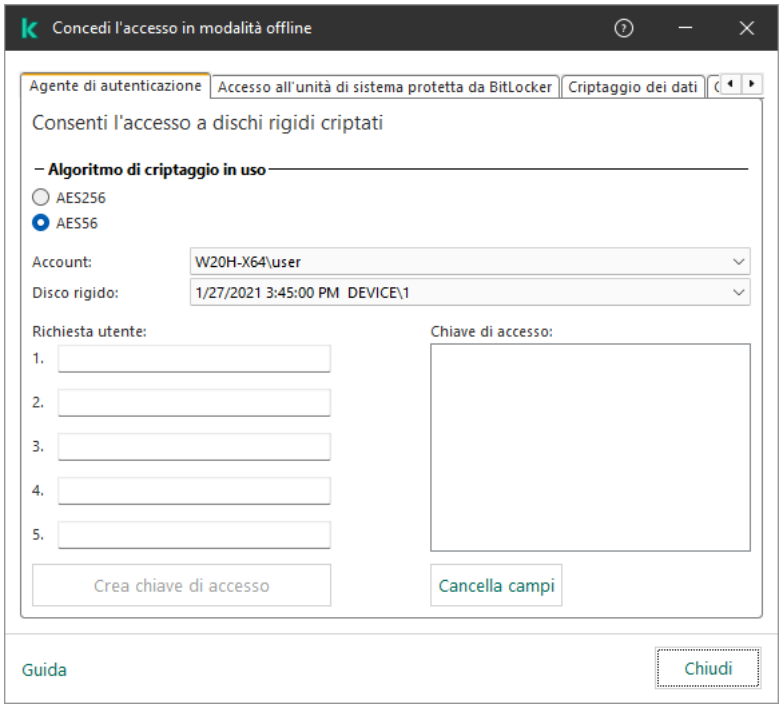
   L'algoritmo di criptaggio dei dati dipende dalla libreria di criptaggio AES inclusa nel pacchetto di distribuzione: *Crittografia avanzata (AES256)* o *Crittografia Lite (AES56)*. La libreria di criptaggio AES viene installata insieme all'applicazione.

7. Nell'elenco a discesa **Account** selezionare il nome dell'account dell'Agente di Autenticazione dell'utente che ha richiesto il ripristino dell'accesso all'unità.

8. Nell'elenco a discesa **Disco rigido** selezionare il disco rigido criptato per cui è necessario ripristinare l'accesso.

9. Nel blocco **Richiesta utente**, immettere le sezioni della richiesta fornite dall'utente.

Di conseguenza, nel campo **Chiave di accesso** verrà visualizzato il contenuto dei blocchi della risposta alla richiesta dell'utente per il ripristino di nome utente e password di un account per l'Agente di Autenticazione. Trasmettere i contenuti dei blocchi della risposta all'utente.



Concessione dell'accesso in modalità offline

Come ottenere i blocchi della risposta per un disco rigido di sistema protetto dalla tecnologia Criptaggio disco Kaspersky in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Risorse (dispositivi)**.

2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso all'unità.

3. Fare clic su **Concedi l'accesso al dispositivo in modalità offline**.

4. Nella finestra visualizzata, selezionare la sezione **Agente di Autenticazione**.

5. Nell'elenco a discesa **Account** selezionare il nome dell'account per l'Agente di Autenticazione creato per l'utente che ha richiesto il ripristino di nome utente e password dell'account per l'Agente di Autenticazione.

6. Immettere i blocchi della richiesta trasmessi dall'utente.

I contenuti dei blocchi della risposta alla richiesta dell'utente di ripristino di nome utente e password dell'account dell'Agente di Autenticazione verranno visualizzati nella parte inferiore della finestra. Trasmettere i contenuti dei blocchi della risposta all'utente.

Al termine della procedura di ripristino, l'Agente di Autenticazione richiederà all'utente di modificare la password.

Ripristino dell'accesso a un disco rigido non di sistema

Il ripristino dell'accesso a un disco rigido non di sistema con la tecnologia Criptaggio disco Kaspersky è composto dai seguenti passaggi:

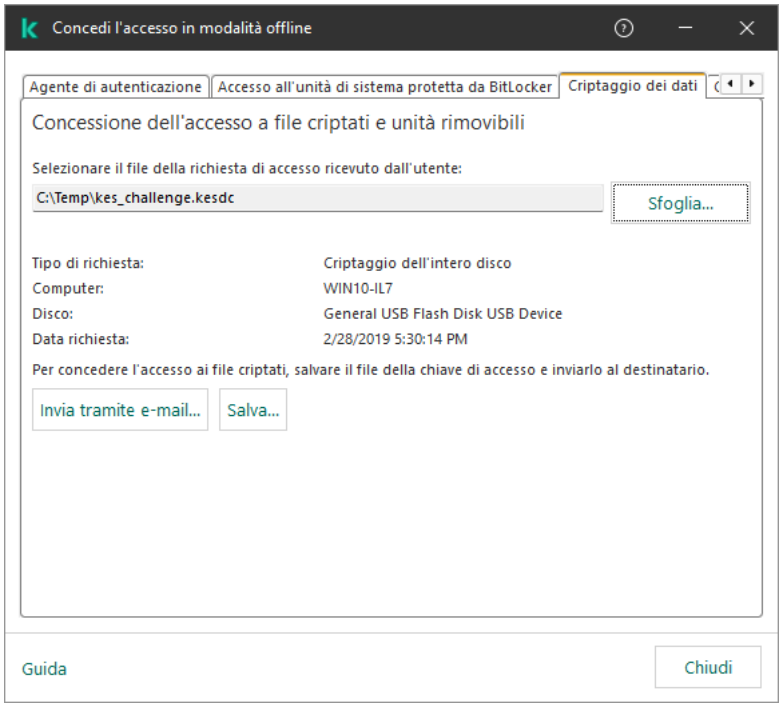
1. L'utente invia un file della richiesta di accesso all'amministratore.
2. L'amministratore aggiunge il file della richiesta di accesso a Kaspersky Security Center, crea un file della chiave di accesso e invia il file all'utente.
3. L'utente aggiunge il file della chiave di accesso a Kaspersky Endpoint Security e ottiene l'accesso al disco rigido.

Per avviare la procedura di ripristino, l'utente deve tentare di accedere a un disco rigido. Di conseguenza, Kaspersky Endpoint Security creerà un file della richiesta di accesso (un file con estensione KESDC), che l'utente deve inviare all'amministratore, ad esempio tramite e-mail.

Come ottenere un file della chiave di accesso per un disco rigido criptato non di sistema in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi**.
3. Nella scheda **Dispositivi** selezionare il computer dell'utente che richiede l'accesso ai dati criptati, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
4. Nel menu di scelta rapida, selezionare **Concedi l'accesso in modalità offline**.
5. Viene visualizzata una finestra, che consente di selezionare la scheda **Criptaggio dei dati**.
6. Nella scheda **Criptaggio dei dati** fare clic sul pulsante **Sfoglia**.
7. Nella finestra per la selezione di un file della richiesta di accesso, specificare il percorso del file ricevuto dall'utente.

Verranno visualizzate le informazioni sulla richiesta dell'utente. Kaspersky Security Center genera un file chiave. Inviare tramite e-mail il file della chiave di accesso ai dati criptati generato all'utente. In alternativa, salvare il file di accesso e utilizzare uno dei metodi disponibili per trasferire il file.



Concessione dell'accesso in modalità offline

Come ottenere un file della chiave di accesso a un disco rigido criptato non di sistema in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso ai dati.
3. Fare clic su **Concedi l'accesso al dispositivo in modalità offline**.
4. Selezionare **Criptaggio dei dati**.
5. Fare clic sul pulsante **Seleziona file** e selezionare il file della richiesta di accesso ricevuto dall'utente (un file con estensione KESDC).

   Web Console visualizzerà le informazioni sulla richiesta. È incluso il nome del computer in cui l'utente richiede l'accesso al file.
6. Fare clic sul pulsante **Salva chiave** e selezionare una cartella per salvare il file della chiave di accesso ai dati criptati (un file con estensione KESDR).

Successivamente, l'utente potrà ottenere la chiave di accesso ai dati criptati, che sarà necessario trasferire all'utente.

Accesso con l'account di servizio dell'Agente di Autenticazione

Kaspersky Endpoint Security consente di aggiungere un account di servizio di Agente di Autenticazione quando si cripta un'unità. L'account di servizio è necessario per accedere al computer, ad esempio quando l'utente dimentica la password. È inoltre possibile utilizzare l'account di servizio come account di riserva. Per aggiungere un account, selezionare un account di servizio in Impostazioni di criptaggio disco e immettere il nome dell'account utente (per impostazione predefinita, `ServiceAccount`). Per autenticarsi utilizzando l'agente, sarà necessaria una password monouso.

Come risalire alla password monouso in Console di amministrazione (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi**.
3. Fare doppio clic per aprire la finestra delle proprietà del computer.
4. Nella finestra delle proprietà del computer, selezionare la sezione **Attività**.
5. Nell'elenco delle attività, selezionare **Gestisci account dell'Agente di Autenticazione** e aprire le proprietà dell'attività facendo doppio clic.
6. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.
7. Nell'elenco degli account, selezionare l'account di servizio di Agente di Autenticazione (ad esempio, `WIN10-USER\ServiceAccount`).
8. Nell'elenco a discesa **Azione**, selezionare **Visualizza account**.
9. Nelle proprietà dell'account, selezionare la casella di controllo **Mostra password originale**.
10. Copiare la password monouso per l'accesso con l'account di servizio.

Come risalire alla password monouso in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Risorse (dispositivi)**.
2. Fare clic sul nome del computer in cui si desidera visualizzare l'elenco degli account dell'Agente di Autenticazione.

   Verranno visualizzate le proprietà del computer.
3. Nelle proprietà del computer, selezionare la scheda **Attività**.
4. Nelle proprietà dell'attività, selezionare **Gestisci account di Agente di Autenticazione**.
5. Nelle proprietà dell'attività, selezionare la scheda **Impostazioni applicazione**.
6. Nell'elenco degli account, selezionare l'account di servizio di Agente di Autenticazione (ad esempio, `WIN10-USER\ServiceAccount`).

7. Nelle proprietà dell'account, selezionare la casella di controllo **Mostra password**.

8. Copiare la password monouso per l'accesso con l'account di servizio.

Kaspersky Endpoint Security aggiorna automaticamente la password ogni volta che un utente si autentica con l'account di servizio. Dopo l'autenticazione tramite l'agente, è necessario immettere la password dell'account Windows. Quando si accede con l'account di servizio, non è possibile utilizzare la tecnologia SSO.

Aggiornamento del sistema operativo

Per l'aggiornamento del sistema operativo di un computer protetto da Criptaggio dell'intero disco sono previste considerazioni speciali. Aggiornare il sistema operativo come segue: aggiornare prima il sistema operativo in un computer, quindi aggiornare il sistema operativo in un numero ridotto di computer, infine aggiornare il sistema operativo in tutti i computer della rete.

Se si utilizza la tecnologia Criptaggio disco Kaspersky, l'Agente di Autenticazione viene caricato prima dell'avvio del sistema operativo. Tramite l'Agente di Autenticazione l'utente può accedere al sistema e ottenere l'accesso alle unità criptate. Viene quindi avviato il caricamento del sistema operativo. Se si avvia un aggiornamento del sistema operativo in un computer protetto tramite la tecnologia Criptaggio disco Kaspersky, la procedura guidata di aggiornamento del sistema operativo rimuoverà l'Agente di Autenticazione. Di conseguenza, il computer può essere bloccato perché il caricatore del sistema operativo non sarà in grado di accedere all'unità criptata.

Funzionalità dell'aggiornamento del sistema operativo:

- **Aggiornamento del sistema operativo tramite WSUS**. È possibile aggiornare il sistema operativo nel solito modo.

- **Aggiornamento del sistema operativo da ISO**. Per aggiornare il sistema operativo, è necessario specificare la cartella con i driver di criptaggio del disco di Kaspersky. L'applicazione copia automaticamente i driver in una cartella separata. Eseguire le seguenti operazioni:

  1. Montare l'immagine ISO.

  2. Avviare l'installazione dell'aggiornamento del sistema con la chiave seguente:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.2\reflect_drivers
     ```

L'aggiornamento automatico del sistema operativo è disponibile solo se nel computer viene eseguito Windows 10 1607 (RS1) o versioni successive. Per eseguire l'upgrade delle versioni precedenti del sistema operativo, è consigliabile decriptare prima il disco, eseguire un upgrade del sistema operativo e quindi criptare il disco.

Se si utilizza la tecnologia Crittografia unità BitLocker, non è necessario decriptare i dischi rigidi per aggiornare Windows 10. Per ulteriori informazioni su BitLocker, visitare il sito Web Microsoft.

Eliminazione degli errori di aggiornamento della funzionalità di criptaggio

Criptaggio dell'intero disco viene aggiornato quando viene eseguito l'upgrade di una versione precedente dell'applicazione a Kaspersky Endpoint Security for Windows 14.2.

Durante l'avvio dell'aggiornamento della funzionalità Criptaggio dell'intero disco possono verificarsi i seguenti errori:

- Impossibile inizializzare l'aggiornamento.
- Il dispositivo è incompatibile con l'Agente di Autenticazione.

Per eliminare gli errori che si verificavano all'avvio del processo di aggiornamento della funzionalità di Criptaggio dell'intero disco nella nuova versione dell'applicazione:

1. Decriptare i dischi rigidi.
2. Criptare nuovamente i dischi rigidi.

Durante l'aggiornamento della funzionalità di Criptaggio dell'intero disco possono verificarsi i seguenti errori:

- Impossibile completare l'aggiornamento.
- Rollback dell'upgrade di Criptaggio dell'intero disco completato con un errore.

Per eliminare gli errori che si sono verificati durante il processo di aggiornamento della funzionalità Criptaggio dell'intero disco,

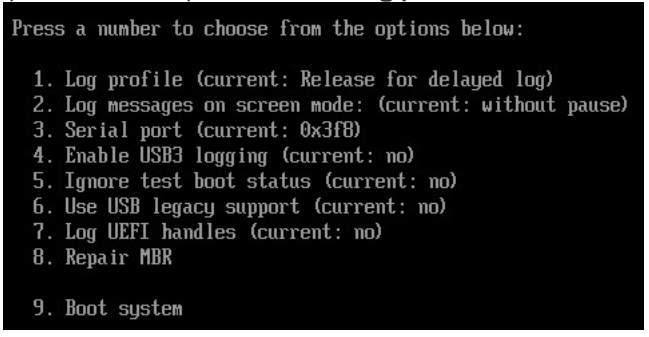
ripristinare l'accesso ai dispositivi criptati utilizzando l'utilità di ripristino.

Tracciamento dell'Agente di Autenticazione

L'applicazione registra informazioni di servizio sull'esecuzione dell'agente di autenticazione e informazioni sulle operazioni dell'utente con l'agente di autenticazione nel file di traccia.

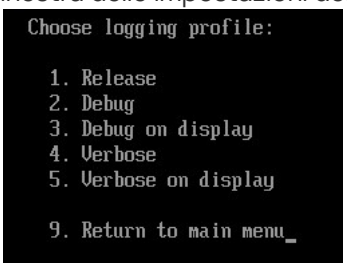
Per abilitare il tracciamento dell'Agente di Autenticazione:

1. Abilitare il tracciamento di Kaspersky Endpoint Security.
2. Riavviare il computer.
3. Non appena viene eseguito l'avvio di un computer con dischi rigidi criptati, premere **F3** per visualizzare una finestra per la configurazione delle impostazioni dell'agente di autenticazione.
4. Dopo l'avvio del caricatore di avvio FDE, selezionare il gestore di avvio **KES (FDE <version>)**.
5. Nel menu del gestore di avvio, passare alle impostazioni di **Log profile**.



Menu del gestore di avvio

6. Selezionare il livello di tracciamento nella finestra delle impostazioni del profilo di registro:



Livelli di traccia dell'agente Agente di Autenticazione

- **Release**. Se questa opzione è selezionata, l'applicazione non registra le informazioni sugli eventi dell'agente di autenticazione nel file di traccia.
- **Debug**. Se questa opzione è selezionata, l'applicazione registra nel file di traccia le informazioni relative all'esecuzione dell'agente di autenticazione e alle operazioni eseguite dall'utente con l'agente di autenticazione.
- **Debug on display**. Se questa opzione è selezionata, l'applicazione registra nel file di traccia le informazioni relative all'esecuzione dell'agente di autenticazione e alle operazioni eseguite dall'utente con l'agente di autenticazione e le trasmette tramite la porta COM.

  Se un computer con dischi rigidi criptati viene connesso a un altro computer tramite la porta COM, è possibile esaminare gli eventi dell'agente di autenticazione dal secondo computer.
- **Verbose**. Se questa opzione è selezionata, l'applicazione registra nel file di traccia informazioni dettagliate relative all'esecuzione dell'agente di autenticazione e alle operazioni eseguite dall'utente con l'agente di autenticazione.

  Il livello di dettaglio delle voci registrate con questa opzione è superiore rispetto al livello dell'opzione **Debug**. Un livello elevato di dettaglio delle voci può rallentare l'avvio dell'agente di autenticazione e del sistema operativo.
- **Verbose on display**. Se questa opzione è selezionata, l'applicazione registra nel file di traccia informazioni dettagliate relative all'esecuzione dell'agente di autenticazione e alle operazioni eseguite dall'utente con l'agente di autenticazione e le trasmette tramite la porta COM.

  Il livello di dettaglio delle voci registrate con questa opzione è superiore rispetto al livello dell'opzione **Debug on display**. Un livello elevato di dettaglio delle voci può rallentare l'avvio dell'agente di autenticazione e del sistema operativo.

Dopo aver selezionato un livello di traccia, il gestore di avvio mostra nuovamente il menu.

7. Nel menu del gestore di avvio, selezionare **Boot system**.

   Il caricatore di avvio FDE avvia l'Agente di Autenticazione.

   Riprodurre il problema.

   I dati vengono registrati nel file di traccia dell'agente di autenticazione se sono presenti dischi rigidi criptati nel computer o durante il criptaggio dell'intero disco.

8. Per interrompere il processo di tracciamento, tornare alla finestra Strumenti di supporto e disabilitare il tracciamento.

Di conseguenza, nella cartella `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` vengono creati file di traccia delle operazioni KES.SRV dell'Agente di Autenticazione. Il file di traccia dell'agente di autenticazione non

viene inviato a Kaspersky, a differenza degli altri file di traccia dell'applicazione. Se necessario, è possibile inviare manualmente il file di traccia dell'agente di autenticazione a Kaspersky per l'analisi.

Modifica del testo della Guida dell'Agente di Autenticazione

Prima di modificare i messaggi della Guida dell'Agente di Autenticazione, consultare l'elenco dei caratteri supportati in un ambiente di preavvio (vedere di seguito).

Per modificare i messaggi della Guida dell'Agente di Autenticazione:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Impostazioni di criptaggio generali**.
4. Nel blocco **Modelli**, fare clic sul pulsante **Guida**.
5. Nella finestra visualizzata, procedere come segue:
   - Selezionare la scheda **Autenticazione** per modificare il testo della Guida visualizzato nella finestra dell'Agente di Autenticazione al momento dell'immissione delle credenziali dell'account.
   - Selezionare la scheda **Cambia password** per modificare il testo della Guida visualizzato nella finestra dell'Agente di Autenticazione al momento della modifica della password dell'account per l'Agente di Autenticazione.
   - Selezionare la scheda **Ripristina password** per modificare il testo della Guida visualizzato nella finestra dell'Agente di Autenticazione al momento del ripristino della password dell'account per l'Agente di Autenticazione.
6. Modificare i messaggi della Guida.

   Se si desidera ripristinare il testo originale, fare clic sul pulsante **Predefinito**.

   È possibile immettere il testo della Guida contenente al massimo 16 righe. La lunghezza massima di una riga è di 64 caratteri.
7. Salvare le modifiche.

Supporto limitato per i caratteri nei messaggi della Guida dell'Agente di Autenticazione

In un ambiente di preavvio, sono supportati i seguenti caratteri Unicode:

- Alfabeto latino base (0000 - 007F)
- Caratteri aggiuntivi latino 1 (0080 - 00FF)
- Latino A esteso (0100 - 017F)

- Latino B esteso (0180 - 024F)
- Caratteri ID estesi non combinati (02B0 - 02FF)
- Segni diacritici combinati (0300 - 036F)
- Alfabeti greco e copto (0370 - 03FF)
- Cirillico (0400 - 04FF)
- Ebraico (0590 - 05FF)
- Script arabo (0600 - 06FF)
- Latino esteso aggiuntivo (1E00 - 1EFF)
- Segni di punteggiatura (2000 - 206F)
- Simboli di valuta (20A0 - 20CF)
- Simboli alfabetici (2100 - 214F)
- Figure geometriche (25A0 - 25FF)
- Moduli di presentazione script arabo B (FE70 - FEFF)

I caratteri che non sono specificati in questo elenco non sono supportati in un ambiente di preavvio. Non è consigliabile utilizzare questi caratteri nei messaggi della Guida dell'Agente di Autenticazione.

Rimozione di oggetti e dati rimanenti dopo aver verificato il funzionamento dell'Agente di Autenticazione

Durante la disinstallazione dell'applicazione, se Kaspersky Endpoint Security rileva oggetti e i dati che sono rimasti sul disco rigido del sistema dopo l'operazione di verifica dell'Agente di Autenticazione, la disinstallazione dell'applicazione viene interrotta e non è possibile completarla finché non si rimuovono tali oggetti e dati.

In seguito all'operazione di verifica dell'Agente di Autenticazione, nei dischi rigidi del sistema possono rimanere oggetti e dati solo in casi eccezionali. Questo può ad esempio avvenire se il computer non è stato riavviato dopo l'applicazione di un criterio di Kaspersky Security Center con impostazioni di criptaggio o in caso di errori nell'avvio dell'applicazione in seguito all'operazione di verifica dell'Agente di Autenticazione.

È possibile rimuovere gli oggetti e i dati rimanenti nel disco rigido del sistema in seguito all'operazione di verifica dell'Agente di Autenticazione nei seguenti modi:

- Utilizzo del criterio di Kaspersky Security Center.
- Utilizzo dell'utilità di ripristino.

Per utilizzare un criterio di Kaspersky Security Center per rimuovere gli oggetti e i dati rimanenti dopo l'operazione di verifica dell'Agente di Autenticazione:

1. Applicare al computer un criterio di Kaspersky Security Center con impostazioni configurate per il decriptaggio di tutti i dischi rigidi del computer.
2. Avviare Kaspersky Endpoint Security.

Per utilizzare l'Utilità di ripristino per rimuovere gli oggetti e i dati rimasti dopo il funzionamento di prova dell'Agente di autenticazione:

1. Eseguire il file denominato fdert.exe, che è il file eseguibile dell'utilità di ripristino. Questo file viene creato da Kaspersky Endpoint Security.
2. Nella finestra Utilità di ripristino, selezionare il dispositivo richiesto.
3. Fare clic su **Esegui scansione**.
4. Se, dopo la diagnosi del disco rigido di sistema, viene visualizzato un messaggio che indica che sono rimasti oggetti e dati dal funzionamento di prova dell'Agente di autenticazione, fare clic su **Elimina oggetti e dati dell'Agente di Autenticazione**.

   Il pulsante **Elimina oggetti e dati dell'Agente di Autenticazione** è disponibile solo se vengono rilevati oggetti e dati rimasti dopo il funzionamento di prova dell'Agente di autenticazione.

Per rimuovere le informazioni sull'incompatibilità dell'applicazione con l'Agente di Autenticazione,

Digitare il comando `avp pbatestreset` nella riga di comando.

BitLocker Management

BitLocker è una tecnologia di criptaggio integrata nei sistemi operativi Windows. Kaspersky Endpoint Security consente di controllare e gestire Bitlocker utilizzando l'infrastruttura Kaspersky Next. BitLocker cripta i volumi logici. BitLocker non può essere utilizzato per il criptaggio delle unità rimovibili. Per informazioni dettagliate su BitLocker, consultare la documentazione di Microsoft.

Quando si cripta il disco, BitLocker inserisce il caricatore di avvio e altri file ausiliari nella system partition. Questa partizione non è criptata. Il sistema operativo crea automaticamente la partizione di sistema durante l'installazione di Windows. Se il disco è completamente partizionato prima dell'installazione di Windows, il sistema operativo non è in grado di creare una partizione di sistema. In questo caso, quando si avvia il criptaggio del disco BitLocker, il sistema operativo richiede all'utente di ripartizionare il disco e creare una partizione di sistema. Dopo la creazione di una partizione di sistema, il sistema operativo avvia il criptaggio BitLocker.

L'algoritmo di criptaggio BitLocker non dipende dalla versione della libreria AES inclusa nel pacchetto di distribuzione (AES256 o AES56). Il criptaggio utilizza la libreria di criptaggio integrata del sistema operativo.

Per impostazione predefinita, l'applicazione utilizza l'algoritmo di criptaggio BitLocker con una lunghezza della chiave effettiva di 256 bit per criptare i dispositivi che non sono mai stati criptati. Per un dispositivo che è stato criptato prima dell'installazione dell'applicazione, l'algoritmo di criptaggio potrebbe essere diverso. Per informazioni dettagliate sulla selezione dell'algoritmo di criptaggio, fare riferimento al sito Web del servizio di assistenza tecnica di Microsoft. A partire dalla versione 12.9, Kaspersky Endpoint Security invia la chiave di ripristino originale per i dispositivi precedentemente criptati da applicazioni di terze parti a Kaspersky Security Center.

BitLocker consente la memorizzazione sicura delle chiavi di accesso utilizzando un Trusted Platform Module. Per *Trusted Platform Module* (TPM) si intende un microchip sviluppato per garantire funzioni di base relative alla sicurezza (ad esempio per archiviare le chiavi di criptaggio). Un Trusted Platform Module viene solitamente installato nella scheda madre del computer e interagisce con tutti gli altri componenti di sistema tramite il bus hardware. L'utilizzo di TPM è il modo più sicuro per memorizzare le chiavi di accesso BitLocker, dal momento che consente la verifica dell'integrità di sistema prima dell'avvio. È comunque possibile criptare le unità in un computer senza un TPM. In questo caso, la chiave di accesso verrà criptata con una password. BitLocker utilizza i seguenti metodi di autenticazione:

- TPM.
- TPM e PIN.
- Password.

Dopo il criptaggio del disco rigido di sistema, l'utente deve eseguire l'autenticazione BitLocker per avviare il sistema operativo. Dopo l'autenticazione, BitLocker consente all'utente di accedere. BitLocker non supporta la tecnologia SSO (Single Sign-On).

Dopo il criptaggio di un'unità, BitLocker crea una chiave di ripristino. Kaspersky Endpoint Security invia la chiave di ripristino a Kaspersky Security Center in modo da poter ripristinare l'accesso al disco, se ad esempio un utente ha dimenticato la propria password.

Se un utente cripta un disco utilizzando BitLocker, Kaspersky Endpoint Security invierà la chiave di ripristino e informazioni sul criptaggio del disco a Kaspersky Security Center.

Se si utilizzano criteri di gruppo Windows, disattivare la gestione BitLocker nelle impostazioni dei criteri. Le impostazioni dei criteri Windows potrebbero entrare in conflitto con le impostazioni dei criteri Kaspersky Endpoint Security. Durante il criptaggio di un'unità, potrebbero verificarsi errori.

Avvio di Crittografia unità BitLocker

Prima di avviare il criptaggio dell'intero disco, è consigliabile verificare che il computer non sia infetto. A tale scopo, avviare l'attività Scansione completa o Scansione delle aree critiche. L'esecuzione del criptaggio dell'intero disco in un computer infetto da un rootkit può rendere inutilizzabile il computer.

Per utilizzare Crittografia unità BitLocker nei computer che eseguono sistemi operativi Windows per server, potrebbe essere necessaria l'installazione del componente Crittografia unità BitLocker. Installare il componente utilizzando gli strumenti del sistema operativo (procedura guidata per l'aggiunta di ruoli e componenti). Per ulteriori informazioni sull'installazione di Crittografia unità BitLocker, consultare la documentazione Microsoft.

Come eseguire Crittografia unità BitLocker tramite Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati → Criptaggio dell'intero disco**.
4. Nell'elenco a discesa **Tecnologia di criptaggio**, selezionare **Crittografia unità BitLocker**.
5. Nell'elenco a discesa **Modalità di criptaggio**, selezionare **Cripta tutti i dischi rigidi**.

   Se nel computer sono installati diversi sistemi operativi, dopo il criptaggio sarà possibile caricare solo il sistema operativo in cui è stato eseguito il criptaggio.

6. Configurare le opzioni avanzate di Crittografia unità BitLocker (vedere la tabella seguente).
7. Salvare le modifiche.

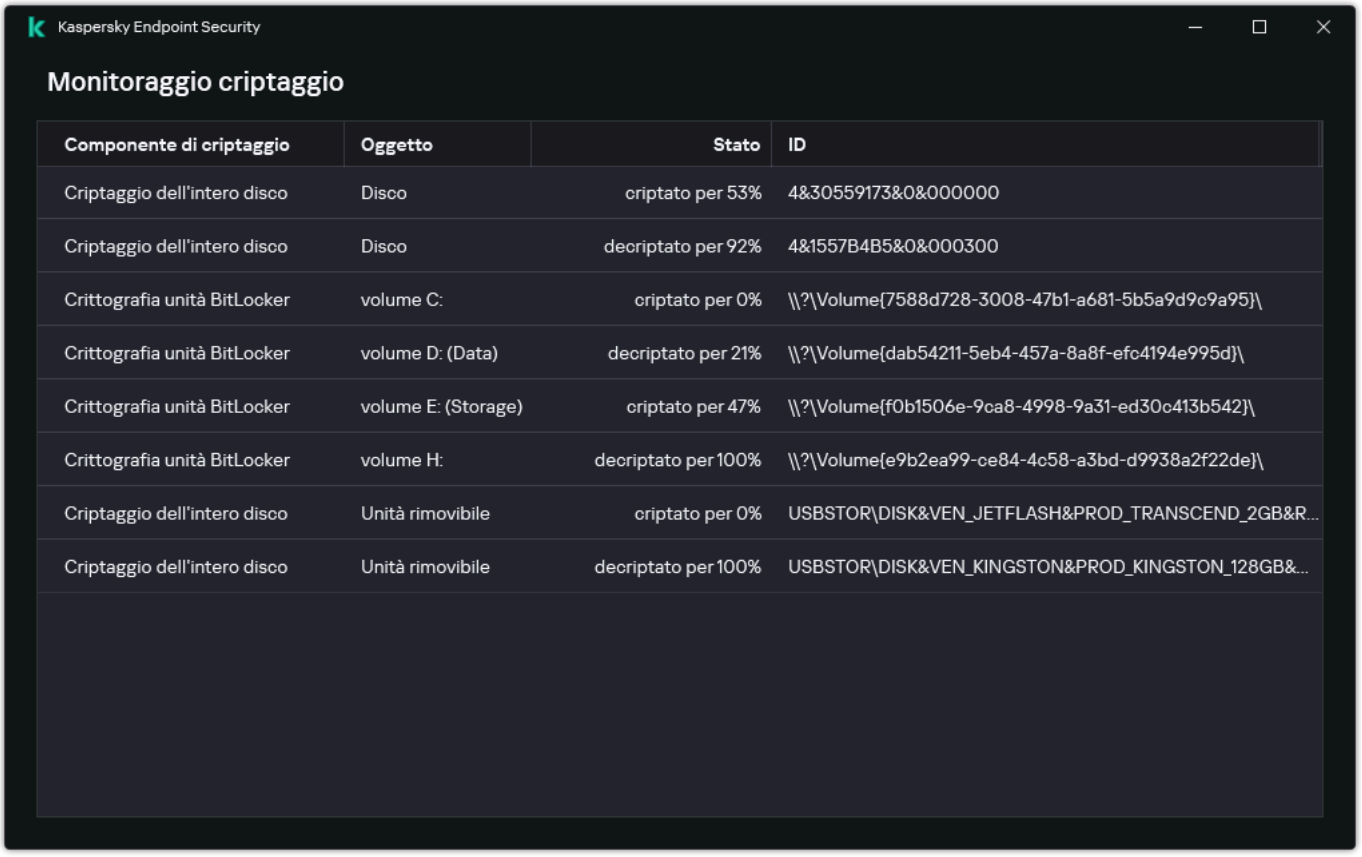
Come eseguire Crittografia unità BitLocker tramite Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Criptaggio dei dati → Criptaggio dell'intero disco**.
5. Selezionare la tecnologia **Criptaggio disco BitLocker**.
6. Nel blocco **Azione sui dispositivi**, selezionare **Cripta tutti i dischi rigidi**.

   Se nel computer sono installati diversi sistemi operativi, dopo il criptaggio sarà possibile caricare solo il sistema operativo in cui è stato eseguito il criptaggio.

7. Configurare le opzioni avanzate di Crittografia unità BitLocker (vedere la tabella seguente).
8. Salvare le modifiche.

È possibile utilizzare lo strumento Monitoraggio criptaggio per controllare il processo di criptaggio o decriptaggio del disco nel computer di un utente. È possibile eseguire lo strumento Monitoraggio criptaggio dalla finestra principale dell'applicazione.



Monitoraggio criptaggio

Dopo aver applicato il criterio, l'applicazione mostrerà le seguenti query, in base alle impostazioni di autenticazione:

- solo TPM. Nessun input richiesto all'utente. Il disco verrà criptato al riavvio del computer.
- TPM + PIN/password. Se è disponibile un modulo TPM, verrà visualizzata una finestra di richiesta del codice PIN. Se non è disponibile un modulo TPM, verrà visualizzata una finestra di richiesta della password per l'autenticazione prima dell'avvio.
- Solo password. Verrà visualizzata una finestra di dialogo di richiesta della password per l'autenticazione del preavvio.

Se è abilitata la modalità di compatibilità Federal Information Processing Standard per il sistema operativo del computer, in Windows 8 e nelle versioni precedenti del sistema operativo verrà visualizzata una richiesta di connessione di un dispositivo di archiviazione per salvare il file della chiave di ripristino. È possibile salvare più file delle chiavi di ripristino in un singolo dispositivo di archiviazione.

Dopo aver impostato una password o un PIN, BitLocker richiederà di riavviare il computer per completare il criptaggio. Successivamente, l'utente deve eseguire la procedura di autenticazione BitLocker. Dopo la procedura di autenticazione, l'utente deve accedere al sistema. Dopo il caricamento del sistema operativo, BitLocker completerà il criptaggio.

Se non è possibile accedere alle chiavi di criptaggio, l'utente può richiedere all'amministratore della rete locale di fornire una chiave di ripristino (nel caso la chiave di ripristino non sia stata salvata in precedenza nel dispositivo di archiviazione o sia andata persa).

Parametro	Descrizione
Consenti l'utilizzo dell'autenticazione BitLocker che richiede l'input da tastiera prima dell'avvio nei tablet	Utilizzo dell'autenticazione che richiede l'input di dati in un ambiente di preavvio, anche se la piattaforma non dispone di funzionalità di input in fase di preavvio (ad esempio, con le tastiere touchscreen nei tablet). Il touchscreen dei computer tablet non è disponibile nell'ambiente di preavvio. Per completare l'autenticazione BitLocker nei computer tablet, l'utente deve connettere ad esempio una tastiera USB. Se la casella di controllo è selezionata, l'utilizzo dell'autenticazione tramite input di preavvio è consentito. È consigliabile utilizzare questa impostazione solo per i dispositivi dotati di strumenti alternativi per l'input dei dati, ad esempio una tastiera USB in aggiunta alle tastiere touchscreen. Se la casella di controllo è deselezionata, Crittografia unità BitLocker non è disponibile nei tablet.
Usa criptaggio hardware (Windows 8 e versioni successive)	Se la casella di controllo è selezionata, l'applicazione applica il criptaggio hardware. Questo consente di aumentare la velocità del criptaggio e di utilizzare meno risorse del computer.
Cripta solo lo spazio su disco utilizzato (Windows 8 e versioni successive)	Questa casella di controllo consente di abilitare o disabilitare l'opzione che limita l'area di criptaggio ai soli settori occupati del disco rigido. Questo limite consente di ridurre il tempo di criptaggio. L'abilitazione o la disabilitazione della funzionalità **Cripta solo lo spazio su disco utilizzato (riduce i tempi di criptaggio)** dopo l'avvio del criptaggio non comporta la modifica di questa impostazione finché i dischi rigidi non vengono decriptati. È necessario selezionare o deselezionare la casella di controllo prima di avviare il criptaggio. Se la casella di controllo è selezionata, vengono criptate solo le parti del disco rigido che sono occupate da file. Kaspersky Endpoint Security cripta automaticamente i nuovi dati man mano che vengono aggiunti. Se la casella di controllo è deselezionata, viene criptato l'intero disco rigido, inclusi i frammenti residui dei file precedentemente eliminati e modificati. Questa opzione è consigliata per i nuovi dischi rigidi in cui non sono stati modificati o eliminati dati. Se si applica il criptaggio a un disco rigido già in uso, è consigliabile criptare l'intero disco rigido. Questo garantisce la protezione di tutti i dati, anche dei dati eliminati potenzialmente ripristinabili. Per impostazione predefinita, la casella di controllo è deselezionata.

Parametro	Descrizione
Metodo di autenticazione	**Solo password (Windows 8 e versioni successive)** Se questa opzione è selezionata, Kaspersky Endpoint Security richiede una password quando si tenta di accedere a un'unità crittografata. Questa opzione può essere selezionata quando non viene utilizzato un Trusted Platform Module (TPM). **Trusted platform module (TPM)** Se questa opzione è selezionata, BitLocker utilizza Trusted Platform Module (TPM). Per *Trusted Platform Module* (TPM) si intende un microchip sviluppato per garantire funzioni di base relative alla sicurezza (ad esempio per archiviare le chiavi di criptaggio). Un Trusted Platform Module in genere è installato nella scheda madre del computer e interagisce con tutti gli altri componenti del sistema tramite il bus hardware. Per i computer che eseguono Windows 7 o Windows Server 2008 R2, è disponibile solo il criptaggio mediante un modulo TPM. Se non è installato un modulo TPM, non è possibile eseguire il criptaggio BitLocker. L'utilizzo di una password in questi computer non è supportato. Un dispositivo dotato di un Trusted Platform Module può creare chiavi di criptaggio che possono essere decriptate solo con il dispositivo. Un Trusted Platform Module cripta le chiavi di criptaggio con la relativa chiave di archiviazione radice. La chiave di archiviazione radice è memorizzata nel Trusted Platform Module. Questo fornisce un livello di protezione aggiuntivo contro i tentativi di violare le chiavi di criptaggio. Questa azione è selezionata per impostazione predefinita. È possibile impostare un ulteriore livello di protezione per l'accesso alla chiave di criptaggio, nonché criptare la chiave con una password o un PIN: • **Usa PIN per TPM**. Se questa casella di controllo è selezionata, è possibile utilizzare un codice PIN per ottenere l'accesso a una chiave di criptaggio archiviata in un Trusted Platform Module (TPM). Se questa casella di controllo è deselezionata, l'utilizzo di codici PIN non è consentito. Per accedere alla chiave di criptaggio, è necessario immettere la password. • **Trusted platform module (TPM) o password se TMP non è disponibile**. Se questa opzione è selezionata, l'utente può utilizzare una password per ottenere l'accesso alle chiavi di criptaggio quando un Trusted Platform Module non è disponibile. Se la casella di controllo è deselezionata e TPM non è disponibile, il criptaggio dell'intero disco non verrà avviato. Il metodo di autenticazione selezionato deve essere configurato specificando i requisiti di password o PIN: • **Lunghezza minima PIN (caratteri)** (il valore predefinito è 6). • **Lunghezza minima password (caratteri)** (il valore predefinito è 8). • **Numero massimo di password/PIN memorizzati** (il valore predefinito è 5). • **Limita periodo di validità password / PIN per TPM (giorni)** (disabilitato per impostazione predefinita). • **Usa PIN avanzato (lettere e numeri)**. *PIN avanzato* consente di utilizzare altri caratteri oltre a quelli numerici: lettere latine maiuscole e minuscole, caratteri speciali e spazi. Disabilitato per impostazione predefinita.
Ricrea automaticamente la chiave di ripristino (giorni)	Aggiorna automaticamente la password per ripristinare l'accesso a un'unità protetta da BitLocker. Se la casella di controllo è selezionata, specificare il periodo di validità della password della chiave di ripristino. In questo modo, si contribuisce a impedire il riutilizzo della password della chiave di ripristino.

Decriptaggio di un disco rigido protetto da BitLocker

Gli utenti possono decriptare un disco utilizzando il sistema operativo (la funzione *Disattiva BitLocker*). Successivamente, Kaspersky Endpoint Security richiederà all'utente di criptare nuovamente il disco. Kaspersky Endpoint Security richiederà di criptare il disco a meno che non si abiliti il decriptaggio del disco nel criterio.

Come decriptare un disco rigido protetto da BitLocker tramite Administration Console (MMC)

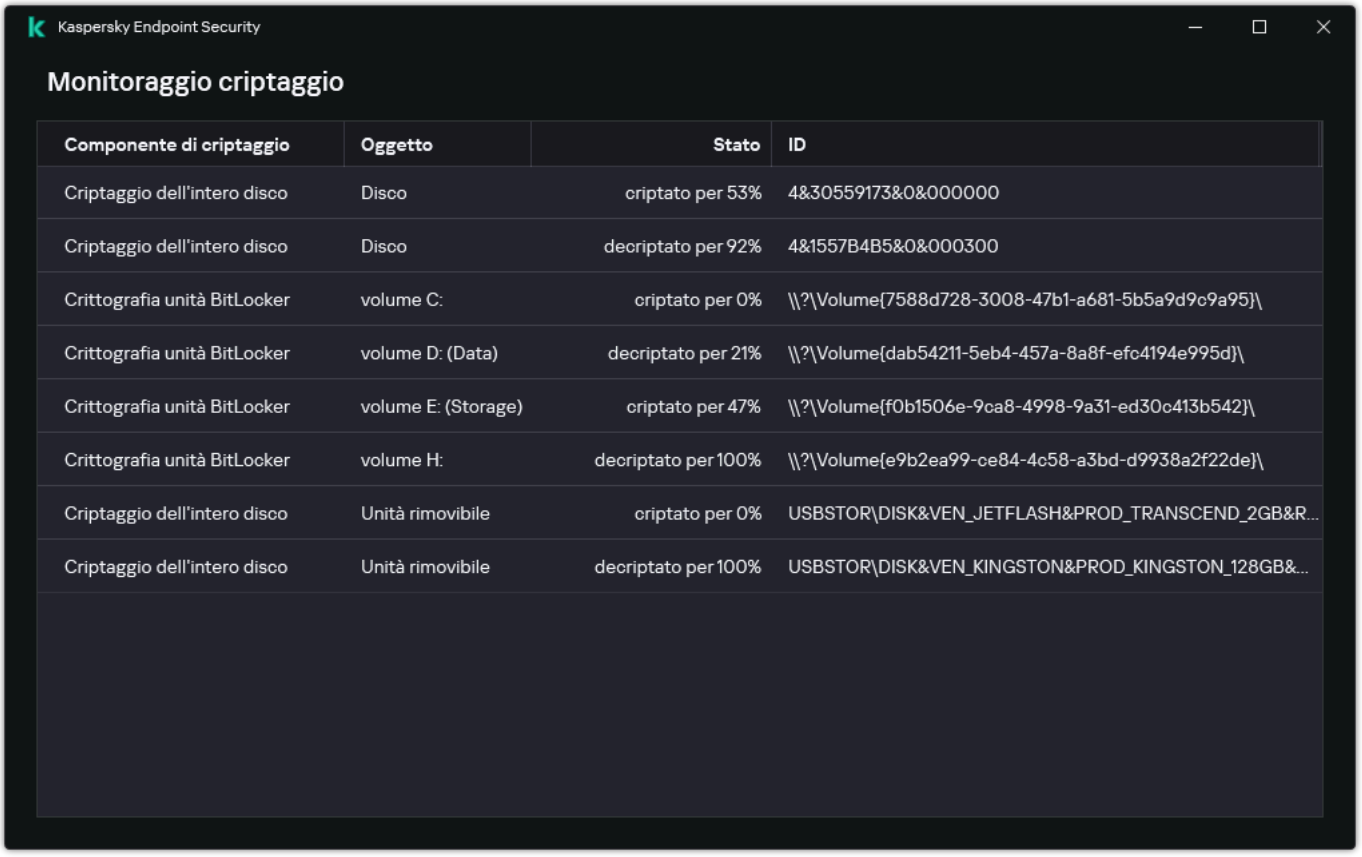
1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati → Criptaggio dell'intero disco**.

4. Nell'elenco a discesa **Tecnologia di criptaggio**, selezionare **Crittografia unità BitLocker**.
5. Nell'elenco a discesa **Modalità di criptaggio**, selezionare **Decripta tutti i dischi rigidi**.
6. Salvare le modifiche.

Come decriptare un disco rigido criptato con BitLocker tramite Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
5. Selezionare la tecnologia **Criptaggio disco BitLocker**.
6. Nel blocco **Azione sui dispositivi**, selezionare **Decripta tutti i dischi rigidi**.
7. Salvare le modifiche.

È possibile utilizzare lo strumento Monitoraggio criptaggio per controllare il processo di criptaggio o decriptaggio del disco nel computer di un utente. È possibile eseguire lo strumento Monitoraggio criptaggio dalla finestra principale dell'applicazione.



Monitoraggio criptaggio

Ripristino dell'accesso a un'unità protetta da BitLocker

Se un utente ha dimenticato la password per l'accesso a un disco rigido criptato con BitLocker, è necessario avviare la procedura di ripristino (richiesta-risposta).

Se nel sistema operativo del computer è abilitata la modalità di compatibilità FIPS (Federal Information Processing Standard), in Windows 8 e versioni precedenti il file della chiave di ripristino viene salvato nell'unità rimovibile prima del criptaggio. Per ripristinare l'accesso all'unità, inserire l'unità rimovibile e seguire le istruzioni visualizzate.

Il ripristino dell'accesso a un disco rigido criptato da BitLocker prevede i seguenti passaggi:

1. L'utente comunica all'amministratore l'ID della chiave di ripristino (vedere la figura seguente).
2. L'amministratore verifica l'ID della chiave di ripristino nelle proprietà del computer in Kaspersky Security Center. L'ID fornito dall'utente deve corrispondere all'ID visualizzato nelle proprietà del computer.
3. Se gli ID della chiave di ripristino corrispondono, l'amministratore fornisce all'utente la chiave di ripristino o invia un file della chiave di ripristino.

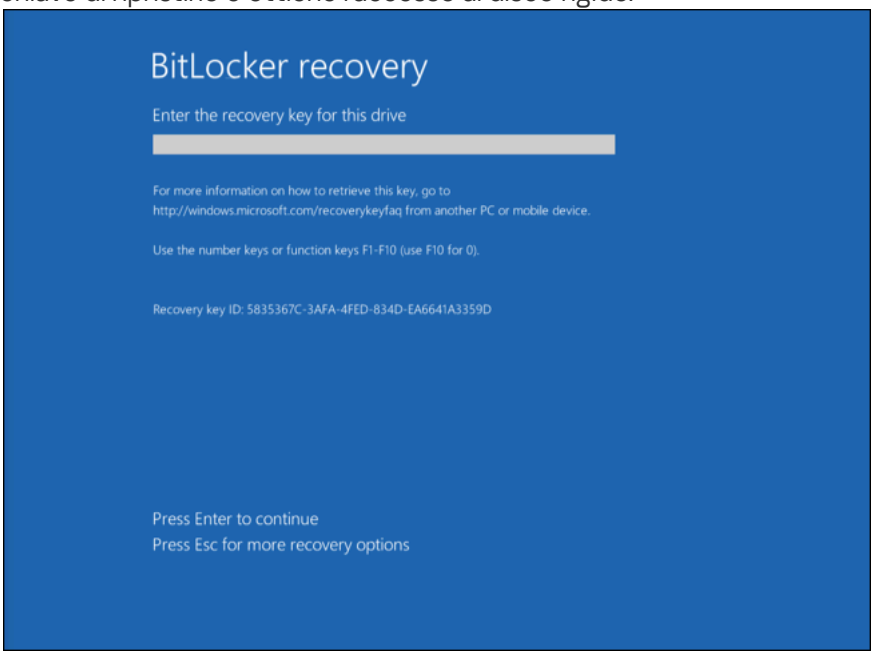
   Un file chiave di ripristino viene utilizzato per i computer che eseguono i seguenti sistemi operativi:

   - Windows 7
   - Windows 8
   - Windows Server 2008;
   - Windows Server 2011;
   - Windows Server 2012;

   Per tutti gli altri sistemi operativi, viene utilizzata una chiave di ripristino.

   Per impedire il riutilizzo della password della chiave di ripristino, è possibile configurare l'aggiornamento automatico della password nelle impostazioni dei criteri.

4. L'utente inserisce la chiave di ripristino e ottiene l'accesso al disco rigido.



Ripristino dell'accesso a un disco rigido criptato da BitLocker

Ripristino dell'accesso a un'unità di sistema

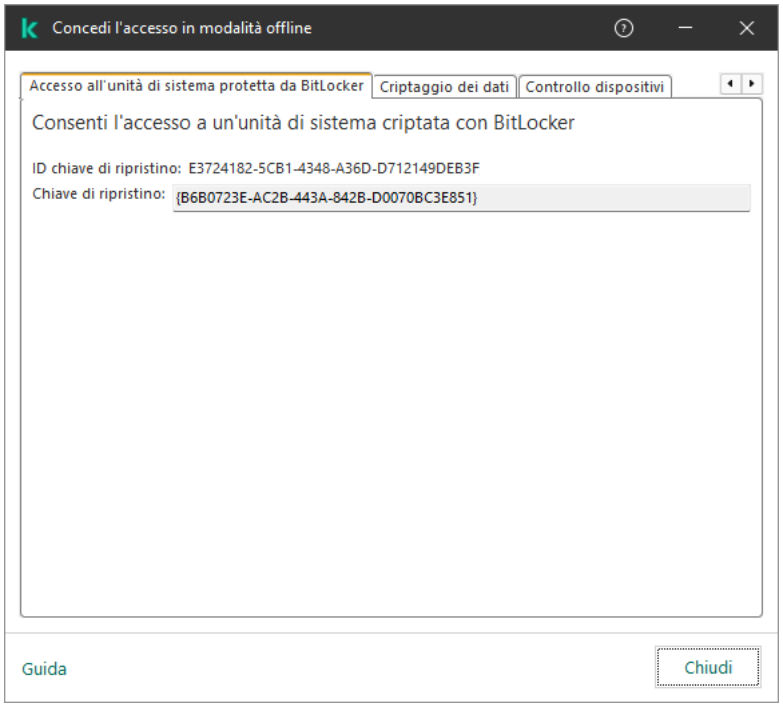
Per avviare la procedura di ripristino, l'utente deve premere il tasto **ESC** nella fase di autenticazione prima dell'avvio.

Come visualizzare la chiave di ripristino per un'unità di sistema criptata da BitLocker in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi gestiti**.
3. Nella scheda **Dispositivi** selezionare il computer dell'utente che richiede l'accesso ai dati criptati, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
4. Nel menu di scelta rapida, selezionare **Concedi l'accesso in modalità offline**.
5. Viene visualizzata una finestra, che consente di selezionare la scheda **Accesso all'unità di sistema protetta da BitLocker**.
6. Richiedere all'utente l'ID della chiave di ripristino indicato nella finestra per l'immissione della password di BitLocker e confrontarlo con l'ID nel campo **ID chiave di ripristino**.

   Se gli ID non corrispondono, la chiave non è valida per ripristinare l'accesso all'unità di sistema specificata. Verificare che il nome del computer selezionato corrisponda al nome del computer dell'utente.

Successivamente, si avrà accesso alla chiave di ripristino o al file della chiave di ripristino, che dovranno essere trasferiti all'utente.



Ripristino dell'accesso a un'unità criptata con BitLocker

Come visualizzare la chiave di ripristino per un'unità di sistema criptata con BitLocker in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso all'unità.
3. Fare clic su **Concedi l'accesso al dispositivo in modalità offline**.
4. Nella finestra visualizzata, selezionare la sezione **BitLocker**.
5. Verificare l'ID della chiave di ripristino. L'ID fornito dall'utente deve corrispondere all'ID visualizzato nelle impostazioni del computer.

   Se gli ID non corrispondono, la chiave non è valida per ripristinare l'accesso all'unità di sistema specificata. Verificare che il nome del computer selezionato corrisponda al nome del computer dell'utente.

6. Fare clic su **Ricevi chiave**.

Successivamente, si avrà accesso alla chiave di ripristino o al file della chiave di ripristino, che dovranno essere trasferiti all'utente.

Dopo il caricamento del sistema operativo, Kaspersky Endpoint Security richiede all'utente di modificare la password o il codice PIN. Dopo aver impostato una nuova password o un nuovo codice PIN, BitLocker creerà una nuova chiave di ripristino e invierà la chiave a Kaspersky Security Center. Di conseguenza, la chiave di ripristino e il file della chiave di ripristino verranno aggiornati. Se l'utente non ha modificato la password, è possibile utilizzare la vecchia chiave di ripristino al successivo caricamento del sistema operativo.

I computer Windows 7 non consentono di modificare la password o il codice PIN. Dopo l'immissione della chiave di ripristino e il caricamento del sistema operativo, Kaspersky Endpoint Security non richiederà all'utente di modificare la password o il codice PIN. È pertanto impossibile impostare una nuova password o un codice PIN. Questo problema deriva dalle caratteristiche specifiche del sistema operativo. Per continuare, è necessario criptare nuovamente il disco rigido.

Ripristino dell'accesso a un'unità non di sistema

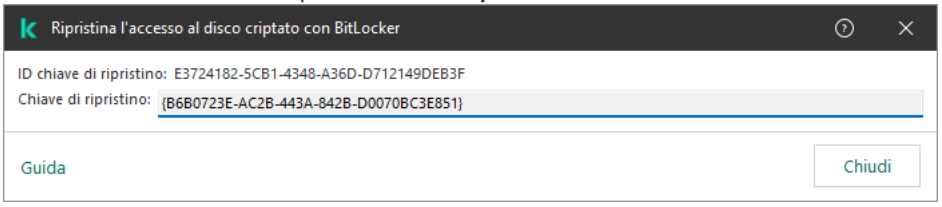
Per avviare la procedura di ripristino, l'utente deve fare clic sul collegamento **Password dimenticata** nella finestra che consente di accedere all'unità. Dopo aver ottenuto l'accesso all'unità criptata, l'utente può abilitare lo sblocco automatico dell'unità durante l'autenticazione di Windows nelle impostazioni di BitLocker.

Come visualizzare la chiave di ripristino per un'unità non di sistema criptata da BitLocker in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura di Administration Console, selezionare la cartella **Avanzate** → **Criptaggio e protezione dei dati** → **Unità criptate**.
3. Nell'area di lavoro selezionare il dispositivo criptato per cui si desidera creare un file chiave di accesso e, nel menu di scelta rapida del dispositivo, fare clic su **Ottieni l'accesso al dispositivo in Kaspersky Endpoint Security**.
4. Richiedere all'utente l'ID della chiave di ripristino indicato nella finestra per l'immissione della password di BitLocker e confrontarlo con l'ID nel campo **ID chiave di ripristino**.

   Se gli ID non corrispondono, la chiave non è valida per ripristinare l'accesso all'unità specificata. Verificare che il nome del computer selezionato corrisponda al nome del computer dell'utente.

5. Inviare all'utente la chiave indicata nel campo **Chiave di ripristino**.



Ripristino dell'accesso a un'unità criptata con BitLocker

Come visualizzare la chiave di ripristino per un'unità non di sistema criptata con BitLocker in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Operazioni → Criptaggio e protezione dei dati → Unità criptate**.
2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso all'unità.
3. Fare clic su **Concedi l'accesso al dispositivo in modalità offline**.

   Viene quindi avviata la procedura guidata per ottenere l'accesso a un dispositivo.
4. Seguire le istruzioni della procedura guidata per concedere l'accesso a un dispositivo:

   a. Selezionare il plug-in **Kaspersky Endpoint Security for Windows**

   b. Verificare l'ID della chiave di ripristino. L'ID fornito dall'utente deve corrispondere all'ID visualizzato nelle impostazioni del computer.

   > Se gli ID non corrispondono, la chiave non è valida per ripristinare l'accesso all'unità di sistema specificata. Verificare che il nome del computer selezionato corrisponda al nome del computer dell'utente.

   c. Fare clic su **Ricevi chiave**.

Successivamente, si avrà accesso alla chiave di ripristino o al file della chiave di ripristino, che dovranno essere trasferiti all'utente.

Sospensione della protezione BitLocker per aggiornare il software

Vi è una serie di considerazioni speciali per l'aggiornamento del sistema operativo, l'installazione di pacchetti di aggiornamento per il sistema operativo o l'aggiornamento di altro software con la protezione BitLocker attivata. L'installazione degli aggiornamenti può richiedere più riavvii del computer. Dopo ogni riavvio, l'utente deve completare l'autenticazione BitLocker. Per accertarsi che gli aggiornamenti vengano installati correttamente, è possibile disattivare temporaneamente l'autenticazione BitLocker. In questo caso, il disco rimane criptato e l'utente può accedere ai dati dopo aver effettuato l'accesso al sistema. Per gestire l'autenticazione BitLocker, è possibile utilizzare l'attività *Gestione della protezione BitLocker*. È possibile utilizzare questa attività per specificare il numero di riavvii del computer che non richiedono l'autenticazione BitLocker. In questo modo, dopo l'installazione degli aggiornamenti e il completamento dell'attività *Gestione della protezione BitLocker*, l'autenticazione BitLocker viene abilitata automaticamente. È possibile abilitare l'autenticazione BitLocker in qualsiasi momento.

Come sospendere la protezione BitLocker tramite Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.
2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Gestione della protezione BitLocker**.

Passaggio 2. Gestione della protezione BitLocker

Configurare l'autenticazione BitLocker. Per sospendere la protezione BitLocker, selezionare **Consenti temporaneamente di ignorare l'autenticazione BitLocker** e immettere il numero di riavvii senza autenticazione BitLocker (da 1 a 15 volte). Se necessario, immettere una data e un'ora di scadenza per l'attività. All'ora specificata, l'attività viene disattivata automaticamente e l'utente deve completare l'autenticazione BitLocker al riavvio del computer.

Passaggio 3. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 4. Definizione del nome dell'attività

Immettere il nome dell'attività, ad esempio *Aggiornamento a Windows 10*.

Passaggio 5. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Come sospendere la protezione BitLocker tramite Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Configurazione delle impostazioni generali dell'attività

Configurare le impostazioni generali dell'attività:

1. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows**.
2. Nell'elenco a discesa **Tipo di attività**, selezionare **Gestione della protezione BitLocker**.
3. Nel campo **Nome attività**, immettere una breve descrizione, ad esempio *Aggiornamento a Windows 10*.
4. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

Passaggio 2. Gestione della protezione BitLocker

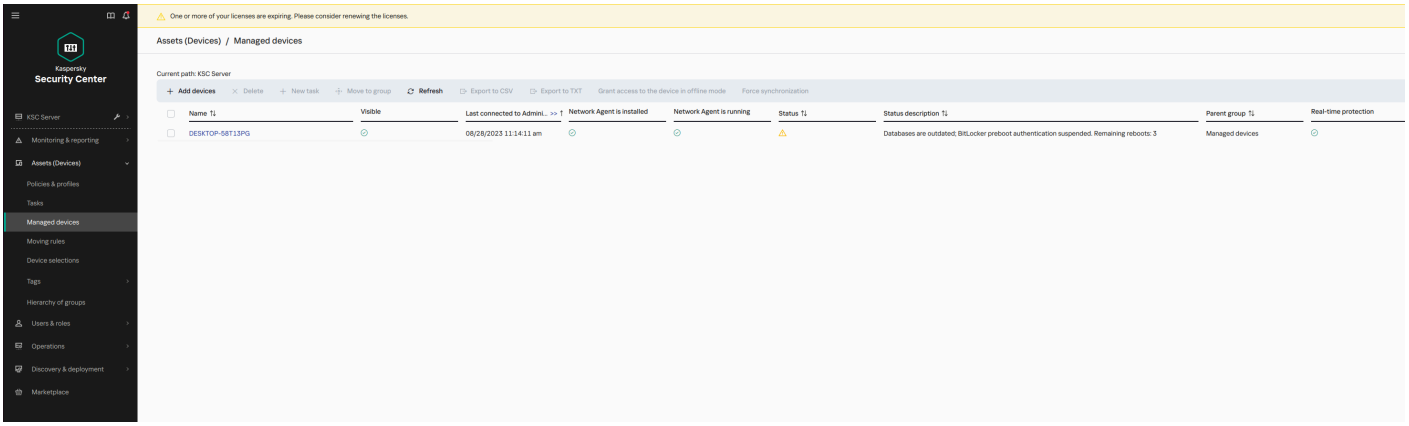
Configurare l'autenticazione BitLocker. Per sospendere la protezione BitLocker, selezionare **Consenti temporaneamente di ignorare l'autenticazione BitLocker** e immettere il numero di riavvii senza autenticazione BitLocker (da 1 a 15 volte). Se necessario, immettere una data e un'ora di scadenza per l'attività. All'ora specificata, l'attività viene disattivata automaticamente e l'utente deve completare l'autenticazione BitLocker al riavvio del computer.

Passaggio 3. Completamento della creazione dell'attività

Terminare la procedura guidata. Verrà visualizzata una nuova attività nell'elenco delle attività.

Per eseguire un'attività, selezionare la casella di controllo accanto all'attività e fare clic sul pulsante **Avvia**.

Di conseguenza, quando l'attività è in esecuzione, dopo il successivo riavvio del computer, BitLocker non richiede l'autenticazione all'utente. Dopo ogni riavvio del computer senza autenticazione BitLocker, Kaspersky Endpoint Security genera un evento corrispondente e registra il numero di riavvii rimanenti. Kaspersky Endpoint Security invia quindi l'evento a Kaspersky Security Center affinché possa essere monitorato dall'amministratore. È inoltre possibile visualizzare il numero di riavvii rimanenti nella cartella **Dispositivi gestiti** della console di Kaspersky Security Center nella descrizione dello stato dei dispositivi.



L'elenco dei dispositivi gestiti

Quando viene raggiunto il numero specificato di riavvii o l'ora di scadenza dell'attività, l'autenticazione BitLocker viene attivata automaticamente. Per accedere ai dati, l'utente deve completare l'autenticazione BitLocker.

Sui computer in cui viene eseguito Windows 7, BitLocker non può conteggiare i riavvii del computer. Il conteggio dei riavvii sui computer Windows 7 è gestito da Kaspersky Endpoint Security. Pertanto, per attivare automaticamente l'autenticazione BitLocker dopo ogni riavvio, è necessario avviare Kaspersky Endpoint Security.

Per attivare l'autenticazione BitLocker in anticipo, aprire le proprietà dell'attività *Gestione della protezione BitLocker* e selezionare **Richiedi autenticazione ogni volta prima dell'avvio**.

Criptaggio a livello di file nelle unità locali del computer

Il criptaggio dei file non è supportato nei computer basati su Arm.

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server.

Il criptaggio dei file presenta le seguenti funzionalità speciali:

- Kaspersky Endpoint Security cripta/decripta i file nelle cartelle predefinite solo per i profili utente locali del sistema operativo. Kaspersky Endpoint Security non cripta o decripta i file nelle cartelle predefinite di profili utente mobili, profili utente bloccati, profili utente temporanei o cartelle reindirizzate.
- Kaspersky Endpoint Security non esegue il criptaggio dei file la cui modifica può danneggiare il sistema operativo e le applicazioni installate. Ad esempio, i seguenti file e cartelle con tutte le cartelle nidificate sono inclusi nell'elenco delle esclusioni di criptaggio:
  - %WINDIR%;
  - %PROGRAMFILES% e %PROGRAMFILES(X86)%;
  - File del Registro di sistema di Windows.

  L'elenco delle esclusioni di criptaggio non può essere visualizzato o modificato. Anche se i file e le cartelle presenti nell'elenco delle esclusioni di criptaggio possono essere aggiunti all'elenco di criptaggio, non verranno criptati durante il criptaggio dei file.

Criptaggio dei file nelle unità locali del computer

Kaspersky Endpoint Security non cripta i file che si trovano nell'archivio cloud di OneDrive o in altre cartelle con OneDrive come nome. Kaspersky Endpoint Security blocca inoltre la copia dei file criptati nelle cartelle OneDrive se tali file non vengono aggiunti alla regola di decriptaggio.

Per criptare i file nelle unità locali:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati → Criptaggio a livello di file**.
4. Nell'elenco a discesa **Modalità di criptaggio**, selezionare **In base alle regole**.
5. Nella scheda **Criptaggio** fare clic sul pulsante **Aggiungi** e selezionare uno dei seguenti elementi nell'elenco a discesa:

   a. Selezionare l'elemento **Cartelle predefinite** per aggiungere a una regola di criptaggio i file nelle cartelle dei profili utente locali suggeriti dagli esperti di Kaspersky.

   - **Documenti**. File nella cartella *Documenti* standard del sistema operativo e relative sottocartelle.
   - **Preferiti**. File nella cartella *Preferiti* standard del sistema operativo e relative sottocartelle.
   - **Desktop**. File nella cartella *Desktop* standard del sistema operativo e relative sottocartelle.
   - **File temporanei**. File temporanei relativi all'esecuzione delle applicazioni installate nel computer. Le applicazioni di Microsoft Office creano ad esempio file temporanei contenenti copie di backup dei documenti.

     Non è consigliabile criptare i file temporanei, poiché può causare perdite di dati. Ad esempio, Microsoft Word crea file temporanei durante l'elaborazione di un documento. Se i file temporanei sono criptati, ma il file originale non lo è, l'utente potrebbe ricevere un errore *Accesso negato* durante il tentativo di salvataggio del documento. Inoltre, Microsoft Word potrebbe salvare il file, ma non sarà possibile aprire il documento la volta successiva, ovvero i dati andranno persi.

   - **File di Outlook**. File relativi all'esecuzione del client di posta di Outlook: file di dati (PST), file di dati offline (OST), file della rubrica offline (OAB) e file della rubrica personale (PAB).

   b. Selezionare l'elemento **Cartella personalizzata** per aggiungere a una regola di criptaggio il percorso di una cartella immesso manualmente.

   Quando si aggiunge il percorso di una cartella, attenersi alle seguenti regole:

   - Utilizzare una variabile di ambiente (ad esempio `%FOLDER%\UserFolder\`). È possibile utilizzare una variabile di ambiente solo una volta e solo all'inizio del percorso.
   - Non utilizzare percorsi relativi.
   - Non utilizzare i caratteri `*` e `?`.
   - Non utilizzare percorsi UNC.
   - Utilizzare `;` o `,` come carattere separatore.

c. Selezionare l'elemento **File per estensione** per aggiungere singole estensioni di file a una regola di criptaggio. Kaspersky Endpoint Security cripta i file con le estensioni specificate in tutte le unità locali del computer.

d. Selezionare l'elemento **File per gruppi di estensioni** per aggiungere gruppi di estensioni di file a una regola di criptaggio (ad esempio *Documenti di Microsoft Office*). Kaspersky Endpoint Security cripta i file con le estensioni elencate nei gruppi di estensioni in tutte le unità locali del computer.

6. Salvare le modifiche.

Non appena il criterio viene applicato, Kaspersky Endpoint Security cripta i file inclusi nella regola di criptaggio e non inclusi nella regola di decriptaggio.

Il criptaggio dei file presenta le seguenti funzionalità speciali:

- Se lo stesso file viene aggiunto sia a una regola di criptaggio che a una regola di decriptaggio, Kaspersky Endpoint Security esegue le seguenti azioni:
  - Se il file non è criptato, Kaspersky Endpoint Security non cripta il file.
  - Se il file è criptato, Kaspersky Endpoint Security decripta il file.
- Kaspersky Endpoint Security continua a criptare i nuovi file se questi file soddisfano i criteri della regola di criptaggio. Quando ad esempio si modificano le proprietà di un file non criptato (percorso o estensione), il file soddisfa i criteri della regola di criptaggio. Kaspersky Endpoint Security cripta il file.
- Quando l'utente crea un nuovo file le cui proprietà soddisfano i criteri della regola di criptaggio, Kaspersky Endpoint Security cripta il file non appena viene aperto.
- Kaspersky Endpoint Security rimanda il criptaggio dei file aperti finché non vengono chiusi.
- Se si sposta un file criptato in un'altra cartella nell'unità locale, il file resta criptato indipendentemente dal fatto che la cartella sia inclusa o meno nella regola di criptaggio.
- Se si decripta un file e lo si copia in un'altra cartella locale che non è inclusa nella regola di decriptaggio, una copia del file potrebbe essere criptata. Per evitare che il file copiato venga criptato, creare una regola di decriptaggio per la cartella di destinazione.

Creazione delle regole di accesso ai file criptati per le applicazioni

Per impostazione predefinita, tutte le applicazioni funzionano con i file criptati in uno stato decriptato. Se si utilizzano spesso determinate applicazioni (ad esempio browser o editor di testo), è possibile creare regole di accesso ai file criptati per proteggere le informazioni.

È consigliabile creare una regola di accesso ai file criptati per i browser Microsoft Internet Explorer e Microsoft Edge. Per via del funzionamento di questi browser, se si carica un file criptato in un sito Web (ad esempio un archivio cloud), il file viene automaticamente decriptato. Ciò può causare una fuga di dati. Non è possibile caricare un file criptato utilizzando questi browser. È consigliabile impostare la regola **Concedi l'accesso ai file criptati solo in testo criptato**. Non è necessario creare una regola per altri browser (ad esempio Google Chrome).

Per creare le regole di accesso ai file criptati per le applicazioni:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati → Criptaggio a livello di file**.
4. Nell'elenco a discesa **Modalità di criptaggio**, selezionare **In base alle regole**.

   Le regole di accesso sono applicate solo nella modalità **In base alle regole**. Dopo avere applicato le regole di accesso nella modalità **In base alle regole**, se si passa alla modalità **Mantieni invariato** Kaspersky Endpoint Security ignorerà tutte le regole di accesso. Tutte le applicazioni avranno accesso a tutti i file criptati.

5. Nella parte destra della finestra selezionare la scheda **Regole per le applicazioni**.
6. Se si desidera selezionare le applicazioni esclusivamente dall'elenco di Kaspersky Security Center, fare clic sul pulsante **Aggiungi** e selezionare nell'elenco a discesa l'elemento **Applicazioni dall'elenco di Kaspersky Security Center**.

   a. Specificare i filtri per restringere l'elenco delle applicazioni nella tabella. A tale scopo, specificare i valori dei parametri **Applicazione**, **Produttore** e **Periodo di aggiunta** e tutte le caselle di controllo nel blocco **Gruppo**.

   b. Fare clic su **Aggiorna**.

   c. Nella tabella verranno elencate le applicazioni che corrispondono ai filtri applicati.

   d. Nella colonna **Applicazione**, selezionare le caselle di controllo accanto alle applicazioni per cui si desidera creare le regole di accesso ai file criptati.

   e. Nell'elenco a discesa **Regola per le applicazioni** selezionare la regola che determinerà l'accesso delle applicazioni ai file criptati.

   f. Nell'elenco a discesa **Azioni per le applicazioni selezionate in precedenza** selezionare l'azione che deve essere eseguita da Kaspersky Endpoint Security sulle regole di accesso ai file criptati create in precedenza per tali applicazioni.

   I dettagli di una regola di accesso ai file criptati per le applicazioni vengono visualizzati nella tabella nella scheda **Regole per le applicazioni**.

7. Se si desidera selezionare manualmente le applicazioni, fare clic sul pulsante **Aggiungi** e selezionare nell'elenco a discesa l'elemento **Applicazioni personalizzate**.

   a. Nel campo di immissione digitare il nome o un elenco di nomi di file eseguibili delle applicazioni con le relative estensioni.

   È anche possibile aggiungere i nomi dei file eseguibili delle applicazioni dall'elenco di Kaspersky Security Center facendo clic sul pulsante **Aggiungi dall'elenco di Kaspersky Security Center**.

   b. Se necessario, nel campo **Descrizione** immettere una descrizione dell'elenco di applicazioni.

   c. Nell'elenco a discesa **Regola per le applicazioni** selezionare la regola che determinerà l'accesso delle applicazioni ai file criptati.

I dettagli di una regola di accesso ai file criptati per le applicazioni vengono visualizzati nella tabella nella scheda **Regole per le applicazioni**.

8. Salvare le modifiche.

Criptaggio dei file creati o modificati da applicazioni specifiche

È possibile creare una regola in base alla quale Kaspersky Endpoint Security cripterà tutti i file creati o modificati dalle applicazioni specificate nella regola.

I file che sono stati creati o modificati dalle applicazioni specificate prima dell'applicazione della regola di criptaggio non saranno criptati.

Per configurare il criptaggio dei file creati o modificati da applicazioni specifiche:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio a livello di file**.
4. Nell'elenco a discesa **Modalità di criptaggio**, selezionare **In base alle regole**.

   Le regole di criptaggio sono applicate solo nella modalità **In base alle regole**. Dopo avere applicato le regole di criptaggio nella modalità **In base alle regole**, se si passa alla modalità **Mantieni invariato**, Kaspersky Endpoint Security ignorerà tutte le regole di criptaggio. I file che sono stati criptati in precedenza rimarranno criptati.

5. Nella parte destra della finestra selezionare la scheda **Regole per le applicazioni**.
6. Se si desidera selezionare le applicazioni esclusivamente dall'elenco di Kaspersky Security Center, fare clic sul pulsante **Aggiungi** e selezionare nell'elenco a discesa l'elemento **Applicazioni dall'elenco di Kaspersky Security Center**.

   a. Specificare i filtri per restringere l'elenco delle applicazioni nella tabella. A tale scopo, specificare i valori dei parametri **Applicazione**, **Produttore** e **Periodo di aggiunta** e tutte le caselle di controllo nel blocco **Gruppo**.

   b. Fare clic su **Aggiorna**.

   Nella tabella verranno elencate le applicazioni che corrispondono ai filtri applicati.

   c. Nella colonna **Applicazione**, selezionare le caselle di controllo accanto alle applicazioni di cui si desidera criptare i file creati.

   d. Nell'elenco a discesa **Regola per le applicazioni**, selezionare **Cripta tutti i file creati**.

   e. Nell'elenco a discesa **Azioni per le applicazioni selezionate in precedenza** selezionare l'azione che deve essere eseguita da Kaspersky Endpoint Security sulle regole di criptaggio dei file create in precedenza per tali applicazioni.

Le informazioni sulla regola di criptaggio per i file creati o modificati dalle applicazioni selezionate vengono visualizzate nella tabella contenuta nella scheda **Regole per le applicazioni**.

7. Se si desidera selezionare manualmente le applicazioni, fare clic sul pulsante **Aggiungi** e selezionare nell'elenco a discesa l'elemento **Applicazioni personalizzate**.

   a. Nel campo di immissione digitare il nome o un elenco di nomi di file eseguibili delle applicazioni con le relative estensioni.

      È anche possibile aggiungere i nomi dei file eseguibili delle applicazioni dall'elenco di Kaspersky Security Center facendo clic sul pulsante **Aggiungi dall'elenco di Kaspersky Security Center**.

   b. Se necessario, nel campo **Descrizione** immettere una descrizione dell'elenco di applicazioni.

   c. Nell'elenco a discesa **Regola per le applicazioni**, selezionare **Cripta tutti i file creati**.

   Le informazioni sulla regola di criptaggio per i file creati o modificati dalle applicazioni selezionate vengono visualizzate nella tabella contenuta nella scheda **Regole per le applicazioni**.

8. Salvare le modifiche.

Generazione di una regola di decriptaggio

Per generare una regola di decriptaggio:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio a livello di file**.
4. Nell'elenco a discesa **Modalità di criptaggio**, selezionare **In base alle regole**.
5. Nella scheda **Decriptaggio** fare clic sul pulsante **Aggiungi** e selezionare uno dei seguenti elementi nell'elenco a discesa:

   a. Selezionare l'elemento **Cartelle predefinite** per aggiungere a una regola di decriptaggio i file nelle cartelle dei profili utente locali suggeriti dagli esperti di Kaspersky.

   b. Selezionare l'elemento **Cartella personalizzata** per aggiungere a una regola di decriptaggio il percorso di una cartella immesso manualmente.

   c. Selezionare l'elemento **File per estensione** per aggiungere singole estensioni di file a una regola di decriptaggio. Kaspersky Endpoint Security non cripta i file con le estensioni specificate in tutte le unità locali del computer.

   d. Selezionare l'elemento **File per gruppi di estensioni** per aggiungere gruppi di estensioni di file a una regola di decriptaggio (ad esempio *Documenti di Microsoft Office*). Kaspersky Endpoint Security non cripta i file con le estensioni elencate nei gruppi di estensioni in tutte le unità locali del computer.

6. Salvare le modifiche.

Se lo stesso file è stato aggiunto sia alla regola di criptaggio che alla regola di decriptaggio, Kaspersky Endpoint Security non cripta il file se non è criptato e decripta il file se è criptato.

Decriptaggio dei file nelle unità locali del computer

Per decriptare i file nelle unità locali:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio a livello di file**.
4. Nella parte destra della finestra selezionare la scheda **Criptaggio**.
5. Rimuovere i file e le cartelle che si desidera decriptare dall'elenco di criptaggio. A tale scopo, selezionare i file, quindi scegliere **Elimina la regola e decripta i file** dal menu di scelta rapida del pulsante **Elimina**.

   I file e le cartelle rimossi dall'elenco di criptaggio vengono automaticamente aggiunti all'elenco di decriptaggio.
6. Creare un elenco di decriptaggio dei file.
7. Salvare le modifiche.

Non appena viene applicato il criterio, Kaspersky Endpoint Security decripta i file criptati aggiunti all'elenco di decriptaggio.

Kaspersky Endpoint Security decripta i file criptati se i relativi parametri (percorso del file / nome del file / estensione del file) cambiano in modo da corrispondere ai parametri degli oggetti aggiunti all'elenco di decriptaggio.

Kaspersky Endpoint Security rimanda il decriptaggio dei file aperti finché non vengono chiusi.

Creazione di pacchetti criptati

Per proteggere i dati quando si inviano file a utenti esterni alla rete aziendale, è possibile utilizzare pacchetti criptati. I pacchetti criptati possono essere utili per il trasferimento di file di grandi dimensioni su unità rimovibili, in quanto i client e-mail presentano restrizioni sulla dimensione dei file.

Prima di creare pacchetti criptati, Kaspersky Endpoint Security richiederà all'utente una password. Per proteggere i dati in modo affidabile, è possibile abilitare il controllo della sicurezza delle password e specificare i requisiti di sicurezza delle password. In questo modo, si impedirà agli utenti di utilizzare password brevi e semplici, ad esempio `1234`.

Come abilitare il controllo della sicurezza delle password durante la creazione degli archivi criptati in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Impostazioni di criptaggio generali**.
4. Nel blocco **Impostazioni password**, fare clic sul pulsante **Impostazioni**.

5. Viene visualizzata una finestra, che consente di selezionare la scheda **Pacchetti criptati**.

6. Configurare le impostazioni di complessità delle password durante la creazione di pacchetti criptati.

Come abilitare il controllo della sicurezza delle password durante la creazione degli archivi criptati in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

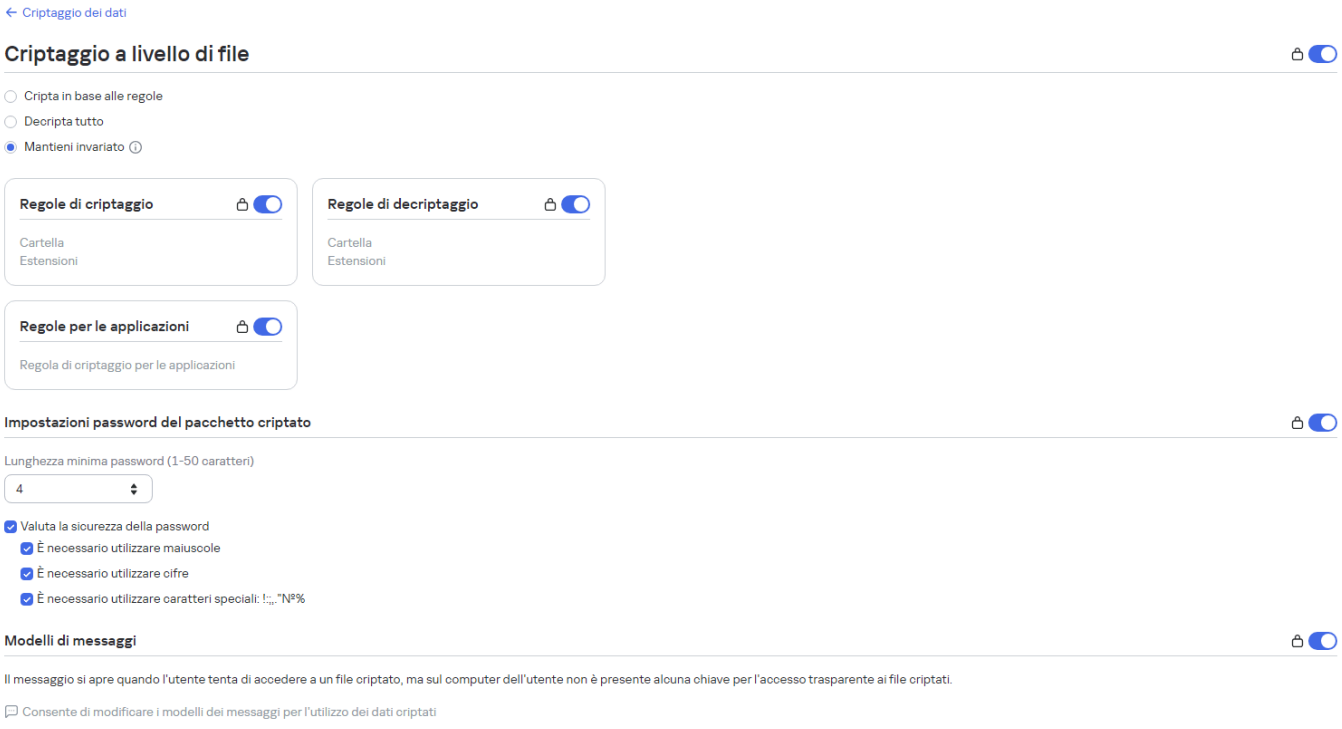
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Criptaggio dei dati** → **Criptaggio a livello di file**.

5. Nel blocco **Impostazioni password del pacchetto criptato**, configurare i criteri di complessità della password richiesti durante la creazione di pacchetti criptati.



Impostazioni di Criptaggio file

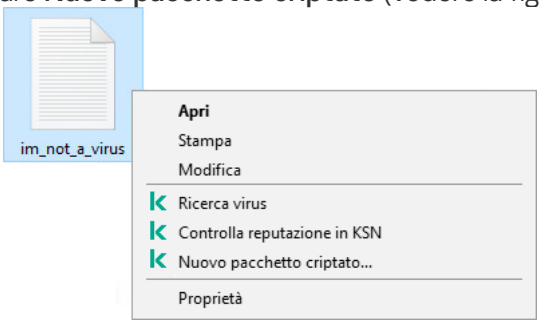
È possibile creare pacchetti criptati su computer in cui è installato Kaspersky Endpoint Security con Criptaggio a livello di file disponibile.

Durante l'aggiunta di un file al pacchetto criptato i cui contenuti si trovano nell'archivio cloud di OneDrive, Kaspersky Endpoint Security scarica i contenuti del file ed esegue il criptaggio.

Per creare un pacchetto criptato:

1. In qualsiasi programma per la gestione dei file, selezionare i file o le cartelle che si desidera aggiungere al pacchetto criptato. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.

2. Nel menu di scelta rapida selezionare **Nuovo pacchetto criptato** (vedere la figura di seguito).



Creazione di un pacchetto criptato

3. Nella finestra visualizzata, specificare la password e confermarla.

   La password deve soddisfare i criteri di complessità specificati nel criterio.

4. Fare clic su **Crea**.

   Verrà avviato il processo di creazione del pacchetto criptato. Kaspersky Endpoint Security non esegue la compressione dei file durante la creazione di un pacchetto criptato. Al termine del processo, nella cartella di destinazione selezionata viene creato un pacchetto criptato autoestraente protetto da password (un file eseguibile con estensione .exe -).

Per accedere ai file in un pacchetto criptato, fare doppio clic su questo per avviare la decompressione guidata, quindi immettere la password. Se la password è stata dimenticata o smarrita, non è possibile ripristinarla e accedere ai file nel pacchetto criptato. È possibile ricreare il pacchetto criptato.

Ripristino dell'accesso ai file criptati

Quando i file vengono criptati, Kaspersky Endpoint Security riceve una chiave di criptaggio necessaria per accedere direttamente ai file criptati. Utilizzando questa chiave di criptaggio, un utente con qualsiasi account Windows attivo durante il criptaggio dei file può accedere direttamente ai file criptati. Gli utenti con account Windows inattivi durante il criptaggio dei file devono eseguire la connessione a Kaspersky Security Center per accedere ai file criptati.

I file criptati possono risultare inaccessibili nelle seguenti circostanze:

- Le chiavi di criptaggio sono archiviate nel computer dell'utente, ma non è disponibile la connessione a Kaspersky Security Center per la gestione delle chiavi. In questo caso, l'utente deve richiedere l'accesso ai file criptati all'amministratore della rete LAN.

  Se l'accesso a Kaspersky Security Center non è disponibile, è necessario:

  - Richiedere una chiave di accesso per accedere ai file criptati nei dischi rigidi del computer.
  - Per accedere ai file criptati archiviati nelle unità rimovibili, richiedere chiavi di accesso distinte per i file criptati in ogni unità rimovibile.

- I componenti di criptaggio sono stati eliminati dal computer dell'utente. In questo caso, l'utente può aprire i file criptati nei dischi locali e rimovibili, ma il contenuto dei file risulterà criptato.

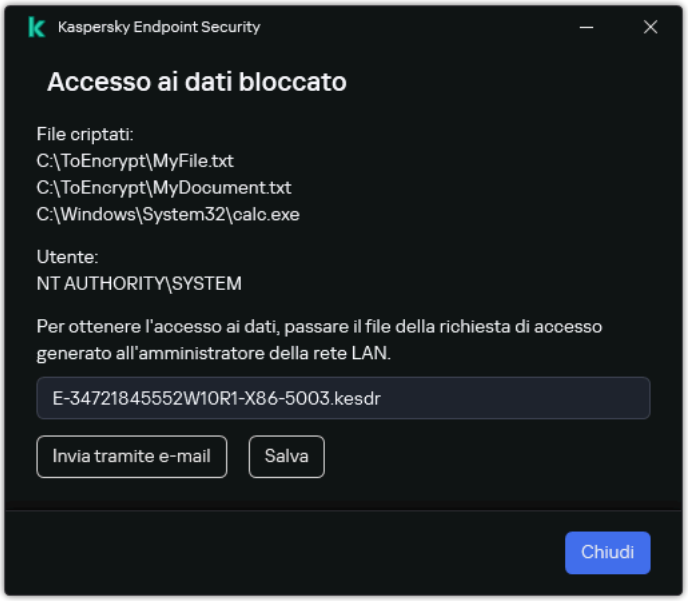
L'utente può utilizzare i file criptati nelle seguenti circostanze:

- I file sono inseriti in pacchetti criptati creati su un computer in cui è installato Kaspersky Endpoint Security.
- I file sono archiviati su unità rimovibili in cui è stata consentita la modalità portatile.

Per ottenere l'accesso ai file criptati, l'utente deve avviare la procedura di ripristino (richiesta-risposta).

Il ripristino dell'accesso ai file criptati prevede i seguenti passaggi:

1. L'utente invia un file della richiesta di accesso all'amministratore (vedere la figura seguente).
2. L'amministratore aggiunge il file della richiesta di accesso a Kaspersky Security Center, crea un file della chiave di accesso e invia il file all'utente.
3. L'utente aggiunge il file della chiave di accesso a Kaspersky Endpoint Security e ottiene l'accesso ai file.



Ripristino dell'accesso ai file criptati

Per avviare la procedura di ripristino, l'utente deve tentare di accedere a un file. Di conseguenza, Kaspersky Endpoint Security creerà un file della richiesta di accesso (un file con estensione KESDC), che l'utente deve inviare all'amministratore, ad esempio tramite e-mail.

Kaspersky Endpoint Security genera un file della richiesta di accesso a tutti i file criptati archiviati nell'unità del computer (unità locale o unità rimovibile).

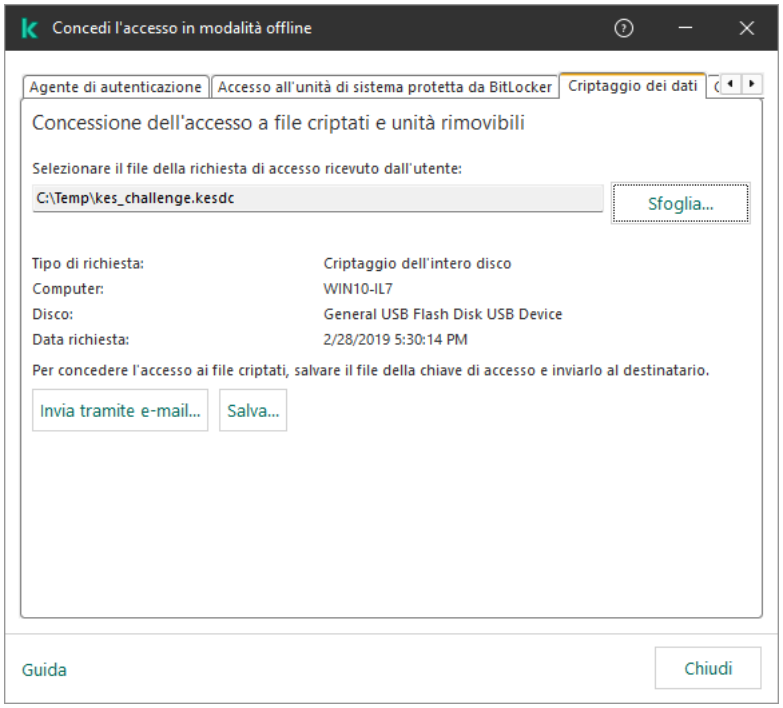
Come ottenere un file della chiave di accesso ai dati criptati in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi**.
3. Nella scheda **Dispositivi** selezionare il computer dell'utente che richiede l'accesso ai dati criptati, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
4. Nel menu di scelta rapida, selezionare **Concedi l'accesso in modalità offline**.
5. Viene visualizzata una finestra, che consente di selezionare la scheda **Criptaggio dei dati**.

6. Nella scheda **Criptaggio dei dati** fare clic sul pulsante **Sfoglia**.

7. Nella finestra per la selezione di un file della richiesta di accesso, specificare il percorso del file ricevuto dall'utente.

Verranno visualizzate le informazioni sulla richiesta dell'utente. Kaspersky Security Center genera un file chiave. Inviare tramite e-mail il file della chiave di accesso ai dati criptati generato all'utente. In alternativa, salvare il file di accesso e utilizzare uno dei metodi disponibili per trasferire il file.



Concessione dell'accesso in modalità offline

Come ottenere un file della chiave di accesso ai dati criptati in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.

2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso ai dati.

3. Fare clic su **Concedi l'accesso al dispositivo in modalità offline**.

4. Selezionare **Criptaggio dei dati**.

5. Fare clic sul pulsante **Seleziona file** e selezionare il file della richiesta di accesso ricevuto dall'utente (un file con estensione KESDC).

   Web Console visualizzerà le informazioni sulla richiesta. È incluso il nome del computer in cui l'utente richiede l'accesso al file.

6. Fare clic sul pulsante **Salva chiave** e selezionare una cartella per salvare il file della chiave di accesso ai dati criptati (un file con estensione KESDR).

Successivamente, l'utente potrà ottenere la chiave di accesso ai dati criptati, che sarà necessario trasferire all'utente.

Dopo la ricezione del file della chiave di accesso ai dati criptati, l'utente deve eseguire il file facendo doppio clic. Successivamente, Kaspersky Endpoint Security concederà l'accesso a tutti i file criptati archiviati nell'unità. Per accedere ai file criptati archiviati in altre unità, è necessario ottenere un file della chiave di accesso separato per ciascuna unità.

Ripristino dell'accesso ai dati criptati dopo un errore del sistema operativo

È possibile ripristinare l'accesso ai dati dopo un errore del sistema operativo solo per il criptaggio a livello di file. Non è possibile ripristinare l'accesso ai dati se si utilizza il criptaggio dell'intero disco.

Per ripristinare l'accesso ai dati criptati dopo un errore del sistema operativo:

1. Reinstallare il sistema operativo senza formattare il disco rigido.
2. Installare Kaspersky Endpoint Security.
3. Stabilire una connessione tra il computer e il Kaspersky Security Center Administration Server che controllava il computer al momento del criptaggio dei dati.

L'accesso ai dati criptati verrà concesso alle stesse condizioni applicate prima che si verificasse l'errore del sistema operativo.

Modifica dei modelli di messaggi per l'accesso ai file criptati

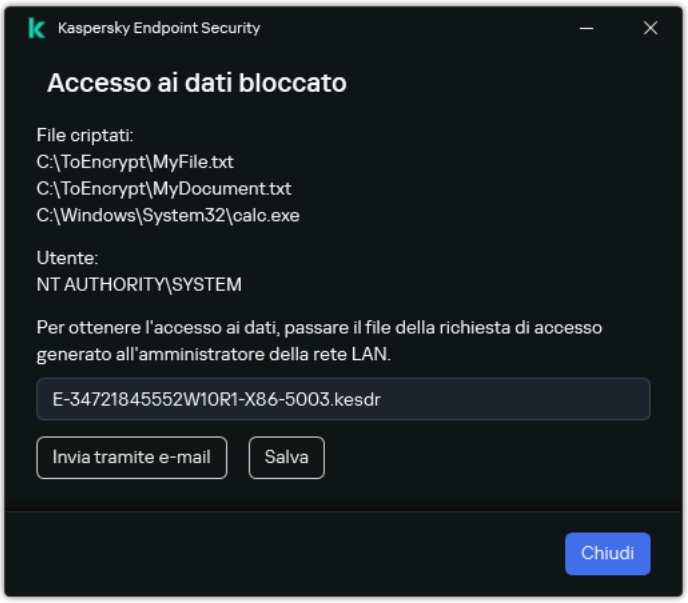
Per modificare i modelli di messaggi per l'accesso ai file criptati:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Impostazioni di criptaggio generali**.
4. Nel blocco **Modelli**, fare clic sul pulsante **Modelli**.
5. Nella finestra visualizzata, procedere come segue:
   - Se si desidera modificare il modello del messaggio dell'utente, selezionare la scheda **Messaggio dell'utente**. Quando l'utente tenta di accedere a un file criptato e nel computer non è disponibile alcuna chiave per l'accesso ai file criptati, viene visualizzata la seguente finestra (vedere la figura riportata di seguito). Facendo clic sul pulsante **Invia tramite e-mail**, viene creato automaticamente un messaggio utente. Questo messaggio è inviato all'amministratore della rete LAN aziendale insieme al file della richiesta di accesso ai file criptati.
   - Se si desidera modificare il modello del messaggio dell'amministratore, selezionare la scheda **Messaggio dell'amministratore**. L'utente riceve questo messaggio dopo che è stato concesso l'accesso ai file criptati.
6. Modificare i modelli dei messaggi.

Per aggiungere una variabile al testo del modello, posizionare il cursore nella posizione desiderata, fare clic su **Variabile** e selezionare la variabile desiderata dall'elenco delle opzioni disponibili.

È anche possibile ripristinare il testo predefinito del modello utilizzando il pulsante **Predefinito**.

7. Salvare le modifiche.



Ripristino dell'accesso ai file criptati

Criptaggio unità rimovibili

Il criptaggio delle unità rimovibili non è supportato nei computer basati su Arm.

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server.

Kaspersky Endpoint Security supporta il criptaggio dei file nei file system FAT32 e NTFS. Se un'unità rimovibile con un file system non supportato è connessa al computer, l'attività di criptaggio per l'unità rimovibile termina con un errore e Kaspersky Endpoint Security assegna lo stato di sola lettura all'unità rimovibile.

Per proteggere i dati nelle unità rimovibili, è possibile utilizzare i seguenti tipi di criptaggio:

- Full Disk Encryption (FDE).

  Criptaggio dell'intera unità rimovibile, incluso il file system.

  Non è possibile accedere ai dati criptati al di fuori della rete aziendale. Inoltre, non è possibile accedere ai dati criptati all'interno della rete aziendale se il computer non è connesso a Kaspersky Security Center (ad es. su un computer "guest").

- File Level Encryption (FLE).

Criptaggio dei soli file in un'unità rimovibile. Il file system rimane invariato.

> Il criptaggio dei file nelle unità rimovibili offre la possibilità di accedere ai dati al di fuori della rete aziendale, utilizzando una modalità speciale chiamata *modalità portatile*.

Durante il criptaggio, Kaspersky Endpoint Security crea una chiave master. Kaspersky Endpoint Security salva la chiave master nei seguenti archivi:

- Kaspersky Security Center.
- Computer dell'utente.

  La chiave master è criptata con la chiave segreta dell'utente.
- Unità rimovibile.

  La chiave master è criptata con la chiave pubblica di Kaspersky Security Center.

Al termine del criptaggio, i dati nell'unità rimovibile sono accessibili all'interno della rete aziendale come se fosse un'unità rimovibile convenzionale senza criptaggio.

Accesso ai dati criptati

Quando viene collegata un'unità rimovibile con dati criptati, Kaspersky Endpoint Security esegue le seguenti azioni:

1. Verifica la presenza di una chiave master nella memoria locale nel computer dell'utente.

   Se viene rilevata la chiave master, l'utente ottiene l'accesso ai dati nell'unità rimovibile.

   Se non viene rilevata la chiave master, Kaspersky Endpoint Security esegue le seguenti azioni:

   a. Invia una richiesta a Kaspersky Security Center.

      Dopo aver ricevuto la richiesta, Kaspersky Security Center invia una risposta contenente la chiave master.

   b. Kaspersky Endpoint Security salva la chiave master nella memoria locale nel computer dell'utente per le operazioni successive con l'unità rimovibile criptata.
2. Decripta i dati.

Funzionalità speciali di criptaggio dell'unità rimovibile

Il criptaggio delle unità rimovibili ha le seguenti funzionalità speciali:

- Il criterio con le impostazioni preimpostate per il criptaggio delle unità rimovibili viene creato per uno specifico gruppo di computer gestiti. Di conseguenza, il risultato dell'applicazione del criterio di Kaspersky Security Center configurato per il criptaggio/decriptaggio delle unità rimovibili dipende dal computer a cui è connessa l'unità rimovibile.
- Kaspersky Endpoint Security non cripta/decripta i file con stato di sola lettura archiviati nelle unità rimovibili.

- I seguenti tipi di dispositivi sono supportati come unità rimovibili:
  - Supporti dati connessi tramite il bus USB
  - Dischi rigidi connessi tramite i bus USB e FireWire
  - Unità SSD connesse tramite i bus USB e FireWire

Avvio del criptaggio delle unità rimovibili

È possibile utilizzare un criterio per decriptare un'unità rimovibile. Un criterio con impostazioni definite per il criptaggio delle unità rimovibili viene generato per un gruppo di amministrazione specifico. Di conseguenza, il risultato del decriptaggio dei dati nelle unità rimovibili dipende dal computer a cui è connessa l'unità rimovibile.

Kaspersky Endpoint Security supporta il criptaggio dei file nei file system FAT32 e NTFS. Se un'unità rimovibile con un file system non supportato è connessa al computer, l'attività di criptaggio per l'unità rimovibile termina con un errore e Kaspersky Endpoint Security assegna lo stato di sola lettura all'unità rimovibile.

Prima di criptare i file in un'unità rimovibile, assicurarsi che sia formattata e che non vi siano partizioni nascoste (come una partizione di sistema EFI). Se l'unità contiene partizioni non formattate o nascoste, il criptaggio dei file potrebbe non riuscire con un errore.

Per criptare le unità rimovibili:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
4. Nell'elenco a discesa **Modalità di criptaggio** selezionare l'azione predefinita che si desidera che Kaspersky Endpoint Security esegua nelle unità rimovibili:
   - **Cripta intera unità rimovibile** (FDE). Kaspersky Endpoint Security cripta i contenuti di un'unità rimovibile settore per settore. Di conseguenza, l'applicazione cripta non solo i file archiviati nell'unità rimovibile ma anche i relativi file system, inclusi i nomi dei file e le strutture di cartelle nell'unità rimovibile.
   - **Cripta tutti i file** (FLE). Kaspersky Endpoint Security cripta tutti i file archiviati nelle unità rimovibili. L'applicazione non cripta i file system delle unità rimovibili, inclusi i nomi dei file e le strutture di cartelle.
   - **Cripta solo i nuovi file** (FLE). Kaspersky Endpoint Security cripta solo i file che sono stati aggiunti alle unità rimovibili o che sono stati archiviati nelle unità rimovibili e modificati dopo l'applicazione del criterio di Kaspersky Security Center.

   Kaspersky Endpoint Security non cripta un'unità rimovibile già criptata.

5. Se si desidera utilizzare la modalità portatile per il criptaggio delle unità rimovibili, selezionare la casella di controllo **Modalità portatile**.

   La *modalità portatile* è una modalità di criptaggio dei file (FLE) nelle unità rimovibili che consente di accedere ai dati all'esterno di una rete aziendale. La modalità portatile consente inoltre di utilizzare i dati criptati nei computer in cui non è installato Kaspersky Endpoint Security.

6. Se si desidera criptare una nuova unità rimovibile è consigliabile selezionare la casella di controllo **Cripta solo lo spazio su disco utilizzato**. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security cripta tutti i file, inclusi i frammenti residui dei file modificati o eliminati.

7. Se si desidera configurare il criptaggio per le unità rimovibili individuali, definire le regole di criptaggio.

8. Se si desidera utilizzare il criptaggio dell'intero disco delle unità rimovibili in modalità offline, selezionare la casella di controllo **Consenti il criptaggio delle unità rimovibili in modalità offline**.

   La *modalità di criptaggio offline* fa riferimento al criptaggio delle unità rimovibili (FDE) quando non è disponibile la connessione a Kaspersky Security Center. Durante il criptaggio, Kaspersky Endpoint Security salva la chiave master solo nel computer dell'utente. Kaspersky Endpoint Security invia la chiave master a Kaspersky Security Center durante la sincronizzazione successiva.

   Se il computer in cui è salvata la chiave master è danneggiato e i dati non vengono inviati a Kaspersky Security Center, non è possibile ottenere l'accesso all'unità rimovibile.

   Se la casella di controllo **Consenti il criptaggio delle unità rimovibili in modalità offline** è deselezionata e non è disponibile la connessione a Kaspersky Security Center, il criptaggio delle unità rimovibili non è possibile.

9. Salvare le modifiche.

Dopo l'applicazione del criterio, quando l'utente si connette a un'unità rimovibile o se l'unità rimovibile è già connessa, Kaspersky Endpoint Security chiede conferma all'utente per eseguire l'operazione di criptaggio (vedere la figura di seguito).

L'applicazione consente di eseguire le seguenti azioni:

- Se l'utente conferma la richiesta di criptaggio, Kaspersky Endpoint Security cripta i dati.
- Se l'utente nega la richiesta di criptaggio, Kaspersky Endpoint Security non modifica i dati e assegna l'accesso di sola lettura a questa unità rimovibile.
- Se l'utente non risponde alla richiesta di criptaggio, Kaspersky Endpoint Security non modifica i dati e assegna l'accesso di sola lettura a questa unità rimovibile. L'applicazione richiede nuovamente conferma alla successiva applicazione di un criterio o alla successiva connessione dell'unità rimovibile.

Se l'utente avvia la rimozione sicura di un'unità rimovibile durante il criptaggio dei dati, Kaspersky Endpoint Security interrompe il processo di criptaggio dei dati e consente la rimozione dell'unità rimovibile prima del completamento del processo di criptaggio. Il criptaggio dei dati continuerà alla successiva connessione dell'unità rimovibile al computer.

Se il criptaggio di un'unità rimovibile non riesce, visualizzare il rapporto **Criptaggio dei dati** nell'interfaccia di Kaspersky Endpoint Security. L'accesso ai file potrebbe essere bloccato da un'altra applicazione. In questo caso, provare a scollegare l'unità rimovibile dal computer e ricollegarla.



Richiesta di criptaggio delle unità rimovibili

Aggiunta di una regola di criptaggio per le unità rimovibili

Per aggiungere una regola di criptaggio per le unità rimovibili:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
4. Fare clic sul pulsante **Aggiungi** e selezionare uno dei seguenti elementi nell'elenco a discesa:
   - Se si desidera aggiungere regole di criptaggio per le unità rimovibili che sono incluse nell'elenco di dispositivi attendibili del componente Controllo dispositivi, selezionare **Dall'elenco di dispositivi attendibili di questo criterio**.
   - Se si desidera aggiungere regole di criptaggio per le unità rimovibili che sono incluse nell'elenco di Kaspersky Security Center, selezionare **Dall'elenco di dispositivi di Kaspersky Security Center**.
5. Nell'elenco a discesa **Modalità di criptaggio per i dispositivi selezionati** selezionare l'azione che deve essere eseguita da Kaspersky Endpoint Security sui file archiviati nelle unità rimovibili selezionate.

6. Selezionare la casella di controllo **Modalità portatile** se si desidera che Kaspersky Endpoint Security prepari le unità rimovibili prima del criptaggio, rendendo possibile utilizzare in modalità portatile i file criptati che contengono.

   La modalità portatile consente di utilizzare i file criptati archiviati nelle unità rimovibili connesse a computer senza funzionalità di criptaggio.

7. Selezionare la casella di controllo **Cripta solo lo spazio su disco utilizzato** se si desidera che Kaspersky Endpoint Security esegua il criptaggio solo dei settori del disco che sono occupati da file.

   Se si applica il criptaggio a un'unità già in uso, è consigliabile criptare l'intera unità. Questo garantisce che tutti i dati siano protetti, anche i dati eliminati che potrebbero ancora contenere informazioni recuperabili. La funzione **Cripta solo lo spazio su disco utilizzato** è consigliabile per le nuove unità che non sono state utilizzate in precedenza.

   Se un dispositivo è stato precedentemente criptato tramite la funzione **Cripta solo lo spazio su disco utilizzato**, dopo avere applicato un criterio in modalità **Cripta intera unità rimovibile**, i settori che non sono occupati da file non saranno criptati.

8. Nell'elenco a discesa **Azioni per i dispositivi selezionati in precedenza** selezionare l'azione che deve essere eseguita da Kaspersky Endpoint Security in base alle regole di criptaggio definite in precedenza per le unità rimovibili:

   - Se si desidera mantenere invariata la regola di criptaggio creata in precedenza per l'unità rimovibile, selezionare **Ignora**.
   - Se si desidera sostituire la regola di criptaggio creata in precedenza per l'unità rimovibile con la nuova regola, selezionare **Aggiorna**.

9. Salvare le modifiche.

Le regole di criptaggio aggiunte per le unità rimovibili verranno applicate alle unità rimovibili connesse a qualsiasi computer dell'organizzazione.

Esportazione e importazione di un elenco di regole di criptaggio per unità rimovibili

È possibile esportare l'elenco delle regole di criptaggio delle unità rimovibili in un file XML. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di regole per lo stesso tipo di unità rimovibili. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dell'elenco delle regole o per eseguire la migrazione delle regole in un server diverso.

Come esportare e importare un elenco di regole di criptaggio delle unità rimovibili in Administration Console (MMC)

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Criptaggio dei dati** → **Criptaggio unità rimovibili**.

5. Nella sezione **Regole di criptaggio per i dispositivi selezionati**, fare clic sul collegamento **<N> regole**.

   Verrà visualizzato un elenco di regole di criptaggio per le unità rimovibili.

6. Per esportare l'elenco delle regole di criptaggio per le unità rimovibili:

   a. Selezionare le regole che si desidera esportare.

   b. Fare clic su **Esporta**.

   c. Confermare di voler esportare solo le regole selezionate o esportare l'intero elenco.

   d. Salvare il file.

      Kaspersky Endpoint Security esporta l'elenco delle regole in un file XML nella cartella dei download predefinita.

7. Per importare l'elenco delle regole:

   a. Fare clic sul collegamento **Importa**.

      Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle regole.

   b. Aprire il file.

      Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

8. Salvare le modifiche.

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio unità rimovibili**.

4. Per esportare l'elenco delle regole di criptaggio per le unità rimovibili:

   a. Selezionare le regole che si desidera esportare. Per selezionare più porte, utilizzare i tasti **CTRL** o **MAIUSC**.

      Se non è stata selezionata alcuna regola, Kaspersky Endpoint Security esporterà tutte le regole.

   b. Fare clic sul collegamento **Esporta**.

   c. Nella finestra visualizzata specificare il nome del file XML in cui si desidera esportare l'elenco delle regole e selezionare la cartella in cui si desidera salvare il file.

   d. Salvare il file.

      Kaspersky Endpoint Security esporta l'intero elenco di regole nel file XML.

5. Per importare un elenco di regole di criptaggio per le unità rimovibili:

   a. Fare clic sul collegamento **Importa**.

      Nella finestra visualizzata selezionare il file XML da cui si desidera importare l'elenco delle regole.

b. Aprire il file.

Se il computer dispone già di un elenco di regole, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

6. Salvare le modifiche.

Modalità portatile per l'accesso ai file criptati nelle unità rimovibili

La *modalità portatile* è una modalità di criptaggio dei file (FLE) nelle unità rimovibili che consente di accedere ai dati all'esterno di una rete aziendale. La modalità portatile consente inoltre di utilizzare i dati criptati nei computer in cui non è installato Kaspersky Endpoint Security.

La modalità portatile è utile nei seguenti casi:

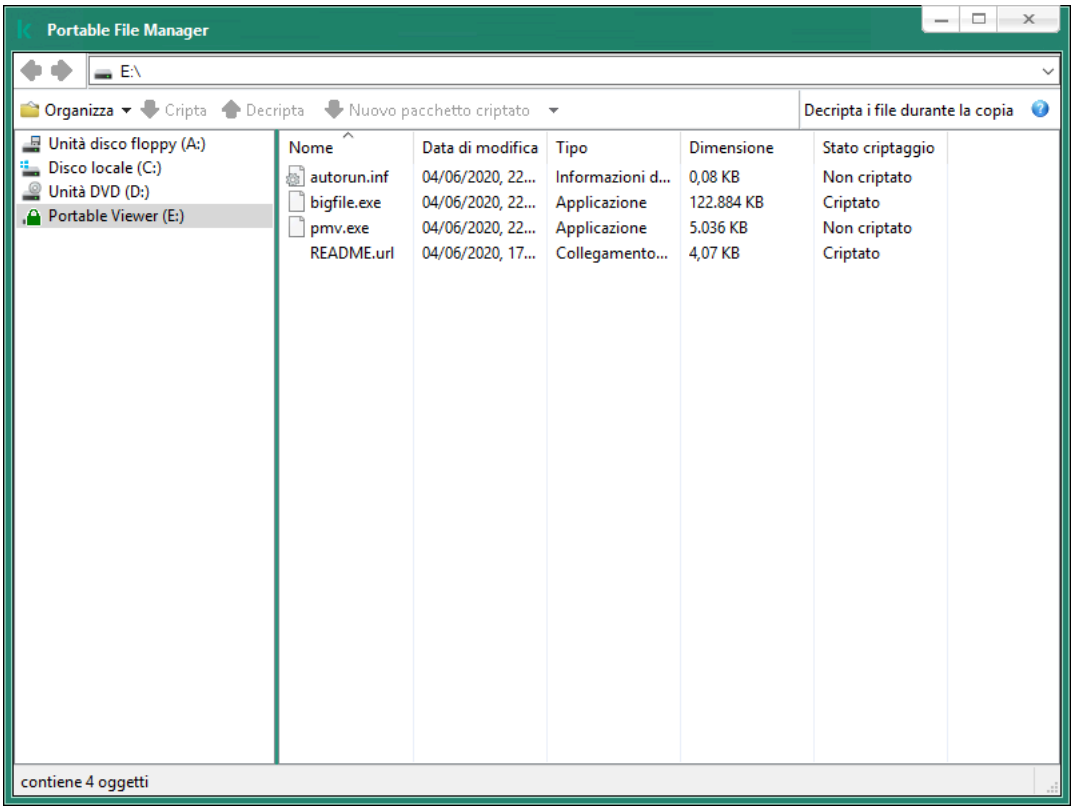
- Non è disponibile la connessione tra il computer e Kaspersky Security Center Administration Server.
- L'infrastruttura è cambiata con la modifica di Kaspersky Security Center Administration Server.
- Kaspersky Endpoint Security non è installato nel computer.

Portable File Manager

Per l'utilizzo della modalità portatile, Kaspersky Endpoint Security installa un modulo di criptaggio speciale denominato *Portable File Manager* in un'unità rimovibile. Portable File Manager offre un'interfaccia per l'utilizzo dei dati criptati se Kaspersky Endpoint Security non è installato nel computer (vedere la figura seguente). Se Kaspersky Endpoint Security è installato nel computer, è possibile utilizzare le unità rimovibili criptate con il consueto strumento per la gestione dei file (ad esempio Esplora risorse).

Portable File Manager memorizza una chiave per criptare i file in un'unità rimovibile. La chiave viene criptata con la password dell'utente. L'utente imposta una password prima di criptare i file in un'unità rimovibile.

Portable File Manager si avvia automaticamente quando un'unità rimovibile viene collegata a un computer in cui non è installato Kaspersky Endpoint Security. Se l'avvio automatico delle applicazioni è disabilitato nel computer, avviare manualmente Portable File Manager. A tale scopo, eseguire il file denominato pmv.exe archiviato nell'unità rimovibile.



Portable File Manager

Supporto della modalità portatile per l'utilizzo dei file criptati

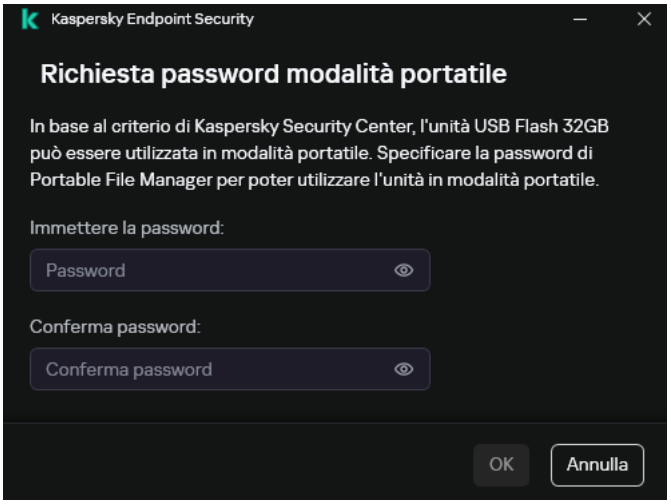
Come abilitare il supporto della modalità portatile per l'utilizzo dei file criptati nelle unità rimovibili in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
4. Nell'elenco a discesa **Modalità di criptaggio per i dispositivi selezionati**, selezionare **Cripta tutti i file** o **Cripta solo i nuovi file**.

   La modalità portatile è disponibile solo con Criptaggio a livello di file (FLE). Non è possibile abilitare il supporto della modalità portatile per Criptaggio dell'intero disco (FDE).

5. Selezionare la casella di controllo **Modalità portatile**.
6. Se necessario, aggiungere regole di criptaggio per singole unità rimovibili.
7. Salvare le modifiche.
8. Dopo aver applicato il criterio, collegare l'unità rimovibile al computer.
9. Confermare l'operazione di criptaggio dell'unità rimovibile.

Verrà visualizzata una finestra in cui è possibile creare una password per Portable File Manager.



Richiesta password modalità portatile

10. Specificare una password che soddisfi i requisiti di complessità e confermarla.
11. Salvare le modifiche.

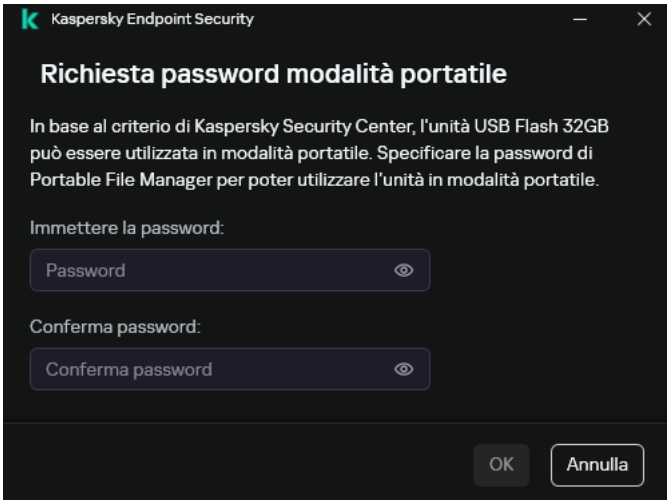
Come abilitare il supporto in modalità portatile per l'utilizzo dei file criptati in unità rimovibili in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
5. Nel blocco **Azione predefinita**, selezionare **Cripta tutti i file** o **Cripta solo i nuovi file**.

   La modalità portatile è disponibile solo con Criptaggio a livello di file (FLE). Non è possibile abilitare il supporto della modalità portatile per Criptaggio dell'intero disco (FDE).
6. Selezionare la casella di controllo **Modalità portatile**.
7. Se necessario, aggiungere regole di criptaggio per singole unità rimovibili.
8. Salvare le modifiche.
9. Dopo aver applicato il criterio, collegare l'unità rimovibile al computer.
10. Confermare l'operazione di criptaggio dell'unità rimovibile.

Verrà visualizzata una finestra in cui è possibile creare una password per Portable File Manager.



Richiesta password modalità portatile

11. Specificare una password che soddisfi i requisiti di complessità e confermarla.

12. Salvare le modifiche.

Kaspersky Endpoint Security cripterà i file presenti nell'unità rimovibile. Nell'unità rimovibile verrà inoltre aggiunto Portable File Manager per l'utilizzo dei file criptati. Se nell'unità rimovibile sono già presenti file criptati, Kaspersky Endpoint Security li cripterà di nuovo utilizzando la propria chiave. Ciò consente all'utente di accedere a tutti i file presenti nell'unità rimovibile in modalità portatile.

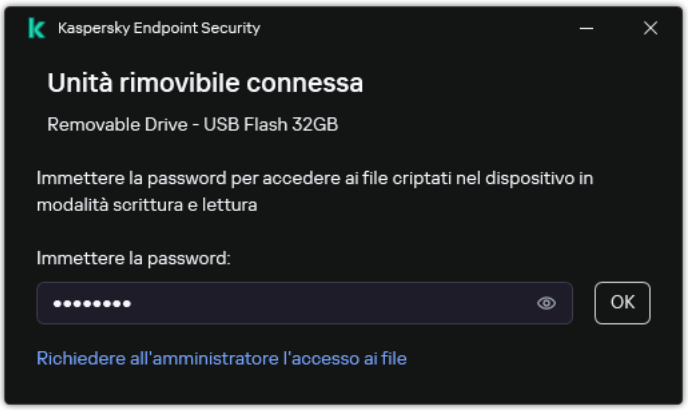
Accesso ai file criptati in un'unità rimovibile

Dopo aver criptato i file in un'unità rimovibile con supporto della modalità portatile, sono disponibili i seguenti metodi di accesso ai file:

- Se Kaspersky Endpoint Security non è installato nel computer, Portable File Manager richiederà all'utente di inserire una password. Sarà necessario immettere la password ogni volta che si riavvia il computer o si riconnette l'unità rimovibile.

- Se il computer si trova al di fuori della rete aziendale e Kaspersky Endpoint Security è installato nel computer, l'applicazione richiederà di inserire la password o di inviare all'amministratore una richiesta di accesso ai file. Dopo aver ottenuto l'accesso ai file in un'unità rimovibile, Kaspersky Endpoint Security salverà la chiave segreta nell'archivio chiavi del computer. Questo consentirà l'accesso ai file in futuro senza immettere una password o inviare una richiesta all'amministratore (vedere la figura riportata di seguito).

- Se il computer si trova all'interno della rete aziendale e Kaspersky Endpoint Security è installato nel computer, si otterrà l'accesso al dispositivo senza immettere una password. Kaspersky Endpoint Security riceverà la chiave segreta da Kaspersky Security Center Administration Server a cui è collegato il computer.



Accesso ai file criptati in un'unità rimovibile

Ripristino della password per l'utilizzo della modalità portatile

Se è stata dimenticata la password per l'utilizzo della modalità portatile, è necessario collegare l'unità rimovibile a un computer in cui è installato Kaspersky Endpoint Security all'interno della rete aziendale. Si avrà accesso ai file perché la chiave segreta è archiviata nell'archivio chiavi del computer o in Administration Server. Decriptare e criptare nuovamente i file con una nuova password.

Funzionalità della modalità portatile quando si collega un'unità rimovibile a un computer di un'altra rete

Se il computer si trova all'esterno della rete aziendale e Kaspersky Endpoint Security è installato nel computer, è possibile accedere ai file nei seguenti modi:

- **Accesso basato sulla password**

  Dopo avere inserito la password sarà possibile visualizzare, modificare e salvare i file in un'unità rimovibile (*accesso trasparente*). Kaspersky Endpoint Security può impostare un diritto di accesso di sola lettura per un'unità rimovibile se i seguenti parametri sono configurati nelle impostazioni dei criteri per il criptaggio delle unità rimovibili:

  - Il supporto della modalità portatile è disabilitato.
  - La modalità **Cripta tutti i file** o **Cripta solo i nuovi file** viene selezionata.

  In tutti gli altri casi, l'utente otterrà l'accesso completo all'unità rimovibile (autorizzazione di lettura/scrittura). L'utente sarà in grado di aggiungere ed eliminare i file.

  È possibile modificare le autorizzazioni di accesso all'unità rimovibile anche mentre l'unità rimovibile è connessa al computer. Se le autorizzazioni di accesso all'unità rimovibile vengono modificate, Kaspersky Endpoint Security bloccherà l'accesso ai file e richiederà di nuovo la password.

  Dopo aver inserito la password, l'utente non potrà applicare le impostazioni del criterio di criptaggio per l'unità rimovibile. In questo caso non sarà possibile decriptare o criptare nuovamente i file nell'unità rimovibile.

- **Chiedere l'accesso ai file all'amministratore**

Se è stata dimenticata la password per l'utilizzo della modalità portatile, chiedere all'amministratore di accedere ai file. Per accedere ai file l'utente deve inviare all'amministratore un file della richiesta di accesso (un file con estensione KESDC). L'utente può ad esempio inviare il file della richiesta di accesso tramite e-mail. L'amministratore invierà un file di accesso ai dati criptati (un file con estensione KESDR).

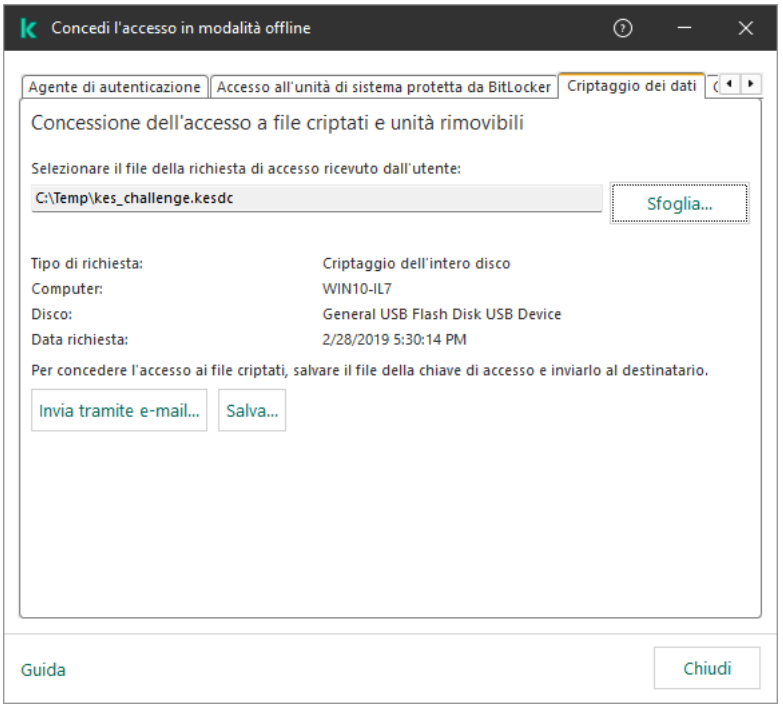
Dopo aver completato la procedura di ripristino della password di richiesta/risposta, l'utente otterrà l'accesso trasparente ai file nell'unità rimovibile e l'accesso completo all'unità rimovibile (autorizzazione di lettura/scrittura).

È ad esempio possibile applicare un criterio di criptaggio dell'unità rimovibile e decriptare i file. Dopo il ripristino della password o dopo l'aggiornamento del criterio, Kaspersky Endpoint Security richiederà di confermare le modifiche.

Come ottenere un file di accesso ai dati criptati in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi**.
3. Nella scheda **Dispositivi** selezionare il computer dell'utente che richiede l'accesso ai dati criptati, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
4. Nel menu di scelta rapida, selezionare **Concedi l'accesso in modalità offline**.
5. Viene visualizzata una finestra, che consente di selezionare la scheda **Criptaggio dei dati**.
6. Nella scheda **Criptaggio dei dati** fare clic sul pulsante **Sfoglia**.
7. Nella finestra per la selezione di un file della richiesta di accesso, specificare il percorso del file ricevuto dall'utente.

Verranno visualizzate le informazioni sulla richiesta dell'utente. Kaspersky Security Center genera un file chiave. Inviare tramite e-mail il file della chiave di accesso ai dati criptati generato all'utente. In alternativa, salvare il file di accesso e utilizzare uno dei metodi disponibili per trasferire il file.



Concessione dell'accesso in modalità offline

Come ottenere un file di accesso ai dati criptati in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Risorse (dispositivi)**.
2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso ai dati.
3. Fare clic su **Concedi l'accesso al dispositivo in modalità offline**.
4. Selezionare **Criptaggio dei dati**.
5. Fare clic sul pulsante **Seleziona file** e selezionare il file della richiesta di accesso ricevuto dall'utente (un file con estensione KESDC).

   Web Console visualizzerà le informazioni sulla richiesta. È incluso il nome del computer in cui l'utente richiede l'accesso al file.
6. Fare clic sul pulsante **Salva chiave** e selezionare una cartella per salvare il file della chiave di accesso ai dati criptati (un file con estensione KESDR).

Successivamente, l'utente potrà ottenere la chiave di accesso ai dati criptati, che sarà necessario trasferire all'utente.

Decriptaggio delle unità rimovibili

È possibile utilizzare un criterio per decriptare un'unità rimovibile. Un criterio con impostazioni definite per il criptaggio delle unità rimovibili viene generato per un gruppo di amministrazione specifico. Di conseguenza, il risultato del decriptaggio dei dati nelle unità rimovibili dipende dal computer a cui è connessa l'unità rimovibile.

Per decriptare le unità rimovibili:

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Criptaggio dei dati → Criptaggio unità rimovibili**.
4. Per decriptare tutti i file criptati archiviati nelle unità rimovibili, dall'elenco a discesa **Modalità di criptaggio** selezionare **Decripta intera unità rimovibile**.

5. Per decriptare i dati archiviati in singole unità rimovibili, modificare le regole di criptaggio per le unità rimovibili di cui si desidera decriptare i dati. A tale scopo:

   a. Nell'elenco delle unità rimovibili per cui sono state configurate regole di criptaggio selezionare la voce corrispondente all'unità rimovibile desiderata.

   b. Fare clic sul pulsante **Imposta una regola** per modificare la regola di criptaggio per l'unità rimovibile selezionata.

   c. Nel menu di scelta rapida del pulsante **Imposta una regola**, selezionare la voce **Decripta intera unità rimovibile**.

6. Salvare le modifiche.

Se pertanto un utente connette un'unità rimovibile o se questa è già connessa, Kaspersky Endpoint Security decripta l'unità rimovibile. L'applicazione segnala all'utente che il processo di decriptaggio può richiedere un certo tempo. Se l'utente avvia la rimozione sicura di un'unità rimovibile durante il decriptaggio dei dati, Kaspersky Endpoint Security interrompe il processo di decriptaggio dei dati e consente la rimozione dell'unità rimovibile prima del completamento dell'operazione di decriptaggio. Il criptaggio dei dati continuerà la volta successiva che l'unità rimovibile viene connessa al computer.

Se il decriptaggio di un'unità rimovibile non riesce, visualizzare il rapporto **Criptaggio dei dati** nell'interfaccia di Kaspersky Endpoint Security. L'accesso ai file potrebbe essere bloccato da un'altra applicazione. In questo caso, provare a scollegare l'unità rimovibile dal computer e ricollegarla.

Visualizzazione dei dettagli sul criptaggio dei dati

Mentre è in corso il criptaggio o il decriptaggio, Kaspersky Endpoint Security utilizza le informazioni sullo stato dei parametri di criptaggio applicati ai computer client da Kaspersky Security Center.

Visualizzazione dello stato di criptaggio

È possibile esaminare lo stato per monitorare il criptaggio dei dati. Kaspersky Endpoint Security assegna i seguenti stati di criptaggio:

- **Non soddisfa il criterio; l'operazione è stata annullata dall'utente**. L'utente ha annullato il criptaggio dei dati.
- **Non soddisfa il criterio a causa di un errore**. Errore di criptaggio dei dati, ad esempio manca una licenza.
- **Applicazione del criterio; è necessario il riavvio**. È in corso il criptaggio dei dati nel computer. Riavviare il computer per completare il criptaggio dei dati.
- **Nessun criterio di criptaggio specificato**. Il criptaggio dei dati è disattivato nelle impostazioni dei criteri.
- **Non supportato**. I componenti di criptaggio dei dati non sono installati nel computer.
- **Applicazione del criterio in corso**. È in corso il criptaggio e/o decriptaggio dei dati nel computer.

Per visualizzare lo stato di criptaggio dei dati del computer:

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Dispositivi gestiti**.
3. Nella scheda **Dispositivi** nell'area di lavoro trascinare la barra di scorrimento completamente a destra. Se la colonna **Stato criptaggio** non viene visualizzata, aggiungere questa colonna nelle impostazioni della console di Kaspersky Security Center.

   Nella colonna **Stato criptaggio** viene mostrato lo stato di criptaggio dei dati nei computer del gruppo di amministrazione selezionato. Questo stato viene determinato in base alle informazioni sul criptaggio dei file nelle unità locali del computer e sul criptaggio dell'intero disco.
4. Se lo stato del criptaggio dei dati per il computer è **Applicazione del criterio in corso**, è possibile monitorare il pannello di avanzamento del criptaggio:
   a. Aprire le proprietà del computer con lo stato **Applicazione del criterio in corso** facendo doppio clic su di esso.
   b. Nella finestra delle proprietà del computer selezionare la sezione **Applicazioni**.
   c. Selezionare **Kaspersky Endpoint Security for Windows** nell'elenco delle applicazioni Kaspersky installate nel computer.
   d. Fare clic su **Statistiche**.
   e. In **Criptaggio dei dispositivi**, è possibile visualizzare lo stato di avanzamento corrente del criptaggio dei dati in percentuale.

Visualizzazione delle statistiche di criptaggio nei dashboard di Kaspersky Security Center

Per visualizzare lo stato di criptaggio nei dashboard di Kaspersky Security Center:

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare il nodo **Administration Server**.
3. Nell'area di lavoro a destra della struttura di Administration Console selezionare la scheda **Statistiche**.
4. Creare una nuova pagina con i riquadri dei dettagli che contengono le statistiche sul criptaggio dei dati. A tale scopo:
   a. Nella scheda **Statistiche** fare clic sul pulsante **Personalizza visualizzazione**.
   b. Nella finestra visualizzata, fare clic sul pulsante **Aggiungi**.
   c. Viene visualizzata una finestra; in tale finestra, nella sezione **Generale**, immettere il nome della pagina.
   d. Nella sezione **Riquadri informazioni**, fare clic sul pulsante **Aggiungi**.
   e. Nella finestra visualizzata, nel gruppo **Stato protezione**, selezionare l'elemento **Criptaggio dei dispositivi**.

f. Fare clic su **OK**.

g. Se necessario, modificare le impostazioni del riquadro dei dettagli. A tale scopo, utilizzare le sezioni **Visualizza** e **Dispositivi**.

h. Fare clic su **OK**.

i. Ripetere i passaggi d - h delle istruzioni, selezionando **Criptaggio unità rimovibili** nella sezione **Stato protezione**.

Il riquadro dei dettagli aggiunto viene visualizzato nell'elenco **Riquadri informazioni**.

j. Fare clic su **OK**.

Il nome della pagina con i riquadri dei dettagli creata nei passaggi precedenti viene visualizzato nell'elenco **Pagine**.

k. Fare clic sul pulsante **Chiudi**.

5. Nella scheda **Statistiche** aprire la pagina creata durante i passaggi precedenti delle istruzioni.

Verranno visualizzati i riquadri dei dettagli, in cui è mostrato lo stato di criptaggio dei computer e delle unità rimovibili.

Visualizzazione degli errori di criptaggio dei file nelle unità locali del computer

Per visualizzare gli errori di criptaggio dei file nelle unità locali del computer:

1. Aprire Kaspersky Security Center Administration Console.

2. Nella struttura della console, selezionare **Dispositivi gestiti**.

3. Nella scheda **Dispositivi**, selezionare il nome del computer nell'elenco, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.

4. Dal menu di scelta rapida del computer selezionare **Proprietà**. Nella finestra visualizzata, selezionare la scheda **Protezione**.

5. Fare clic sul collegamento **Visualizza errori di criptaggio dei dati** per aprire la finestra **Errori di criptaggio dei dati**.

In questa finestra sono visualizzati i dettagli sugli errori di criptaggio dei file nelle unità locali del computer. Quando un errore viene corretto, Kaspersky Security Center rimuove i dettagli sull'errore dalla finestra **Errori di criptaggio dei dati**.

Visualizzazione del rapporto sul criptaggio dei dati

Kaspersky Security Center consente di creare rapporti sul criptaggio dei dati:

- **Rapporto sullo stato di criptaggio dei dispositivi gestiti**. Il rapporto include informazioni sulla conformità dello stato di criptaggio del computer ai criteri di criptaggio.
- **Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa**. Il rapporto include informazioni sullo stato di criptaggio dei dispositivi esterni e dei dispositivi di archiviazione.
- **Rapporto sui diritti di accesso alle unità criptate**. Il rapporto include informazioni sullo stato degli account che hanno accesso alle unità criptate.
- **Rapporto sugli errori di criptaggio dei file**. Il rapporto include informazioni sugli errori che si sono verificati durante l'esecuzione delle attività di criptaggio o decriptaggio dei dati nei computer.
- **Rapporto sul blocco dell'accesso ai file criptati**. Il rapporto include informazioni sulle applicazioni che non possono accedere ai file criptati.

Per visualizzare il rapporto sul criptaggio dei dati:

1. Aprire Kaspersky Security Center Administration Console.
2. Nel nodo **Administration Server** della struttura di Administration Console selezionare la scheda **Rapporti**.
3. Fare clic sul pulsante **Nuovo modello di rapporto**.

   Verrà avviata la Creazione guidata nuovo modello di rapporto.
4. Attenersi alle istruzioni della Creazione guidata nuovo modello di rapporto. Nella finestra **Selezione del tipo di modello di rapporto** nella sezione **Altro**, selezionare uno dei rapporti sul criptaggio dei dati.

   Dopo avere completato la Creazione guidata nuovo modello di rapporto, il nuovo modello di rapporto viene visualizzato nella tabella della scheda **Rapporti**.
5. Selezionare il modello di rapporto che è stato creato nei passaggi precedenti delle istruzioni.
6. Nel menu di scelta rapida del modello selezionare **Visualizza rapporto**.

Verrà avviato il processo di generazione del rapporto. Il rapporto viene visualizzato in una nuova finestra.

Utilizzo dei dispositivi criptati quando non è possibile accedervi

Ottenimento dell'accesso ai dispositivi criptati

Per un utente può essere necessario richiedere l'accesso a dispositivi criptati nei seguenti casi:

- Il disco rigido è stato criptato in un altro computer.
- La chiave di criptaggio per un dispositivo non è presente sul computer (ad esempio, al primo tentativo di accesso all'unità rimovibile criptata sul computer) e il computer non è connesso a Kaspersky Security Center.

  Dopo che l'utente ha applicato la chiave di accesso al dispositivo criptato, Kaspersky Endpoint Security salva la chiave di criptaggio nel computer dell'utente e consente l'accesso al dispositivo durante i tentativi di accesso successivi, anche se la connessione a Kaspersky Security Center non è disponibile.

L'accesso ai dispositivi criptati può essere ottenuto come segue:

1. L'utente utilizza l'interfaccia dell'applicazione di Kaspersky Endpoint Security per creare un file della richiesta di accesso con l'estensione kesdc e lo invia all'amministratore della rete LAN aziendale.
2. L'amministratore utilizza Kaspersky Security Center Administration Console per creare un file chiave di accesso con l'estensione kesdr e lo invia all'utente.
3. L'utente applica la chiave di accesso.

Ripristino dei dati nei dispositivi criptati

Un utente può utilizzare l'Utilità di Ripristino del Dispositivo Criptato (di seguito denominata utilità di ripristino) per gestire i dispositivi criptati. Questo può essere necessario nei seguenti casi:

- La procedura per l'utilizzo di una chiave di accesso per ottenere l'accesso ha avuto esito negativo.
- I componenti di criptaggio non sono stati installati nel computer con il dispositivo criptato.

I dati necessari per ripristinare l'accesso ai dispositivi criptati tramite l'utilità di ripristino risiedono nella memoria del computer dell'utente in formato non criptato per un certo periodo di tempo. Per ridurre il rischio di accessi non autorizzati a tali dati, è consigliabile ripristinare l'accesso ai dispositivi criptati in computer attendibili.

I dati nei dispositivi criptati possono essere ripristinati come segue:

1. L'utente utilizza l'utilità di ripristino per creare un file della richiesta di accesso con l'estensione fdertc e lo invia all'amministratore della rete LAN aziendale.

2. L'amministratore utilizza Kaspersky Security Center Administration Console per creare un file chiave di accesso con l'estensione fdertr e lo invia all'utente.

3. L'utente applica la chiave di accesso.

Per ripristinare i dati in dischi rigidi di sistema criptati, l'utente può anche specificare le credenziali dell'account per l'Agente di Autenticazione nell'utilità di ripristino. Se i metadati dell'account per l'Agente di Autenticazione sono danneggiati, l'utente deve eseguire la procedura di ripristino tramite un file di richiesta di accesso.

Prima del ripristino dei dati nei dispositivi criptati, è consigliabile annullare il criterio di Kaspersky Security Center o disabilitare il criptaggio nelle impostazioni del criterio di Kaspersky Security Center nel computer in cui verrà eseguita la procedura. Questo impedisce che il dispositivo venga nuovamente criptato.

Ripristino dei dati utilizzando l'utilità di ripristino FDERT

In caso di errore del disco rigido, il file system potrebbe essere danneggiato. In tal caso, i dati protetti dalla tecnologia Criptaggio disco Kaspersky non saranno disponibili. È possibile decriptare i dati e copiarli in una nuova unità.

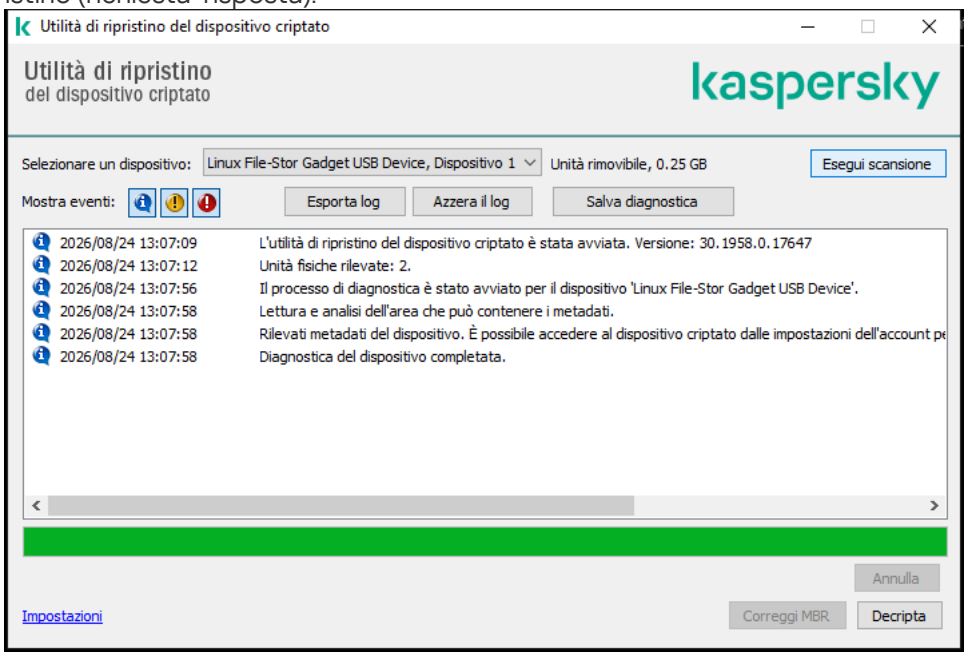
Il ripristino dei dati in un'unità protetta dalla tecnologia Criptaggio disco Kaspersky prevede i seguenti passaggi:

1. Creare un'utilità di ripristino standalone (vedere la figura seguente).

2. Collegare un'unità a un computer in cui non sono installati componenti di criptaggio Kaspersky Endpoint Security.

3. Eseguire l'utilità di ripristino e diagnosticare il disco rigido.

4. Accedere ai dati sul disco. A tale scopo, immettere le credenziali dell'Agente di Autenticazione o avviare la procedura di ripristino (richiesta-risposta).



Utilità di ripristino FDERT

Creazione di un'utilità di ripristino standalone

Per creare il file eseguibile dell'utilità di ripristino:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra visualizzata, fare clic sul pulsante **Ripristina dispositivo criptato**.

   Verrà avviata l'utilità di Ripristino del Dispositivo Criptato.
3. Fare clic sul pulsante **Crea utilità di ripristino standalone** nella finestra dell'utilità di ripristino.
4. Salvare l'utilità di ripristino standalone nella memoria del computer.

Successivamente, il file eseguibile dell'utilità di ripristino (fdert.exe) verrà salvato nella cartella specificata. Copiare l'unità di ripristino in un computer in cui non sono presenti componenti di criptaggio Kaspersky Endpoint Security. Questo impedisce che l'unità venga nuovamente criptata.

I dati necessari per ripristinare l'accesso ai dispositivi criptati tramite l'utilità di ripristino risiedono nella memoria del computer dell'utente in formato non criptato per un certo periodo di tempo. Per ridurre il rischio di accessi non autorizzati a tali dati, è consigliabile ripristinare l'accesso ai dispositivi criptati in computer attendibili.

Ripristino dei dati in un disco rigido

Per ripristinare l'accesso a un dispositivo criptato utilizzando l'utilità di ripristino:

1. Eseguire il file denominato fdert.exe, che è il file eseguibile dell'utilità di ripristino. Questo file viene creato da Kaspersky Endpoint Security.

2. Nella finestra Restore Utility, selezionare il dispositivo criptato a cui si desidera ripristinare l'accesso.

3. Fare clic sul pulsante **Esegui scansione** per consentire all'utilità di definire le azioni da eseguire sul dispositivo: se deve essere sbloccato o decriptato.

   Se il computer ha accesso alle funzionalità di criptaggio di Kaspersky Endpoint Security, l'utilità di ripristino richiede di sbloccare il dispositivo. Anche se lo sblocco non comporta il decriptaggio del dispositivo, il dispositivo diventa direttamente accessibile in seguito allo sblocco. Se il computer non ha accesso alle funzionalità di criptaggio di Kaspersky Endpoint Security, l'utilità di ripristino richiede di decriptare il dispositivo.

4. Se si desidera importare informazioni di diagnostica, fare clic sul pulsante **Salva diagnostica**.

   L'utilità salverà un archivio con i file contenenti informazioni di diagnostica.

5. Fare clic sul pulsante **Correggi MBR** se la diagnostica del disco rigido di sistema criptato restituisce un messaggio che indica problemi relativi al record di avvio principale (MBR) del dispositivo.

   La correzione del record di avvio principale del dispositivo può velocizzare il processo di acquisizione delle informazioni necessarie per lo sblocco o il decriptaggio del dispositivo.

6. Fare clic sul pulsante **Sblocca** o **Decripta**, a seconda dei risultati della diagnostica.

7. Se si desidera ripristinare i dati utilizzando un account dell'Agente di Autenticazione, selezionare l'opzione **Usa le impostazioni dell'account per l'Agente di Autenticazione** e immettere le credenziali dell'Agente di Autenticazione.

   Questo metodo è possibile solo durante il ripristino dei dati in un disco rigido di sistema. Se il disco rigido di sistema è danneggiato e i dati dell'account per l'Agente di Autenticazione sono andati persi, è necessario ottenere una chiave di accesso dall'amministratore della rete LAN aziendale per ripristinare i dati in un dispositivo criptato.

8. Se si desidera avviare la procedura di ripristino, attenersi alla seguente procedura:

   a. Selezionare l'opzione **Specificare manualmente la chiave di accesso dispositivo**.

   b. Fare clic sul pulsante **Ricevi chiave di accesso** e salvare il file della richiesta di accesso nella memoria del computer (un file con estensione FDERTC).

   c. Inviare il file della richiesta di accesso all'amministratore della rete LAN aziendale.

      Non chiudere la finestra **Ricevere una chiave di accesso dispositivo** finché non si riceve la chiave di accesso. Riaprendo questa finestra, non sarà possibile applicare la chiave di accesso creata precedentemente dall'amministratore.

   d. Ricevere e salvare il file di accesso (un file con estensione FDERTR) creato e inviato dall'amministratore della LAN aziendale (vedere le istruzioni seguenti).

   e. Scaricare il file di accesso nella finestra **Ricevere una chiave di accesso dispositivo**.

9. Se si sta decriptando un dispositivo, è necessario configurare ulteriori impostazioni di decriptaggio:

    - Specificare l'area da decriptare:

        - Se si desidera decriptare l'intero dispositivo, selezionare l'opzione **Decripta intero dispositivo**.

        - Se si desidera decriptare una parte dei dati in un dispositivo, selezionare l'opzione **Decripta singole aree del dispositivo** e specificare i limiti dell'area di decriptaggio.

    - Selezionare la posizione per la scrittura dei dati decriptati:

        - Se si desidera riscrivere i dati nel dispositivo originale con i dati decriptati, deselezionare la casella di controllo **Decripta in un file immagine del disco**.

        - Se si desidera salvare i dati decriptati separatamente dai dati criptati originali, selezionare la casella di controllo **Decripta in un file immagine del disco** e utilizzare il pulsante **Sfoglia** per specificare il percorso in cui salvare il file VHD.

10. Fare clic su **OK**.

Verrà avviato il processo di sblocco o decriptaggio del dispositivo.

Come creare un file di accesso ai dati criptati in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella struttura di Administration Console, selezionare la cartella **Avanzate → Criptaggio e protezione dei dati → Unità criptate**.

3. Nell'area di lavoro selezionare il dispositivo criptato per cui si desidera creare un file chiave di accesso e, nel menu di scelta rapida del dispositivo, fare clic su **Ottieni l'accesso al dispositivo in Kaspersky Endpoint Security**.

    Se non si è certi del computer per cui è stato generato il file della richiesta di accesso, nella struttura di Administration Console selezionare la cartella **Avanzate → Criptaggio e protezione dei dati** e nell'area di lavoro fare clic su **Recupera chiave di criptaggio dispositivo in Kaspersky Endpoint Security**.

4. Nella finestra visualizzata, selezionare l'algoritmo di criptaggio da utilizzare: AES256 o AES56.

    L'algoritmo di criptaggio dei dati dipende dalla libreria di criptaggio AES inclusa nel pacchetto di distribuzione: *Crittografia avanzata (AES256)* o *Crittografia Lite (AES56)*. La libreria di criptaggio AES viene installata insieme all'applicazione.

5. Fare clic su **Sfoglia** per aprire una finestra; in questa finestra, specificare il percorso del file della richiesta con l'estensione fdertc che è stato ricevuto dell'utente.

6. Fare clic su **Sblocca**.

Verranno visualizzate le informazioni sulla richiesta dell'utente. Kaspersky Security Center genera un file chiave. Inviare tramite e-mail il file della chiave di accesso ai dati criptati generato all'utente. In alternativa, salvare il file di accesso e utilizzare uno dei metodi disponibili per trasferire il file.

Come creare un file di accesso ai dati criptati in Web Console

1. Nella finestra principale di Web Console, fare clic su **Operazioni → Criptaggio e protezione dei dati → Unità criptate**.
2. Selezionare la casella di controllo accanto al nome del computer nel quale si desidera ripristinare i dati.
3. Fare clic su **Concedi l'accesso al dispositivo in modalità offline**.

   Viene quindi avviata la procedura guidata per ottenere l'accesso a un dispositivo.
4. Seguire le istruzioni della procedura guidata per concedere l'accesso a un dispositivo:

   a. Selezionare il plug-in Kaspersky Endpoint Security for Windows.

   b. Selezionare l'algoritmo di criptaggio da utilizzare: AES256 o AES56.

   L'algoritmo di criptaggio dei dati dipende dalla libreria di criptaggio AES inclusa nel pacchetto di distribuzione: *Crittografia avanzata (AES256)* o *Crittografia Lite (AES56)*. La libreria di criptaggio AES viene installata insieme all'applicazione.

   c. Selezionare il file della richiesta di accesso ricevuto dall'utente (un file con estensione FDERTC).

   d. Selezionare una cartella per salvare il file della chiave di accesso ai dati criptati (un file con estensione FDERTR).

Successivamente, l'utente potrà ottenere la chiave di accesso ai dati criptati, che sarà necessario trasferire all'utente.

Creazione di un Rescue Disk del sistema operativo

Il Rescue Disk del sistema operativo può essere utile quando per qualsiasi motivo non è possibile accedere a un disco rigido criptato e il caricamento del sistema operativo non riesce.

È possibile caricare un'immagine del sistema operativo Windows utilizzando il Rescue Disk e ripristinare l'accesso al disco rigido criptato tramite l'utilità di ripristino inclusa nell'immagine del sistema operativo.

Per creare un Rescue Disk del sistema operativo:

1. Creare un file eseguibile per l'utilità di Ripristino del Dispositivo Criptato.
2. Creare un'immagine personalizzata di Ambiente preinstallazione di Windows. Durante la creazione dell'immagine personalizzata di Ambiente preinstallazione di Windows, aggiungere all'immagine il file eseguibile dell'utilità di ripristino.
3. Salvare l'immagine personalizzata di Ambiente preinstallazione di Windows in un supporto di avvio, ad esempio un CD o un'unità rimovibile.

   Per istruzioni sulla creazione di un'immagine personalizzata di Ambiente preinstallazione di Windows, vedere la documentazione di Microsoft (ad esempio, in Microsoft TechNet).

Soluzioni Detection and Response

Le soluzioni Kaspersky Detection and Response sono sistemi di sicurezza per il rilevamento di minacce avanzate e indicatori di attacco su diversi livelli dell'infrastruttura di un'organizzazione. Le soluzioni di rilevamento e risposta forniscono informazioni sulla minaccia rilevata e consentono di gestire le azioni di Threat Response.

Pertanto, la soluzione Detection and Response esegue le seguenti operazioni:

- Ricevere informazioni sul funzionamento di un computer, server o altri dispositivi (telemetria).
- Analizzare automaticamente le informazioni per rilevare le minacce.
- Generare i dettagli degli avvisi come colonne della catena di sviluppo delle minacce per l'analisi e la scelta delle azioni di Threat Response.
- Eseguire azioni di Threat Response (ad esempio, l'isolamento della rete del computer).

Kaspersky Endpoint Security supporta le soluzioni Detection and Response tramite un agente integrato. L'agente integrato invia i dati di telemetria ai server delle soluzioni ed esegue le azioni di Threat Response. L'agente integrato supporta:

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) versione 7.1 o precedenti
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

È possibile utilizzare la soluzione Kaspersky Endpoint Security con Detection and Response in varie configurazioni, ad esempio [EDR Optimum+MDR].

Licenze di MDR ed EDR Optimum

Kaspersky Endpoint Security supporta le funzionalità delle soluzioni Kaspersky Managed Detection and Response (MDR) e Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). È possibile utilizzare Kaspersky Endpoint Security con queste soluzioni in varie configurazioni e creare un sistema di protezione personalizzato che soddisfi requisiti particolari. A tale scopo, è necessario acquistare una licenza per ciascuna soluzione. La licenza può coprire il diritto di utilizzare una singola soluzione (ad esempio, solo il componente aggiuntivo MDR) o più soluzioni, il componente aggiuntivo [EDR Optimum+MDR].

MDR ed EDR Optimum supportano i seguenti metodi di gestione delle licenze:

- La funzionalità MDR o EDR Optimum è inclusa nella licenza di Kaspersky Endpoint Security for Windows.

  La funzionalità è disponibile immediatamente dopo l'attivazione di Kaspersky Endpoint Security for Windows. È necessario aggiungere solo una chiave.

- Licenze separate per MDR o EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  La funzionalità diventa disponibile dopo l'aggiunta di una chiave separata per il componente aggiuntivo MDR, il componente aggiuntivo EDR Optimum o il componente aggiuntivo [EDR Optimum+MDR]. Di conseguenza, nel computer vengono aggiunte due chiavi: una per Kaspersky Endpoint Security e l'altra per MDR o EDR Optimum. La chiave di Kaspersky Endpoint Security deve essere la prima ad essere aggiunta.

Kaspersky Endpoint Security consente di aggiungerne solo una *chiave attiva* per le licenze MDR ed EDR Optimum. Pertanto, se è necessario attivare entrambe queste soluzioni, è necessario aggiungere una chiave del [EDR Optimum+MDR] Add-on anziché una chiave separata per ogni soluzione. È inoltre possibile aggiungere una *chiave di riserva*.

Se è stato utilizzato un file BLOB durante la distribuzione di MDR, non è necessaria una chiave separata per attivare MDR. Il file BLOB contiene già le informazioni sulla licenza.

Licenze iniziali delle soluzioni

Alla prima distribuzione di MDR ed EDR Optimum, le soluzioni vengono attivate nello stesso modo dell'applicazione Kaspersky Endpoint Security. È possibile aggiungere una chiave utilizzando l'attività *Aggiungi chiave* oppure utilizzare la funzionalità di distribuzione automatica delle chiavi. La chiave di licenza viene aggiunta all'applicazione come seconda chiave attiva o come chiave di riserva se si seleziona la casella di controllo pertinente.

Passaggio da una licenza all'altra

Se nell'organizzazione è già distribuita una di queste soluzioni e la chiave corrispondente è stata aggiunta all'applicazione, la gestione delle licenze della nuova configurazione comporta alcune considerazioni speciali. Quando si passa a un'altra licenza, l'applicazione non aggiunge la nuova chiave all'applicazione, ma sostituisce la chiave attuale con la nuova chiave. Il motivo è la restrizione che consente all'applicazione di aggiungere una sola chiave per attivare MDR ed EDR Optimum.

Si supponga ad esempio che nell'organizzazione sia distribuita la soluzione [EDR Optimum+MDR] e che si decida di passare alla configurazione del componente aggiuntivo MDR. Per passare alla nuova configurazione, è necessario sostituire la chiave del [EDR Optimum+MDR] Add-on con la chiave del componente aggiuntivo MDR.

Una licenza separata per EDR Optimum e MDR (componente aggiuntivo [EDR Optimum+MDR]) non è più disponibile. Se si desidera utilizzare entrambe le soluzioni, è necessario attivare MDR utilizzando un file BLOB ed EDR Optimum con una chiave di licenza.

Con la funzionalità di distribuzione automatica delle chiavi, l'applicazione rifiuta le chiavi di licenza che coprono lo stesso numero di soluzioni. In altre parole, se è stata aggiunta una chiave del componente aggiuntivo EDR Optimum, non è possibile sostituirla con una chiave del componente aggiuntivo MDR. È tuttavia possibile sostituire la chiave del componente aggiuntivo EDR Optimum con una chiave del componente aggiuntivo [EDR Optimum+MDR]. L'applicazione rifiuta le chiavi anche se si tenta di sostituire una chiave del componente aggiuntivo MDR con una chiave del componente aggiuntivo EDR. Per sostituire una chiave, è possibile eseguire l'attività *Aggiungi chiave*. L'attività *Aggiungi chiave* consente di sostituire le chiavi di licenza con un numero qualsiasi di soluzioni.

Se è stata aggiunta una chiave di riserva del componente aggiuntivo [EDR Optimum+MDR] Add-on, per aggiungere correttamente una chiave attiva per il componente aggiuntivo EDR Optimum o del componente aggiuntivo MDR, è innanzitutto necessario sostituire la chiave di riserva con una chiave del componente aggiuntivo EDR Optimum o una chiave del componente aggiuntivo MDR oppure, in alternativa, rimuovere la chiave di riserva e sostituire la chiave attiva.

Compatibilità con le soluzioni EDR di terzi

È possibile utilizzare Kaspersky Endpoint Security per proteggere workstation e server insieme a soluzioni EDR di terzi. Per eliminare i falsi positivi, è consigliabile aggiungere i file eseguibili di Kaspersky Endpoint Security e Network Agent all'area attendibile della soluzione EDR di terzi.

Area attendibile per la compatibilità con le soluzioni EDR di terzi

	Kaspersky Endpoint Security for Windows	Kaspersky Security Center Network Agent
Cartella di lavoro	`C:\Program Files (x86)\Kaspersky Lab\KES.14.2.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

File eseguibili	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent supporta l'interazione tra l'applicazione e altre soluzioni Kaspersky per il rilevamento delle minacce avanzate (ad esempio Kaspersky Sandbox). Le soluzioni Kaspersky sono compatibili con versioni specifiche di Kaspersky Endpoint Agent.

Per utilizzare Kaspersky Endpoint Agent come parte delle soluzioni Kaspersky, è necessario attivare tali soluzioni con un codice di licenza corrispondente.

Per informazioni complete su Kaspersky Endpoint Agent incluso nella soluzione software in uso e per informazioni complete sulla soluzione standalone, fare riferimento alla Guida del prodotto attinente:

- Guida di Kaspersky Anti Targeted Attack Platform
- Guida di Kaspersky Sandbox
- Guida di Kaspersky Endpoint Detection and Response Optimum
- Guida di Kaspersky Managed Detection and Response

Il kit di distribuzione per Kaspersky Endpoint Security versioni 11.2.0-11.8.0 include Kaspersky Endpoint Agent. È possibile selezionare Kaspersky Endpoint Agent durante l'installazione di Kaspersky Endpoint Security for Windows. Di conseguenza, nel computer verranno installate due applicazioni: KEA e KES. In Kaspersky Endpoint Security 11.9.0, il pacchetto di distribuzione di Kaspersky Endpoint Agent non fa più parte del kit di distribuzione di Kaspersky Endpoint Security.

Corrispondenza delle versioni di KEA (come parte di KES) alle versioni di KES

Kaspersky Endpoint Security for Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

Kaspersky sta trasferendo tutte le funzioni di Detection and Response affinché funzionino con l'agente integrato di Kaspersky Endpoint Security anziché con Kaspersky Endpoint Agent. Kaspersky sta gradualmente aggiungendo il supporto per queste soluzioni e eliminando gradualmente Kaspersky Endpoint Agent (vedere la tabella di seguito). A partire dalla versione 12.1, l'applicazione supporta tutte le soluzioni Detection and Response. Inoltre, a partire dalla versione 12.1, l'applicazione non è più compatibile con Kaspersky Endpoint Agent e non è più possibile installare entrambe le applicazioni affiancate nello stesso computer.

Versione di Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (componente Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (componente Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Agente integrato**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Agente integrato**	**Agente integrato**	**Agente integrato**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**	Kaspersky Endpoint Agent
12.6	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**	**Agente integrato**

Migrazione della configurazione [KES+KEA] alla configurazione [KES+agente integrato]

Kaspersky Endpoint Security include agenti integrati per l'utilizzo delle soluzioni Detection and Response. Non è più necessaria un'applicazione Kaspersky Endpoint Agent separata per utilizzare tali soluzioni. Quando si distribuisce Kaspersky Endpoint Security nei computer in cui è installato Kaspersky Endpoint Agent, le soluzioni Detection and Response continueranno a funzionare con Kaspersky Endpoint Security. Inoltre, Kaspersky Endpoint Agent verrà rimosso dal computer.

Il kit di distribuzione per Kaspersky Endpoint Security versioni 11.2.0-11.8.0 include Kaspersky Endpoint Agent. È possibile selezionare Kaspersky Endpoint Agent durante l'installazione di Kaspersky Endpoint Security for Windows. Di conseguenza, nel computer verranno installate due applicazioni: KEA e KES. In Kaspersky Endpoint Security 11.9.0, il pacchetto di distribuzione di Kaspersky Endpoint Agent non fa più parte del kit di distribuzione di Kaspersky Endpoint Security.

La migrazione della configurazione [KES+KEA] a [KES+agente integrato] prevede i seguenti passaggi:

1. **Upgrade di Kaspersky Security Center**

   Upgrade di tutti i componenti di Kaspersky Security Center alla versione 13.2 o successiva, incluso Network Agent nei computer dell'utente e Web Console.

2. **Upgrade del plug-in Web di Kaspersky Endpoint Security**

In Kaspersky Security Center Web Console, eseguire l'upgrade del plug-in Web di Kaspersky Endpoint Security alla versione 11.7.0 o successiva. Per gestire i componenti di EDR Optimum e Kaspersky Sandbox, è necessario utilizzare Web Console.

Per utilizzare Kaspersky Anti Targeted Attack Platform (EDR), è necessario un plug-in Web per Kaspersky Endpoint Security versione 12.1 o successiva.

Per utilizzare Kaspersky Anti Targeted Attack Platform (NDR), è necessario un plug-in Web per Kaspersky Endpoint Security versione 12.7 o successiva.

3. **Migrazione di criterio e attività**

   Utilizzare la migrazione guidata di criteri e attività di Kaspersky Endpoint Agent per eseguire la migrazione delle impostazioni di Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows.

   Viene creato un nuovo criterio di Kaspersky Endpoint Security. Il nuovo criterio presenta lo stato *Inattivo*. Per applicare il criterio, aprire le proprietà del criterio, accettare l'Informativa di Kaspersky Security Network e impostare lo stato su *Attivo*.

4. **Funzionalità di concessione di licenze**

   Se si utilizza una licenza comune di Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security per attivare Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Agent, la funzionalità EDR Optimum verrà attivata automaticamente dopo l'upgrade dell'applicazione alla versione 11.7.0. Non è necessario eseguire altre operazioni.

   Se si utilizza una licenza del componente aggiuntivo standalone di Kaspersky Endpoint Detection and Response Optimum per attivare la funzionalità EDR Optimum, è necessario accertarsi che la chiave del componente aggiuntivo EDR Optimum sia aggiunta al repository di Kaspersky Security Center e che la funzionalità di distribuzione della chiave di licenza automatica sia abilitata. Dopo aver eseguito l'upgrade dell'applicazione alla versione 11.7.0, la funzionalità EDR Optimum viene attivata automaticamente.

   Se si utilizza una licenza di Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security per attivare Kaspersky Endpoint Agent e una licenza diversa per attivare Kaspersky Endpoint Security for Windows, è necessario sostituire la chiave di Kaspersky Endpoint Security con la chiave comune di Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security. È possibile sostituire la chiave tramite l'attività *Aggiungi chiave*.

   Non è necessario attivare la funzionalità Kaspersky Sandbox. La funzionalità Kaspersky Sandbox sarà disponibile subito dopo l'upgrade e l'attivazione di Kaspersky Endpoint Security for Windows.

   Solo la licenza Kaspersky Anti Targeted Attack Platform può essere utilizzata per attivare Kaspersky Endpoint Security come parte della soluzione Kaspersky Anti Targeted Attack Platform. Dopo aver eseguito l'upgrade dell'applicazione alla versione 12.1, la funzionalità EDR (KATA) viene attivata automaticamente. Non è necessario eseguire altre operazioni.

5. **Upgrade dell'applicazione Kaspersky Endpoint Security**

   Per eseguire l'upgrade dell'applicazione e la migrazione delle funzionalità EDR Optimum e Kaspersky Sandbox, è consigliata un'attività di installazione remota.

Per eseguire l'upgrade dell'applicazione con un'attività di installazione remota, è necessario modificare le seguenti impostazioni:

- Selezionare i componenti per le soluzioni Detection and Response nelle impostazioni del pacchetto di installazione.
- Escludere il componente Kaspersky Endpoint Agent nelle impostazioni del pacchetto di installazione (per Kaspersky Endpoint Security for Windows versioni 11.2.0-11.8.0).
- Se l'opzione Protezione tramite password è abilitata per limitare l'accesso a Kaspersky Endpoint Agent, immettere la password di disinstallazione dell'applicazione nelle impostazioni dell'attività *Installa l'applicazione in remoto*. È possibile immettere la password di disinstallazione a partire da Kaspersky Security Center Linux 15.1.

È inoltre possibile eseguire l'applicazione con i seguenti metodi:

- Utilizzando il servizio di aggiornamento di Kaspersky (Seamless Update - SMU).
- In locale, utilizzando l'Installazione guidata.

Kaspersky Endpoint Security supporta la selezione automatica dei componenti quando si effettua l'upgrade dell'applicazione in un computer con l'applicazione Kaspersky Endpoint Agent installata. La selezione automatica dei componenti dipende dalle autorizzazioni dell'account utente che sta effettuando l'upgrade dell'applicazione.

Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando il file EXE o MSI nell'account di sistema (SYSTEM), Kaspersky Endpoint Security ottiene l'accesso alle licenze correnti delle soluzioni Kaspersky. Pertanto, se nel computer è installato Kaspersky Endpoint Agent e la soluzione EDR Optimum è attivata, il programma di installazione di Kaspersky Endpoint Security configura automaticamente il set di componenti e seleziona il componente EDR Optimum. In questo modo, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent. L'esecuzione del programma di installazione MSI nell'account di sistema (SYSTEM) viene in genere eseguita quando si effettua l'upgrade tramite Kaspersky Update Service (SMU) o quando si distribuisce un pacchetto di installazione tramite Kaspersky Security Center.

Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando un file MSI in un account utente senza privilegi, Kaspersky Endpoint Security non sarà in grado di accedere alle licenze correnti delle soluzioni Kaspersky. In questo caso, Kaspersky Endpoint Security seleziona automaticamente i componenti in base alla configurazione di Kaspersky Endpoint Agent. A questo punto, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent.

6. **Riavvio del computer**

   Riavviare il computer per completare l'aggiornamento dell'applicazione con l'agente integrato. Quando si effettua l'upgrade dell'applicazione, il programma di installazione rimuove Kaspersky Endpoint Agent prima che il computer venga riavviato. Una volta riavviato il computer, il programma di installazione aggiunge l'agente integrato. In altre parole, Kaspersky Endpoint Security non esegue le funzioni di EDR e Kaspersky Sandbox finché il computer non viene riavviato.

7. **Verifica dell'integrità di Kaspersky Endpoint Detection and Response Optimum e Kaspersky Sandbox**

Se dopo l'upgrade il computer presenta lo stato *Critico* nella console di Kaspersky Security Center:

- Accertarsi che nel computer sia installato Network Agent versione 13.2 o successiva.
- Controllare lo stato operativo dell'agente integrato visualizzando *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non installato*, installare il componente tramite l'attività *Modifica i componenti dell'applicazione*.
- Accertarsi di accettare l'Informativa di Kaspersky Security Network nel nuovo criterio di Kaspersky Endpoint Security for Windows.

- Assicurarsi che la funzionalità EDR Optimum sia attivata utilizzando il *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non incluso nella licenza*, accertarsi che la funzionalità di distribuzione della chiave di licenza automatica di EDR Optimum sia attivata.

Migrazione di criteri e attività per Kaspersky Endpoint Agent

Kaspersky Endpoint Security for Windows include una procedura guidata per la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security. È possibile eseguire la migrazione delle impostazioni di criteri e attività per le seguenti soluzioni:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Una procedura guidata per la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security funziona solo in Web Console e Cloud Console. In Administration Console (MMC), è possibile eseguire la migrazione delle impostazioni solo per la soluzione Kaspersky Anti Targeted Attack Platform (EDR) utilizzando la Migrazione guidata standard dei criteri e delle attività di Kaspersky Security Center.

È consigliabile iniziare con la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security su un singolo computer, quindi di eseguire l'operazione su un gruppo di computer e completare la migrazione su tutti i computer dell'organizzazione.

Per eseguire la migrazione delle impostazioni di criteri e attività da Kaspersky Endpoint Agent a Kaspersky Endpoint Security,

nella finestra principale di Web Console, fare clic su **Operazioni → Migrazione da Kaspersky Endpoint Agent**.

Viene eseguita la migrazione guidata di criteri e attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Migrazione dei criteri

La migrazione guidata crea un nuovo criterio che unisce le impostazioni dei criteri di Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Nell'elenco dei criteri, selezionare i criteri di Kaspersky Endpoint Agent di cui si desidera unire le impostazioni con il criterio di Kaspersky Endpoint Security. Fare clic sul criterio di Kaspersky Endpoint Agent per selezionare il criterio di Kaspersky Endpoint Security con cui unire le impostazioni. Verificare di aver selezionato i criteri corretti, quindi procedere con il passaggio successivo.

Passaggio 2. Migrazione delle attività

La migrazione guidata crea nuove attività per Kaspersky Endpoint Security. Nell'elenco delle attività, selezionare le attività di Kaspersky Endpoint Agent che si desidera creare per il criterio di Kaspersky Endpoint Security. La procedura guidata supporta le attività di Kaspersky Endpoint Detection and Response e Kaspersky Sandbox. Procedere con il passaggio successivo.

Passaggio 3. Completamento della procedura guidata

Terminare la procedura guidata. Di conseguenza, la procedura guidata esegue le seguenti operazioni:

- Crea un nuovo criterio di Kaspersky Endpoint Security.

  Il criterio unisce le impostazioni da Kaspersky Endpoint Security e Kaspersky Endpoint Agent Il criterio è denominato *<Nome del criterio di Kaspersky Endpoint Security> e <Nome del criterio di Kaspersky Endpoint Agent>*. Il nuovo criterio presenta lo stato *Inattivo*. Per continuare, modificare gli stati dei criteri di Kaspersky Endpoint Agent e Kaspersky Endpoint Security in *Inattivo* e attivare il nuovo criterio unito.

  > Dopo aver eseguito la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows, accertarsi che la funzionalità di trasferimento dei dati ad Administration Server (dati dei file in quarantena e dati della catena di sviluppo delle minacce) sia configurata. I valori del parametro di trasferimento dei dati non vengono migrati dal criterio di Kaspersky Endpoint Agent.

  Durante la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security per la soluzione Kaspersky Anti Targeted Attack Platform (EDR), è possibile che si verifichino errori durante la connessione del computer ai server di Central Node. Questa situazione è causata dalla migrazione guidata in Web Console, che ignora le seguenti impostazioni dei criteri e non le migra:

  - Divieto di modifica delle impostazioni **Connessione ai server KATA** ("lucchetto").

    Per impostazione predefinita, le impostazioni possono essere modificate (il "lucchetto" è aperto). Pertanto, le impostazioni non vengono applicate al computer. È necessario vietare la modifica delle impostazioni e chiudere il "lucchetto".

  - Contenitore crittografico.

    Se si utilizza l'autenticazione a due vie per la connessione ai server di Central Node, è necessario aggiungere di nuovo il contenitore crittografico. La migrazione guidata migra correttamente il certificato TLS del server.

  La Migrazione guidata dei criteri e delle attività in Administration Console (MMC) migra tutte le impostazioni per la soluzione Kaspersky Anti Targeted Attack Platform (EDR).

- Crea nuove attività di Kaspersky Endpoint Security.

  Le nuove attività sono copie delle attività di Kaspersky Endpoint Agent per Kaspersky Endpoint Detection and Response e Kaspersky Sandbox. Allo stesso tempo, la procedura guidata lascia le attività Kaspersky Endpoint Agent immutate.

Come eseguire la migrazione delle impostazioni di criteri e attività da Kaspersky Endpoint Agent a Kaspersky Endpoint Security in Administration Console (MMC) (solo per KATA (EDR))

1. In Administration Console, selezionare Administration Server e fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.

2. Selezionare **Tutte le attività → Conversione guidata in batch criteri e attività**.

Viene avviata la procedura Conversione guidata criteri e attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione dell'applicazione con cui è necessario convertire i criteri e le attività

In questa fase, è necessario selezionare Kaspersky Endpoint Security for Windows. Procedere con il passaggio successivo.

Passaggio 2. Conversione dei criteri

La Migrazione guidata crea un nuovo criterio di Kaspersky Endpoint Security in cui verranno migrate le impostazioni del criterio di Kaspersky Endpoint Agent. Nell'elenco dei criteri, selezionare i criteri di Kaspersky Endpoint Agent di cui si desidera trasferire le impostazioni nel criterio di Kaspersky Endpoint Security. Procedere con il passaggio successivo.

A questo punto, la migrazione guidata inizia a convertire i criteri. Durante la conversione dei criteri, la Migrazione guidata richiede di accettare l'Informativa di Kaspersky Security Network. I nuovi criteri verranno denominati *<nome criterio> (convertito)*.

Passaggio 3. Conversione delle attività

Ignorare questo passaggio. La procedura guidata supporta solo le attività di Kaspersky Endpoint Detection and Response Optimum e Kaspersky Sandbox. La gestione di questi componenti è disponibile solo in Web Console. Procedere con il passaggio successivo.

Passaggio 4. Completamento della procedura guidata

Terminare la procedura guidata. Come risultato della procedura guidata, verrà creato un nuovo criterio di Kaspersky Endpoint Security.

Endpoint Detection and Response Agent (EDR Agent)

A partire da Kaspersky Endpoint Security 12.3 for Windows, l'applicazione include la configurazione di Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* è un'applicazione che viene installata su singole workstation e server nell'infrastruttura IT dell'organizzazione per supportare le seguenti soluzioni Detection and Response di Kaspersky:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (a partire dalla versione 12.6)
- Kaspersky Anti Targeted Attack Platform (NDR) (a partire dalla versione 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (a partire dalla versione 12.11)

EDR Agent non supporta l'integrazione con la soluzione Kaspersky Endpoint Detection and Response Expert (cloud).

EDR Agent monitora continuamente i processi in esecuzione su questi computer, le connessioni di rete aperte e i file modificati. I componenti di protezione e controllo dell'applicazione non sono disponibili per EDR Agent.

EDR Agent è compatibile con le applicazioni PPE di terzi. Ciò consente di utilizzare strumenti di sicurezza dell'infrastruttura di terzi insieme a Kaspersky Detection and Response.

Per distribuire EDR Agent, nel computer deve essere installato Network Agent e il computer deve essere aggiunto alla console di Kaspersky Security Center. Per abilitare l'interazione di EDR Agent con Kaspersky Security Center, è necessario installare il plug-in di gestione Kaspersky Endpoint Security for Windows. È possibile specificare le impostazioni di EDR Agent utilizzando un criterio di gruppo. Per integrare EDR Agent, è necessario configurare l'integrazione nelle sezioni appropriate del criterio.

Le seguenti applicazioni Kaspersky devono essere installate sull'infrastruttura per supportare le soluzioni Kaspersky Detection and Response:

	• Network Agent • EDR Agent
Endpoint	
	Plug-in di gestione di Kaspersky Endpoint Security for Windows
Kaspersky Security Center	
	
Soluzioni Detection and Response: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

Installazione di EDR Agent

Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent (EDR Agent) per le soluzioni Kaspersky Detection and Response viene installato allo stesso modo.

EDR Agent può essere installato nel computer in uno dei seguenti modi:

- Da remoto tramite Kaspersky Security Center.
- In locale, utilizzando l'Installazione guidata.
- In locale sulla riga di comando (solo per KATA (EDR) ed EDR Expert (on-premises)).

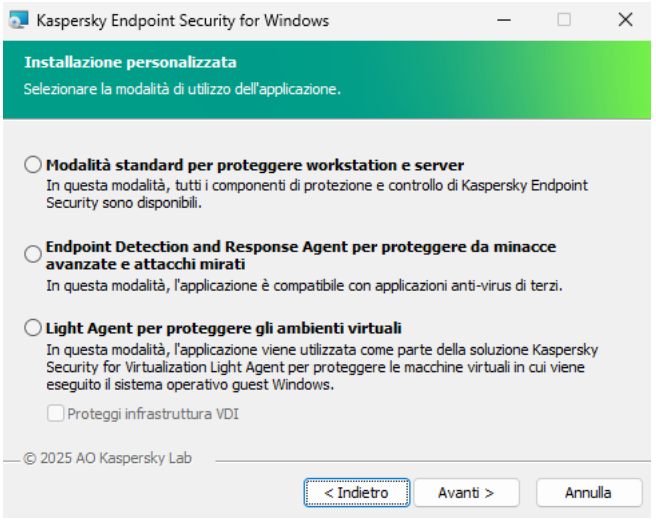
Per installare EDR Agent, è necessario selezionare la configurazione appropriata nelle impostazioni del pacchetto di installazione o in Installazione guidata.

Come installare EDR Agent utilizzando l'Installazione guidata

1. Copiare la cartella del kit di distribuzione nel computer dell'utente.
2. Eseguire setup_kes.exe.

   Verrà avviata l'Installazione guidata.

Configurazione di Kaspersky Endpoint Security



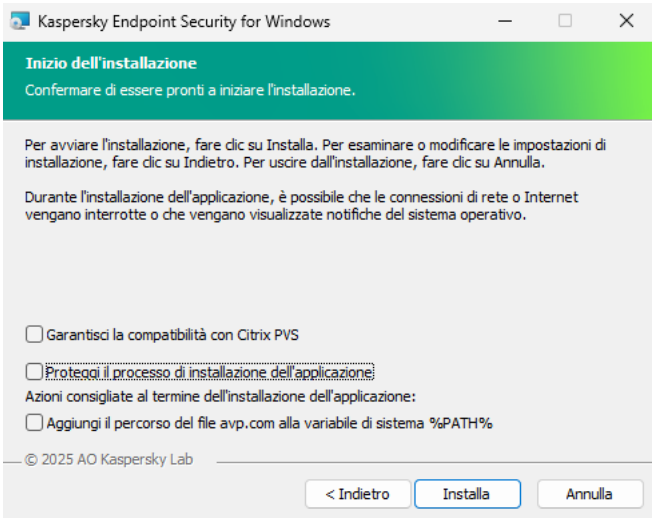
Scelta della configurazione dell'applicazione

Selezionare la configurazione **Endpoint Detection and Response Agent**. In questa configurazione, è possibile installare solo i componenti che forniscono supporto per le soluzioni Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), così come KUMA. Questa configurazione è necessaria se nell'organizzazione viene distribuita una Endpoint Protection Platform (EPP) di terzi insieme a una soluzione Kaspersky Detection and Response. Ciò rende Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent compatibile con le applicazioni EPP di terzi.

Componenti di Kaspersky Endpoint Security

Selezionare i componenti che si desidera installare. È possibile modificare i componenti dell'applicazione disponibili dopo l'installazione dell'applicazione. A tale scopo, è necessario eseguire nuovamente l'Installazione guidata e scegliere di modificare i componenti disponibili.

Impostazioni avanzate



Impostazioni avanzate di installazione dell'applicazione

Proteggi il processo di installazione dell'applicazione. La protezione dell'installazione include la protezione dalla sostituzione del pacchetto di distribuzione con applicazioni dannose, bloccando l'accesso alla cartella di installazione di Kaspersky Endpoint Security e bloccando l'accesso alla sezione del Registro di sistema che contiene le chiavi dell'applicazione. Se tuttavia è impossibile installare l'applicazione (ad esempio, durante l'esecuzione dell'installazione remota tramite Windows Remote Desktop), è possibile disabilitare la protezione del processo di installazione.

Garantisci la compatibilità con Citrix PVS. È possibile abilitare il supporto di Citrix Provisioning Services per installare Kaspersky Endpoint Security in una macchina virtuale.

Aggiungi il percorso del file avp.com alla variabile di sistema %PATH%. È possibile aggiungere il percorso di installazione alla variabile %PATH% per agevolare l'utilizzo dell'interfaccia della riga di comando.

Come installare EDR Agent dalla riga di comando (solo per KATA (EDR) e EDR Expert (on-premises))

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.

2. Passare alla cartella in cui si trova il pacchetto di distribuzione di Kaspersky Endpoint Security.

3. Eseguire il seguente comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
```

oppure

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

Di conseguenza, nel computer viene installata l'applicazione EDR Agent per l'integrazione con Kaspersky Anti Targeted Attack Platform (EDR) o Kaspersky Endpoint Detection and Response Expert (on-premises). È possibile verificare che l'applicazione sia installata e controllare le impostazioni dell'applicazione eseguendo il comando `status`.

Come installare EDR Agent utilizzando Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare la cartella **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.

   Si aprirà un elenco di pacchetti di installazione che sono stati scaricati in Kaspersky Security Center.
3. Aprire le proprietà del pacchetto di installazione.

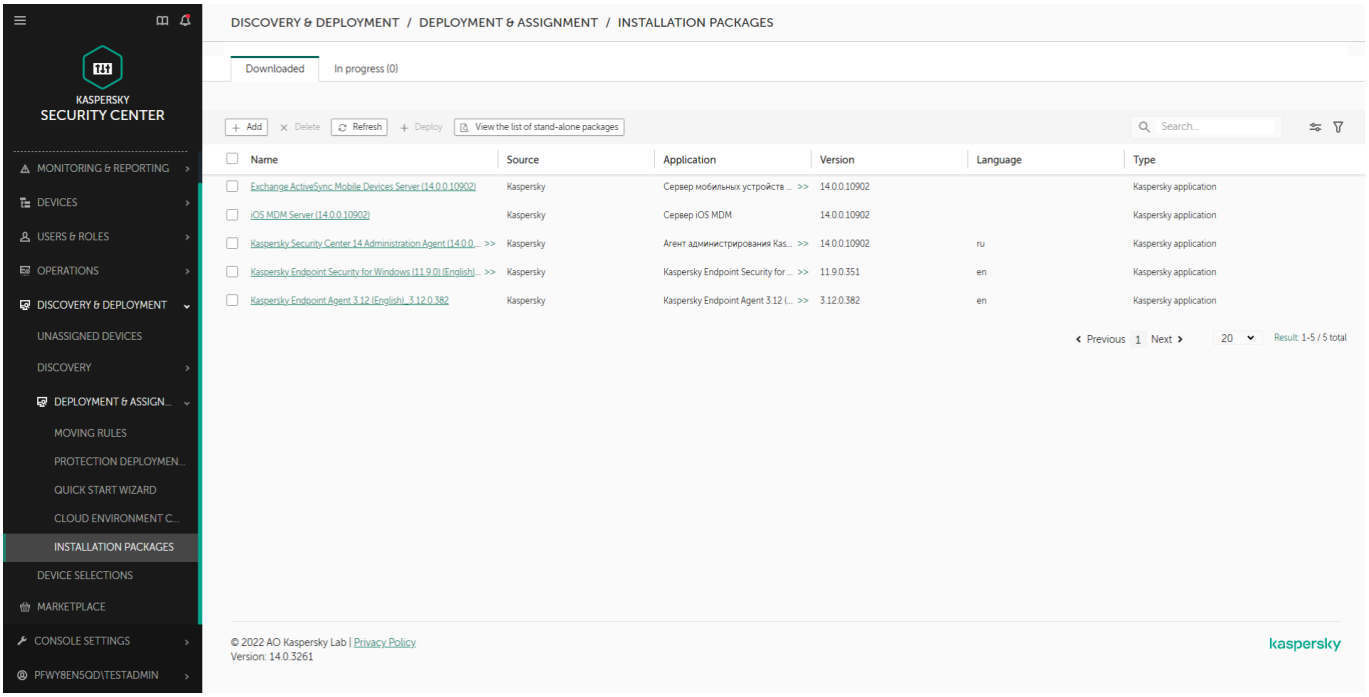
   Se necessario, creare un nuovo pacchetto di installazione.
4. Passare alla sezione **Componenti della protezione**.
5. Selezionare la configurazione **Endpoint Detection and Response Agent per proteggere da minacce avanzate e attacchi mirati**. In questa configurazione, è possibile installare solo i componenti che forniscono supporto per le soluzioni Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), così come KUMA. Questa configurazione è necessaria se nell'organizzazione viene distribuita una Endpoint Protection Platform (EPP) di terzi insieme a una soluzione Kaspersky Detection and Response. Ciò rende Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent compatibile con le applicazioni EPP di terzi.
6. Selezionare i componenti che si desidera installare.

   È possibile modificare i componenti dell'applicazione disponibili dopo l'installazione dell'applicazione.
7. Salvare le modifiche.
8. Creare di un'attività di installazione remota. Nelle proprietà dell'attività, quindi selezionare il pacchetto di installazione creato.

Come installare EDR Agent utilizzando Web Console

1. Nella finestra principale di Web Console, fare clic su **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

Si aprirà un elenco di pacchetti di installazione che sono stati scaricati in Kaspersky Security Center.



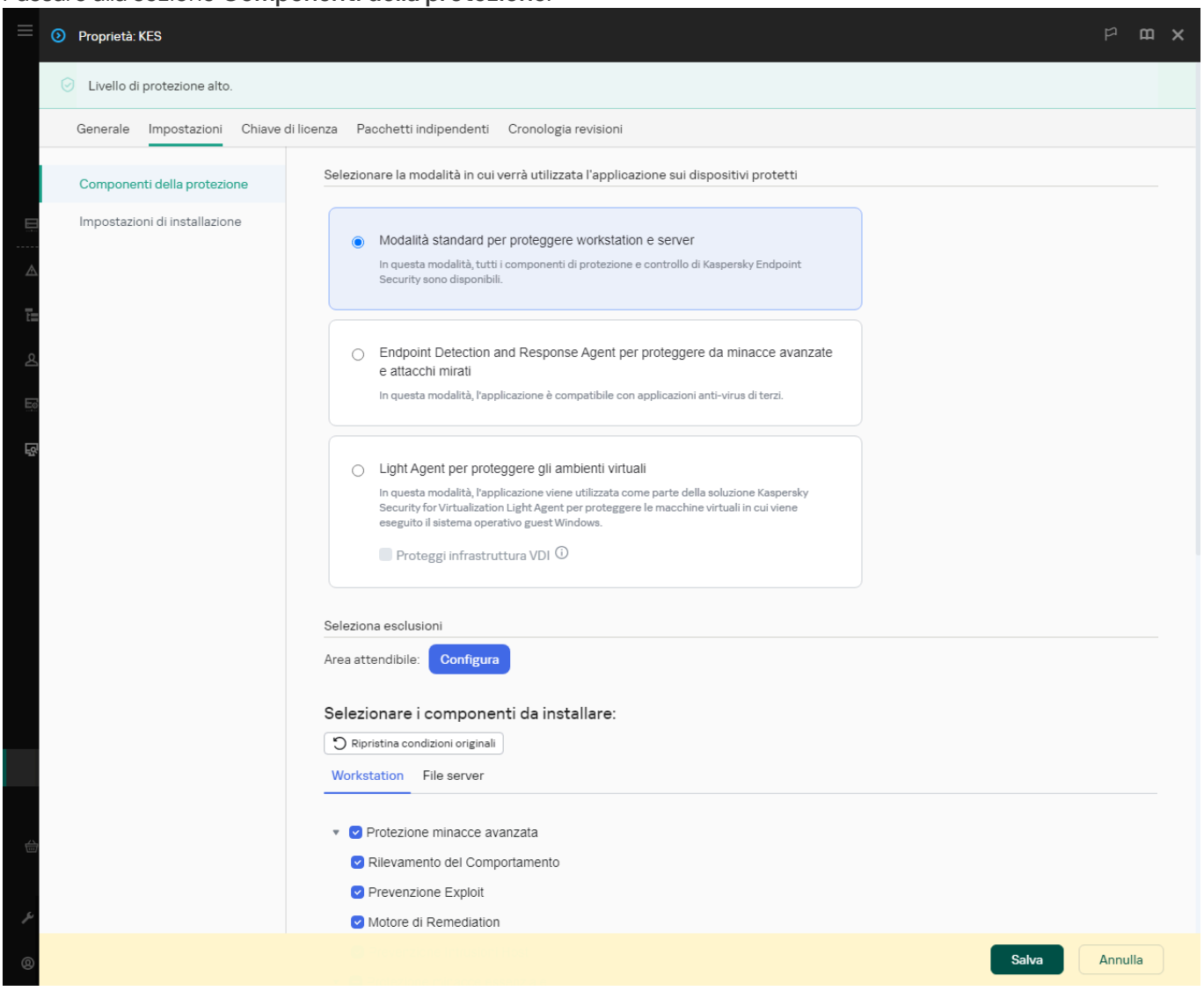
Elenco dei pacchetti di installazione

2. Aprire le proprietà del pacchetto di installazione.

   Se necessario, creare un nuovo pacchetto di installazione.

3. Selezionare la scheda **Impostazioni**.

4. Passare alla sezione **Componenti della protezione**.



Componenti inclusi nel pacchetto di installazione

5. Selezionare la configurazione **Endpoint Detection and Response Agent**. In questa configurazione, è possibile installare solo i componenti che forniscono supporto per le soluzioni Detection and Response: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises), così come KUMA. Questa configurazione è necessaria se nell'organizzazione viene distribuita una Endpoint Protection Platform (EPP) di terzi insieme a una soluzione Kaspersky Detection and Response. Ciò rende Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent compatibile con le applicazioni EPP di terzi.

6. Selezionare i componenti che si desidera installare.

   È possibile modificare i componenti dell'applicazione disponibili dopo l'installazione dell'applicazione.

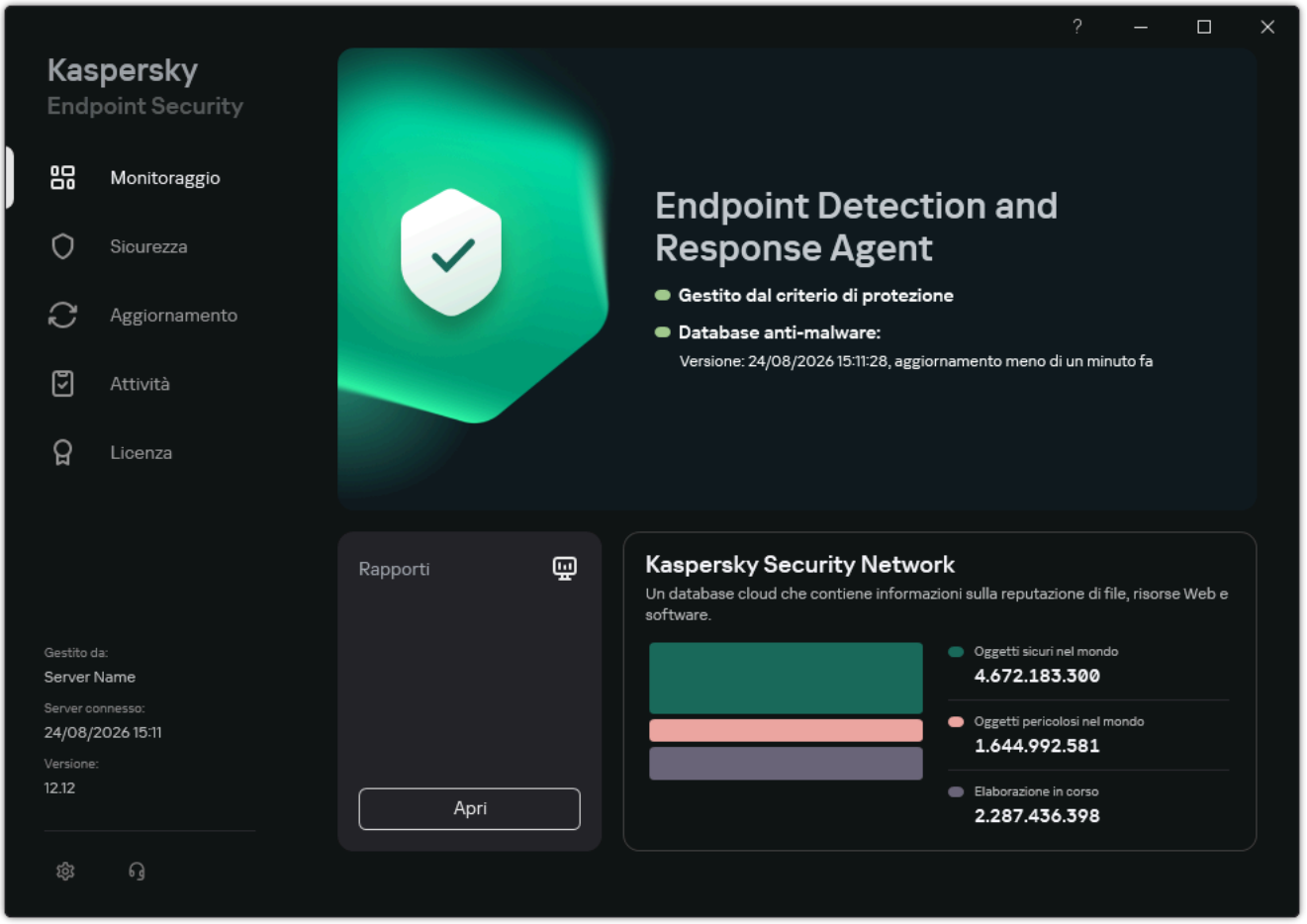
7. Salvare le modifiche.

8. Creare di un'attività di installazione remota. Nelle proprietà dell'attività, quindi selezionare il pacchetto di installazione creato.

Di conseguenza, EDR Agent viene installato nel computer dell'utente. È possibile utilizzare l'interfaccia dell'applicazione e nell'area di notifica viene visualizzata un'icona dell'applicazione .

In Kaspersky Security Center, il computer in cui è installata l'applicazione nella configurazione di EDR Agent presenta lo stato *Critico* - . Il computer presenta questo stato perché il componente Protezione minacce file è assente. Non è necessario eseguire alcuna azione.

Se non è stato possibile installare EDR Agent in un computer con un'applicazione EPP di terzi perché il programma di installazione ha rilevato software incompatibile nel computer, è possibile ignorare il controllo del software incompatibile.



Finestra principale di EDR Agent

A questo punto, è necessario configurare l'integrazione con la soluzione Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) o Kaspersky Anti Targeted Attack (NDR). È inoltre possibile specificare le impostazioni avanzate dell'applicazione e, ad esempio, creare un'area attendibile o nascondere l'interfaccia dell'applicazione. Sono disponibili le impostazioni nelle seguenti sezioni:

- Kaspersky Security Network
- Impostazioni applicazione
- Impostazioni di rete
- Esclusioni
- Rapporti

- Interfaccia
- Gestione impostazioni

Integrazione di EDR Agent con MDR

EDR Agent è installato su workstation e server nell'infrastruttura IT dell'organizzazione. EDR Agent elabora i dati e li invia tramite i flussi di Kaspersky Security Network a Kaspersky Managed Detection and Response.

Affinché Kaspersky Managed Detection and Response funzioni con Administration Server tramite Kaspersky Security Center Web Console, è necessario stabilire una nuova connessione sicura: una *connessione in background*. Kaspersky Managed Detection and Response richiede di stabilire una connessione in background durante la distribuzione della soluzione. Verificare che la connessione in background venga stabilita.

Stabilire una connessione in background in Web Console

1. Nella finestra principale di Web Console, fare clic su **Impostazioni** → **Integrazione**.
2. Passare alla sezione **Integrazione**.
3. Attivare l'interruttore **Connessione in background per l'integrazione Abilitato**.
4. Salvare le modifiche.

L'integrazione con Kaspersky Managed Detection and Response prevede i seguenti passaggi:

1. **Installazione del componente Managed Detection and Response**

   È possibile selezionare il componente MDR durante l'installazione o l'upgrade, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

   > Per installare il componente Managed Detection and Response senza riavviare il computer utilizzando l'attività *Modifica i componenti dell'applicazione*, è necessario disabilitare l'opzione **Controlla le applicazioni di terzi incompatibili** nelle impostazioni dell'attività.

2. **Configurazione di Kaspersky Private Security Network**

   > Ignorare questo passaggio se si utilizza Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configura automaticamente Kaspersky Private Security Network quando si installa il plug-in MDR.

   Kaspersky Private Security Network (KPSN) è una soluzione che consente agli utenti di computer che ospitano Kaspersky Endpoint Security o altre applicazioni Kaspersky di ottenere l'accesso ai database di reputazione di Kaspersky e ad altri dati statistici senza inviare dati a Kaspersky dai propri computer.

   Caricare il file di configurazione di Kaspersky Security Network nelle proprietà di Administration Server. Il file di configurazione di Kaspersky Security Network si trova nell'archivio ZIP del file di configurazione MDR. È possibile ottenere l'archivio ZIP in Kaspersky Managed Detection and Response Console. Per informazioni dettagliate su Kaspersky Private Security Network, consultare la Guida di Kaspersky Security Center. È inoltre possibile caricare un file di configurazione di Kaspersky Security Network nel computer dalla riga di comando (vedere le istruzioni di seguito).

Come configurare l'istanza privata di Kaspersky Private Security Network dalla riga di comando

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.
3. Eseguire il seguente comando:

   ```
   avp.com KSN /private <file name>
   ```

   dove `<file name>` è il nome del file di configurazione contenente le impostazioni di Kaspersky Private Security Network (formato file PKCS7 o PEM).

   Esempio:
   `avp.com KSN /private C:\kpsn_config.pkcs7`

Di conseguenza, Kaspersky Endpoint Security utilizzerà Kaspersky Private Security Network per determinare la reputazione di file, applicazioni e siti Web. La sezione **Kaspersky Security Network** delle impostazioni dei criteri mostrerà il seguente stato operativo: *Infrastruttura: Kaspersky Private Security Network*.

Per consentire il funzionamento di Managed Detection and Response è necessario abilitare la modalità KSN estesa.

3. **Attivazione di Kaspersky Managed Detection and Response**

A partire da Kaspersky Endpoint Security for Windows 12.10, per attivare la funzionalità Managed Detection and Response, in alternativa a un codice di attivazione, è inoltre possibile utilizzare un file chiave.

È necessario acquistare una licenza separata per MDR (componente aggiuntivo Kaspersky Managed Detection and Response).

La funzionalità diventa disponibile dopo aver aggiunto una chiave separata per il componente aggiuntivo Kaspersky Managed Detection and Response. La licenza per la funzionalità Managed Detection and Response standalone è la stessa della licenza di Kaspersky Endpoint Security.

Verificare che la funzionalità MDR sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

4. **Abilitazione del componente Managed Detection and Response**

Caricare il file di configurazione BLOB nel criterio di Kaspersky Endpoint Security (vedere le istruzioni di seguito). Il file BLOB contiene l'ID client e le informazioni sulla licenza per Kaspersky Managed Detection and Response. Il file BLOB si trova nell'archivio ZIP del file di configurazione MDR. È possibile ottenere l'archivio ZIP in Kaspersky Managed Detection and Response Console. Per informazioni dettagliate su un file BLOB, consultare la Guida di Kaspersky Managed Detection and Response.

A partire da Kaspersky Endpoint Security 12.6 for Windows, l'aggiunta di un file BLOB è facoltativa per Kaspersky Managed Detection and Response senza tenant se si dispone di una licenza corrente.

Come abilitare Managed Detection and Response in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.

4. Selezionare la casella di controllo **Managed Detection and Response (Industrial CyberSecurity)**.

5. Nella sezione **Impostazioni** fare clic su **Carica** e selezionare il file BLOB ricevuto in Kaspersky Managed Detection and Response Console. Il file ha l'estensione P7.

   Per impostazione predefinita, l'utente può gestire le impostazioni dell'applicazione (il "lucchetto" è aperto). Per applicare il criterio nei computer, chiudere i lucchetti .

6. Salvare le modifiche.

Come abilitare il componente Managed Detection and Response in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Configurazione agenti integrati** → **Managed Detection and Response**.

5. Attivare l'interruttore **Managed Detection and Response ABILITATO**.

6. Fare clic su **Carica** e selezionare il file BLOB ottenuto in Kaspersky Managed Detection and Response Console. Il file ha l'estensione P7.

   Per impostazione predefinita, l'utente può gestire le impostazioni dei criteri (il "lucchetto" è aperto). Per applicare il criterio nei computer, chiudere i lucchetti .

7. Salvare le modifiche.

Come abilitare il componente Managed Detection and Response dalla riga di comando

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.

2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

3. Eseguire il seguente comando:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Per eseguire questo comando, Protezione tramite password deve essere abilitato. L'utente deve avere l'autorizzazione **Configura le impostazioni dell'applicazione**.

Successivamente Kaspersky Endpoint Security verificherà il file BLOB. La verifica del file BLOB include il controllo della firma digitale e del periodo licenza. Se il file BLOB viene verificato, Kaspersky Endpoint Security scaricherà il file e lo invierà al computer durante la successiva sincronizzazione con Kaspersky Security Center. Controllare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Managed Detection and Response** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

5. **Configurazione di altri componenti dell'applicazione per la ricezione della telemetria**

   Per consentire il funzionamento di Managed Detection and Response, è necessario abilitare i seguenti componenti.

   - Kaspersky Security Network (modalità estesa).
   - Rilevamento del Comportamento.
   - Prevenzione Exploit.
   - Protezione minacce web.
   - Protezione minacce di posta.
   - Protezione minacce file.
   - Protezione minacce di rete.
   - Firewall.
   - Protezione AMSI.
   - Scansione in background.

     1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
     2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

        Verrà visualizzata la finestra delle proprietà del criterio.
     3. Selezionare la scheda **Impostazioni applicazione**.
     4. Passare a **Configurazione agenti integrati** → **Managed Detection and Response**.
     5. Attivare l'interruttore **Managed Detection and Response ABILITATO**.
     6. Salvare le modifiche.

     1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
     2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
     3. Nella finestra del criterio, selezionare **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
     4. Selezionare la casella di controllo **Managed Detection and Response (Industrial CyberSecurity)**.
     5. Salvare le modifiche.

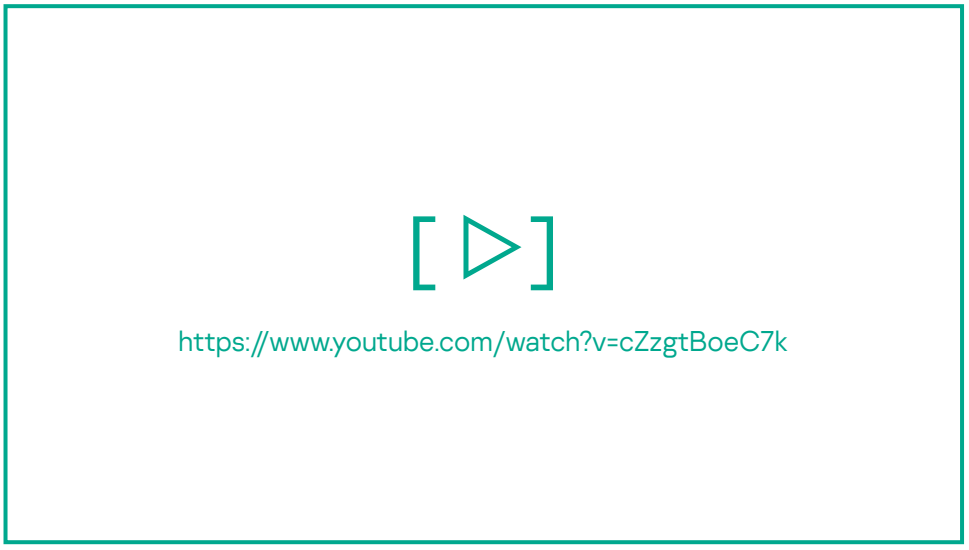
Integrazione di EDR Agent con EDR (KATA)

EDR Agent è installato su workstation e server nell'infrastruttura IT dell'organizzazione. Su questi computer, EDR Agent monitora continuamente i processi, le connessioni di rete aperte e i file modificati e invia i dati di monitoraggio al server con il componente Central Node.

Per l'integrazione con EDR (KATA), è necessario abilitare il componente Endpoint Detection and Response (KATA) e configurare EDR Agent.

Per il corretto funzionamento di Endpoint Detection and Response (KATA), è necessario soddisfare le seguenti condizioni:

- Kaspersky Anti Targeted Attack Platform versioni 5.0–7.1.
- Kaspersky Security Center versione 14.2 o successiva. Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità Endpoint Detection and Response (KATA).



https://www.youtube.com/watch?v=cZzgtBoeC7k

L'integrazione con Endpoint Detection and Response (KATA) prevede i seguenti passaggi:

1. **Attivazione di Endpoint Detection and Response (KATA)**

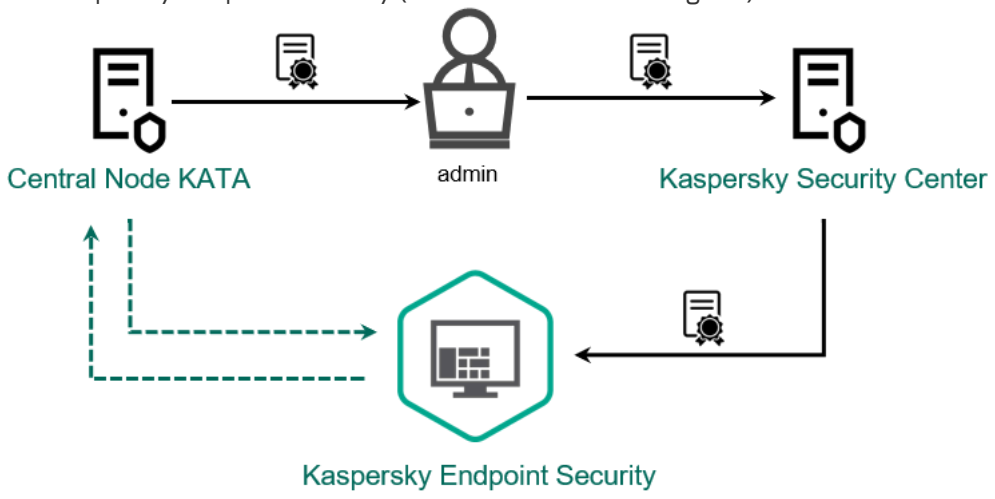
   È necessario acquistare una licenza separata per EDR (KATA) (componente aggiuntivo Kaspersky Endpoint Detection and Response (KATA)).

   La funzionalità diventa disponibile dopo aver aggiunto una chiave separata per Kaspersky Endpoint Detection and Response (KATA). La licenza per la funzionalità Endpoint Detection and Response (KATA) autonoma è la stessa della licenza di Kaspersky Endpoint Security.

   Verificare che la funzionalità EDR (KATA) sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

2. **Connessione a Central Node**

Kaspersky Anti Targeted Attack Platform richiede di stabilire una connessione attendibile tra Kaspersky Endpoint Security e il componente Central Node. Per configurare una connessione attendibile, è necessario utilizzare un certificato TLS. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Quindi è necessario aggiungere il certificato TLS a Kaspersky Endpoint Security (vedere le istruzioni di seguito).



Aggiunta di un certificato TLS a Kaspersky Endpoint Security

Per impostazione predefinita, Kaspersky Endpoint Security controlla solo il certificato TLS di Central Node. Per rendere la connessione più sicura, è inoltre possibile abilitare la verifica del computer in Central Node (autenticazione a due vie). Per abilitare questa verifica, è necessario attivare l'autenticazione a due vie nelle impostazioni di Central Node e Kaspersky Endpoint Security. Per utilizzare l'autenticazione a due vie, è necessario anche un contenitore crittografico. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform).

Come connettere un computer Kaspersky Endpoint Security a Central Node tramite Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Detection and Response → Endpoint Detection and Response Expert (on-premises)**.
5. Selezionare la casella di controllo **Endpoint Detection and Response Expert (on-premises)**.
6. Fare clic su **Impostazioni della connessione al server**.
7. Configurare la connessione al server:
   - **Timeout (sec)**. Timeout massimo di risposta del server di Central Node. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server Central Node.
   - **Certificato TLS del server**. Certificato TLS per stabilire una connessione attendibile con il server di Central Node. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform).

- **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

  Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

8. Fare clic su **OK**.
9. Aggiungere i server di Central Node. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.

   È possibile aggiungere più indirizzi server di Central Node. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.
10. Se necessario, configurare la telemetria.
11. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come connettere un computer Kaspersky Endpoint Security a Central Node tramite Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response Expert (on-premises)**.
5. Attivare l'interruttore **Endpoint Detection and Response Expert (on-premises) ABILITATO**.
6. Per configurare EDR (KATA), selezionare **Endpoint Detection and Response Expert (versione 7.1 o precedente)** dall'elenco delle soluzioni.
7. Fare clic su **Impostazioni di connessione**.
8. Configurare la connessione al server:

   - **Timeout (sec)**. Timeout massimo di risposta del server di Central Node. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server Central Node.
   - **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server di Central Node. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform).

- **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

  Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

9. Fare clic su **OK**.
10. Aggiungere i server di Central Node. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.

    È possibile aggiungere più indirizzi server di Central Node. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.
11. Se necessario, configurare la telemetria.
12. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Di conseguenza, il computer viene aggiunto alla console di Kaspersky Anti Targeted Attack Platform. Controllare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Endpoint Detection and Response Expert (on-premises)** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

Integrazione di EDR Agent con NDR (KATA)

EDR Agent è installato su workstation e server nell'infrastruttura IT dell'organizzazione. Su questi computer, EDR Agent monitora continuamente i processi, le connessioni di rete aperte e i file modificati e invia i dati di monitoraggio al server con il componente Central Node.

Per l'integrazione con NDR (KATA), è necessario abilitare il componente Network Detection and Response (KATA) e configurare EDR Agent.

Per il corretto funzionamento di Network Detection and Response (KATA), è necessario soddisfare le seguenti condizioni:

- Kaspersky Anti Targeted Attack Platform versione 7.0 o successiva.
- Kaspersky Security Center versione 14.2 o successiva. Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità Network Detection and Response (KATA).

https://www.youtube.com/watch?v=gd-rySv0ThQ

L'integrazione con Network Detection and Response (KATA) prevede i seguenti passaggi:

1. **Attivazione di Network Detection and Response (KATA)**

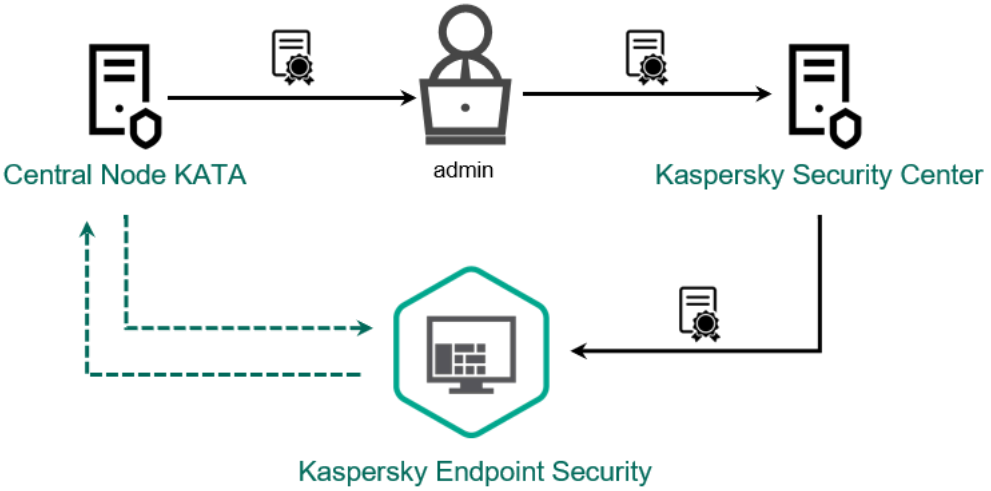
   È necessario acquistare una licenza separata per NDR (KATA) (componente aggiuntivo Kaspersky Network Detection and Response (KATA)).

   La funzionalità diventa disponibile dopo aver aggiunto una chiave separata per Kaspersky Network Detection and Response (KATA). La licenza per la funzionalità Network Detection and Response (KATA) autonoma è la stessa della licenza di Kaspersky Endpoint Security.

   Verificare che la funzionalità NDR (KATA) sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

2. **Connessione a Central Node**

   Kaspersky Anti Targeted Attack Platform richiede di stabilire una connessione attendibile tra Kaspersky Endpoint Security e il componente Central Node. Per configurare una connessione attendibile, è necessario utilizzare un certificato TLS. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Quindi è necessario aggiungere il certificato TLS a Kaspersky Endpoint Security (vedere le istruzioni di seguito).



Aggiunta di un certificato TLS a Kaspersky Endpoint Security

Per impostazione predefinita, Kaspersky Endpoint Security controlla solo il certificato TLS di Central Node. Per rendere la connessione più sicura, è inoltre possibile abilitare la verifica del computer in Central Node (autenticazione a due vie). Per abilitare questa verifica, è necessario attivare l'autenticazione a due vie nelle impostazioni di Central Node e Kaspersky Endpoint Security. Per utilizzare l'autenticazione a due vie, è necessario anche un contenitore crittografico. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform).

Come connettere un computer Kaspersky Endpoint Security a Central Node tramite Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Detection and Response** → **Network Detection and Response (KATA)**.
4. Selezionare la casella di controllo **Network Detection and Response (KATA)**.
5. Fare clic su **Impostazioni di connessione**.
6. Configurare la connessione al server:
   - **Timeout (sec)**. Timeout massimo di risposta del server di Central Node. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server Central Node.
   - **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server di Central Node. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform).
   - **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

     Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.
7. Fare clic su **OK**.
8. Aggiungere i server di Central Node. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.
9. È possibile aggiungere più indirizzi server di Central Node. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

10. Se necessario, configurare la telemetria.

11. Salvare le modifiche.

Come connettere un computer Kaspersky Endpoint Security a Central Node tramite Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Configurazione agenti integrati → Network Detection and Response (KATA)**.

5. Attivare l'interruttore **Network Detection and Response (KATA) ABILITATO**.

6. Fare clic su **Impostazioni di connessione**.

7. Configurare la connessione al server:

   - **Timeout (sec)**. Timeout massimo di risposta del server di Central Node. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server Central Node.

   - **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server di Central Node. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform).

   - **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

     Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

8. Fare clic su **OK**.

9. Aggiungere i server di Central Node. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.

10. È possibile aggiungere più indirizzi server di Central Node. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

11. Se necessario, configurare la telemetria.

12. Salvare le modifiche.

Di conseguenza, il computer viene aggiunto alla console di Kaspersky Anti Targeted Attack Platform. Controllare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Network Detection and Response (KATA)** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

Integrazione di EDR Agent con EDR Expert (on-premises)

EDR Agent è installato su workstation e server nell'infrastruttura IT dell'organizzazione. Su questi computer, EDR Agent monitora continuamente i processi, le connessioni di rete aperte e i file modificati e invia i dati di monitoraggio al server EDR Expert (on-premises).

Per l'integrazione con le soluzioni EDR Expert (on-premises), è necessario abilitare il componente Endpoint Detection and Response Expert (on-premises e configurare EDR Agent.

L'integrazione con Endpoint Detection and Response Expert (on-premises) prevede i seguenti passaggi:

1. **Attivazione di Kaspersky Endpoint Detection and Response Expert (on-premises)**

   È necessario acquistare una licenza separata per EDR Expert (on-premises) (componente aggiuntivo Kaspersky Endpoint Detection and Response Expert (on-premises)).

   La funzionalità diventa disponibile dopo aver aggiunto una chiave separata per Kaspersky Endpoint Detection and Response Expert (on-premises). La licenza per la funzionalità Endpoint Detection and Response Expert (on-premises) autonoma è la stessa della licenza di Kaspersky Endpoint Security.

   Verificare che la funzionalità EDR Expert (on-premises) sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

2. **Connessione al server di raccolta della telemetria e al server di risposta**

   Kaspersky Endpoint Detection and Response Expert (on-premises) richiede una connessione attendibile tra Kaspersky Endpoint Security e due server:

   - Un *server di raccolta della telemetria* è un server che fa parte di una soluzione SIEM che raccoglie, normalizza, correla, analizza e archivia le informazioni sugli eventi che si verificano nel computer.
   - Un *server di risposta* è un server per la ricezione e la scansione dei dati, lo studio del comportamento degli oggetti e la pubblicazione dei risultati di tali studi.

   Per configurare una connessione attendibile, è necessario utilizzare un certificato TLS. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). Quindi è necessario aggiungere il certificato TLS a Kaspersky Endpoint Security (vedere le istruzioni di seguito).

   Per impostazione predefinita, Kaspersky Endpoint Security controlla solo il certificato TLS dei server. Per rendere la connessione più sicura, è inoltre possibile abilitare la verifica del computer nel server (autenticazione a due vie). Per abilitare questa verifica, è necessario attivare l'autenticazione a due vie nelle impostazioni del server e Kaspersky Endpoint Security. Per utilizzare l'autenticazione a due vie, è necessario anche un contenitore crittografico. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un cripto-contenitore nella piattaforma Open Single Management (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)).

Come connettere un computer Kaspersky Endpoint Security a EDR Expert (on-premises) tramite Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati → Endpoint Detection and Response Expert (on-premises)**.
5. Attivare l'interruttore **Endpoint Detection and Response Expert (on-premises) ABILITATO**.
6. Per configurare EDR Expert (on-premises), selezionare **Endpoint Detection and Response Expert (versione 8.0 o successiva)** dall'elenco delle soluzioni.
7. Configurare la connessione ai *server di raccolta della telemetria*:

   a. Nella sezione **Connessione ai server di raccolta della telemetria**, fare clic sul collegamento **Impostazioni di connessione**.

   b. Configurare la connessione ai server di raccolta della telemetria:

   - **Timeout (sec)**. Timeout massimo del server di KUMA. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server.
   - **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)).
   - **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un cripto-contenitore nella piattaforma Open Single Management (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). Dopo aver configurato le impostazioni del server, è necessario abilitare anche l'autenticazione a due vie nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

     Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

   c. Fare clic su **OK**.

   d. Aggiungere i server di raccolta della telemetria. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.

   È possibile aggiungere più indirizzi di server di raccolta della telemetria. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

   e. Se necessario, configurare la telemetria.

8. Configurare la connessione ai *server di risposta*:

   a. Nel blocco **Connessione ai server di risposta**, configurare l'impostazione **Invia richiesta di sincronizzazione al server ogni (min)**. Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security riceve le attività di risposta alle minacce e invia i risultati delle attività.

   b. Fare clic sul collegamento **Impostazioni di connessione**.

   c. Configurare la connessione ai server di risposta:

      - **Timeout (sec)**. Timeout massimo del server di KUMA. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server.

      - **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)).

      - **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un cripto-contenitore nella piattaforma Open Single Management (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). Dopo aver configurato le impostazioni del server, è necessario abilitare anche l'autenticazione a due vie nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

        Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

   d. Fare clic su **OK**.

   e. Aggiungere i server di risposta. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.

      È possibile aggiungere più indirizzi server di risposta. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Di conseguenza, il computer viene aggiunto nell'OSMP (Open Single Management Platform). Controllare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Endpoint Detection and Response Expert (on-premises)** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

Compatibilità con le applicazioni EPP di terzi

EDR Agent supporta la funzionalità delle soluzioni Kaspersky Detection and Response. I componenti di protezione e controllo non sono disponibili per EDR Agent. Questa configurazione consente l'installazione di applicazioni EPP di terzi e la distribuzione delle soluzioni Kaspersky Detection and Response nell'infrastruttura dell'organizzazione.

EDR Agent è compatibile con le applicazioni EPP dei seguenti fornitori:

- **Dr.Web**

  EDR Agent è compatibile con Dr.Web Agent for Windows versione 13 e Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR Agent è compatibile con Dallas Lock 8.0-C versione 843.2.

  > Per l'esecuzione di EDR Agent in un computer in cui è installato il software Dallas Lock, è necessario consentire la connessione ai servizi esterni di Kaspersky nelle impostazioni del modulo Firewall.

- **Secret Net Studio**

  EDR Agent è compatibile con Secret Net Studio versione 8.11 (20851).

  > L'applicazione non può essere installata in un computer in cui Secret Net Studio è distribuito con il componente Antivirus. Per rendere possibile l'interoperabilità, è necessario rimuovere il componente Antivirus da Secret Net Studio.

- **Trend Micro**

  EDR Agent è compatibile con Trend Micro Vision One (incluso Security Agent versione 14.0.20731).

  EDR Agent è compatibile con Trend Micro Deep Security versione 20.0.3-18160 (incluso Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent è compatibile con Sophos Intercept X versione 2024.1.2 (incluso Endpoint Agent) e Sophos Core Agent versione 2026.2.1.3.

- **Bitdefender**

  EDR Agent è compatibile con Bitdefender Endpoint Security Tools versione 8.26.7.647.

- **ESET**

  EDR Agent è compatibile con ESET Endpoint Security versione 13.0.2044.0 e ESET Management Agent versione 13.2.1189.0.

> Nei computer in cui viene eseguito Windows 11 for Arm64, EDR Agent non è compatibile con Bitdefender Endpoint Security Tools.

Le applicazioni devono essere installate nel seguente ordine: installare innanzitutto l'applicazione EPP, quindi Kaspersky Security Center Network Agent e infine EDR Agent. Ciò è necessario perché il programma di installazione dell'applicazione EPP potrebbe rilevare EDR Agent e Network Agent come software incompatibile e rimuoverli. Il funzionamento di EDR Agent e Network Agent deve essere controllato anche dopo l'aggiornamento dell'applicazione EPP di terzi, poiché il relativo programma di installazione potrebbe eseguire nuovamente la scansione del computer alla ricerca di software incompatibile e rimuovere le applicazioni.

Se non è stato possibile installare EDR Agent in un computer con un'applicazione EPP di terzi perché il programma di installazione ha rilevato software incompatibile nel computer, è possibile ignorare il controllo del software incompatibile.

Managed Detection and Response



Kaspersky Endpoint Security for Windows supporta l'integrazione con la soluzione Managed Detection and Response. La soluzione *Kaspersky Managed Detection and Response (MDR)* rileva e analizza automaticamente gli incidenti di sicurezza nell'infrastruttura. A tale scopo, MDR utilizza i dati di telemetria ricevuti dagli endpoint e dal Machine Learning. MDR invia i dati sugli incidenti agli esperti di Kaspersky. Gli esperti possono quindi elaborare l'incidente e, ad esempio, aggiungere una nuova voce ai database anti-virus. In alternativa, gli esperti possono proporre suggerimenti sull'elaborazione dell'incidente e, ad esempio, suggerire di isolare il computer dalla rete. Per informazioni dettagliate sul funzionamento della soluzione, consultare la Guida di Kaspersky Managed Detection and Response.

Configurazioni di Kaspersky Endpoint Security per l'integrazione con MDR

È possibile utilizzare le seguenti configurazioni per l'utilizzo con MDR:

- **[KES+agente integrato]**. In questa configurazione, Kaspersky Endpoint Security funge sia da applicazione che garantisce la sicurezza del computer sia da applicazione per l'utilizzo con MDR.
- **[EPP di terzi+EDR Agent]**. In questa configurazione, la sicurezza dell'infrastruttura IT è garantita da Endpoint Protection Platform (EPP) di terzi. L'interazione con MDR è fornita da Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent (EDR Agent). In questa configurazione, EDR Agent è compatibile con le applicazioni PPE di terzi.

Integrazione dell'agente integrato con MDR

Per configurare l'integrazione con Kaspersky Managed Detection and Response, è necessario abilitare il componente Managed Detection and Response e configurare Kaspersky Endpoint Security.

Affinché Kaspersky Managed Detection and Response funzioni con Administration Server tramite Kaspersky Security Center Web Console, è necessario stabilire una nuova connessione sicura: una *connessione in background*. Kaspersky Managed Detection and Response richiede di stabilire una connessione in background durante la distribuzione della soluzione. Verificare che la connessione in background venga stabilita.

Stabilire una connessione in background in Web Console

1. Nella finestra principale di Web Console, fare clic su **Impostazioni** → **Integrazione**.
2. Passare alla sezione **Integrazione**.
3. Attivare l'interruttore **Connessione in background per l'integrazione Abilitato**.
4. Salvare le modifiche.

L'integrazione con Kaspersky Managed Detection and Response prevede i seguenti passaggi:

1. **Installazione del componente Managed Detection and Response**

È possibile selezionare il componente MDR durante l'installazione o l'upgrade, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

Per installare il componente Managed Detection and Response senza riavviare il computer utilizzando l'attività *Modifica i componenti dell'applicazione*, è necessario disabilitare l'opzione **Controlla le applicazioni di terzi incompatibili** nelle impostazioni dell'attività.

2 Configurazione di Kaspersky Private Security Network

Ignorare questo passaggio se si utilizza Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configura automaticamente Kaspersky Private Security Network quando si installa il plug-in MDR.

Kaspersky Private Security Network (KPSN) è una soluzione che consente agli utenti di computer che ospitano Kaspersky Endpoint Security o altre applicazioni Kaspersky di ottenere l'accesso ai database di reputazione di Kaspersky e ad altri dati statistici senza inviare dati a Kaspersky dai propri computer.

Caricare il file di configurazione di Kaspersky Security Network nelle proprietà di Administration Server. Il file di configurazione di Kaspersky Security Network si trova nell'archivio ZIP del file di configurazione MDR. È possibile ottenere l'archivio ZIP in Kaspersky Managed Detection and Response Console. Per informazioni dettagliate su Kaspersky Private Security Network, consultare la Guida di Kaspersky Security Center. È inoltre possibile caricare un file di configurazione di Kaspersky Security Network nel computer dalla riga di comando (vedere le istruzioni di seguito).

Come configurare l'istanza privata di Kaspersky Private Security Network dalla riga di comando

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.
3. Eseguire il seguente comando:

   ```
   avp.com KSN /private <file name>
   ```

   dove `<file name>` è il nome del file di configurazione contenente le impostazioni di Kaspersky Private Security Network (formato file PKCS7 o PEM).

   Esempio:
   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Di conseguenza, Kaspersky Endpoint Security utilizzerà Kaspersky Private Security Network per determinare la reputazione di file, applicazioni e siti Web. La sezione **Kaspersky Security Network** delle impostazioni dei criteri mostrerà il seguente stato operativo: *Infrastruttura: Kaspersky Private Security Network*.

Per consentire il funzionamento di Managed Detection and Response è necessario abilitare la modalità KSN estesa.

3 Attivazione di Kaspersky Managed Detection and Response

A partire da Kaspersky Endpoint Security for Windows 12.10, per attivare la funzionalità Managed Detection and Response, in alternativa a un codice di attivazione, è inoltre possibile utilizzare un file chiave.

Kaspersky Managed Detection and Response supporta i seguenti metodi di concessione di licenza:

- La funzionalità Managed Detection and Response è inclusa nella licenza di Kaspersky Endpoint Security for Windows.

  La funzionalità è disponibile immediatamente dopo l'attivazione di Kaspersky Endpoint Security for Windows.

- Viene utilizzata una licenza separata di MDR (componente aggiuntivo di Kaspersky Managed Detection and Response).

  La funzionalità diventa disponibile dopo aver aggiunto una chiave separata per il componente aggiuntivo Kaspersky Managed Detection and Response. Di conseguenza, nel computer vengono aggiunte due chiavi: una per Kaspersky Endpoint Security e l'altra per Kaspersky Managed Detection and Response.

  La licenza per la funzionalità Managed Detection and Response standalone è la stessa della licenza di Kaspersky Endpoint Security.

Verificare che la funzionalità MDR sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

4. **Abilitazione del componente Managed Detection and Response**

Caricare il file di configurazione BLOB nel criterio di Kaspersky Endpoint Security (vedere le istruzioni di seguito). Il file BLOB contiene l'ID client e le informazioni sulla licenza per Kaspersky Managed Detection and Response. Il file BLOB si trova nell'archivio ZIP del file di configurazione MDR. È possibile ottenere l'archivio ZIP in Kaspersky Managed Detection and Response Console. Per informazioni dettagliate su un file BLOB, consultare la Guida di Kaspersky Managed Detection and Response.

A partire da Kaspersky Endpoint Security 12.6 for Windows, l'aggiunta di un file BLOB è facoltativa per Kaspersky Managed Detection and Response senza tenant se si dispone di una licenza corrente.

Come abilitare Managed Detection and Response in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Selezionare la casella di controllo **Managed Detection and Response (Industrial CyberSecurity)**.
5. Nella sezione **Impostazioni** fare clic su **Carica** e selezionare il file BLOB ricevuto in Kaspersky Managed Detection and Response Console. Il file ha l'estensione P7.

   Per impostazione predefinita, l'utente può gestire le impostazioni dell'applicazione (il "lucchetto" è aperto). Per applicare il criterio nei computer, chiudere i lucchetti .

6. Salvare le modifiche.

Come abilitare il componente Managed Detection and Response in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Configurazione agenti integrati** → **Managed Detection and Response**.
5. Attivare l'interruttore **Managed Detection and Response ABILITATO**.
6. Fare clic su **Carica** e selezionare il file BLOB ottenuto in Kaspersky Managed Detection and Response Console. Il file ha l'estensione P7.

   Per impostazione predefinita, l'utente può gestire le impostazioni dei criteri (il "lucchetto" è aperto). Per applicare il criterio nei computer, chiudere i lucchetti .
7. Salvare le modifiche.

Come abilitare il componente Managed Detection and Response dalla riga di comando

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.
3. Eseguire il seguente comando:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Per eseguire questo comando, Protezione tramite password deve essere abilitato. L'utente deve avere l'autorizzazione **Configura le impostazioni dell'applicazione**.

Successivamente Kaspersky Endpoint Security verificherà il file BLOB. La verifica del file BLOB include il controllo della firma digitale e del periodo licenza. Se il file BLOB viene verificato, Kaspersky Endpoint Security scaricherà il file e lo invierà al computer durante la successiva sincronizzazione con Kaspersky Security Center. Controllare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Managed Detection and Response** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

5. **Configurazione di altri componenti dell'applicazione per la ricezione della telemetria**

   Per consentire il funzionamento di Managed Detection and Response, è necessario abilitare i seguenti componenti.

   - Kaspersky Security Network (modalità estesa).
   - Rilevamento del Comportamento.
   - Prevenzione Exploit.
   - Protezione minacce web.
   - Protezione minacce di posta.
   - Protezione minacce file.
   - Protezione minacce di rete.
   - Firewall.

- Protezione AMSI.
- Scansione in background.

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Managed Detection and Response**.
5. Attivare l'interruttore **Managed Detection and Response ABILITATO**.
6. Salvare le modifiche.

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Selezionare la casella di controllo **Managed Detection and Response (Industrial CyberSecurity)**.
5. Salvare le modifiche.

Guida alla migrazione da KEA a KES per MDR

Kaspersky Endpoint Security for Windows include un agente integrato per la soluzione Kaspersky Managed Detection and Response. Non è più necessaria un'applicazione Kaspersky Endpoint Agent separata per utilizzare MDR. Tutte le funzioni di Kaspersky Endpoint Agent verranno eseguite da Kaspersky Endpoint Security.

Quando si distribuisce Kaspersky Endpoint Security nei computer in cui è installato Kaspersky Endpoint Agent, la soluzione Kaspersky Managed Detection and Response continuerà a funzionare con Kaspersky Endpoint Security. Inoltre, Kaspersky Endpoint Agent verrà rimosso dal computer. Lo stesso comportamento nel sistema si verificherà quando si aggiorna Kaspersky Endpoint Security alla versione 11.6.0 o successiva.

> Kaspersky Endpoint Security non è compatibile con Kaspersky Endpoint Agent. Non è possibile installare entrambe queste applicazioni nello stesso computer.

Le seguenti condizioni devono essere soddisfatte affinché Kaspersky Endpoint Security funzioni come parte di Kaspersky Managed Detection and Response:

- Kaspersky Security Center versione 13.2 o successiva (incluso Network Agent). Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità Managed Detection and Response.
- Viene stabilita una connessione in background tra Kaspersky Security Center Web Console e Administration Server. Affinché MDR funzioni con Administration Server tramite Kaspersky Security Center Web Console, è necessario stabilire una nuova connessione sicura: una *connessione in background*.

Passaggi per la migrazione della configurazione [KES+KEA] a [KES+agente integrato] per MDR

1. **Upgrade del plug-in di gestione di Kaspersky Endpoint Security**

   Il componente MDR può essere gestito utilizzando il plug-in di gestione di Kaspersky Endpoint Security versione 11.6 o successiva. A seconda del tipo di console di Kaspersky Security Center in uso, aggiornare il plug-in di gestione in Administration Console (MMC) o il plug-in Web in Web Console.

2. **Migrazione di criteri e attività**

   Trasferire le impostazioni di Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows. Sono disponibili le seguenti opzioni:

   - Una migrazione guidata da Kaspersky Endpoint Agent a Kaspersky Endpoint Security. Una migrazione guidata da Kaspersky Endpoint Agent a Kaspersky Endpoint Security funziona solo in Web Console

     Come eseguire la migrazione delle impostazioni di criteri e attività da Kaspersky Endpoint Agent a Kaspersky Endpoint Security in Web Console

Nella finestra principale di Web Console, fare clic su **Operazioni** → **Migrazione da Kaspersky Endpoint Agent**.

Viene eseguita la migrazione guidata di criteri e attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Migrazione dei criteri

La migrazione guidata crea un nuovo criterio che unisce le impostazioni dei criteri di Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Nell'elenco dei criteri, selezionare i criteri di Kaspersky Endpoint Agent di cui si desidera unire le impostazioni con il criterio di Kaspersky Endpoint Security. Fare clic sul criterio di Kaspersky Endpoint Agent per selezionare il criterio di Kaspersky Endpoint Security con cui unire le impostazioni. Verificare di aver selezionato i criteri corretti, quindi procedere con il passaggio successivo.

Passaggio 2. Migrazione delle attività

La migrazione guidata non supporta le attività di MDR. Ignorare questo passaggio.

Passaggio 3. Completamento della procedura guidata

Terminare la procedura guidata. Come risultato della procedura guidata, verrà creato un nuovo criterio di Kaspersky Endpoint Security. Il criterio unisce le impostazioni da Kaspersky Endpoint Security e Kaspersky Endpoint Agent Il criterio è denominato *<Nome del criterio di Kaspersky Endpoint Security> e <Nome del criterio di Kaspersky Endpoint Agent>*. Il nuovo criterio presenta lo stato *Inattivo*. Per continuare, modificare gli stati dei criteri di Kaspersky Endpoint Agent e Kaspersky Endpoint Security in *Inattivo* e attivare il nuovo criterio unito.

- Una Conversione guidata di criteri e attività in batch standard. La Conversione guidata di criteri e attività in batch è disponibile solo in Administration Console (MMC). Per ulteriori dettagli su Conversione guidata di criteri e attività in batch, consultare la Guida di Kaspersky Security Center.

3. **Licenza della funzionalità MDR**

   Per attivare Kaspersky Endpoint Security come parte della soluzione Kaspersky Managed Detection and Response, è necessaria una licenza separata per il componente aggiuntivo Kaspersky Managed Detection and Response. È possibile aggiungere la chiave tramite l'attività *Aggiungi chiave*. Di conseguenza, verranno aggiunte due chiavi all'applicazione: *Kaspersky Endpoint Security* e *Kaspersky Managed Detection and Response*.

4. **Installazione/upgrade dell'applicazione Kaspersky Endpoint Security**

   Per migrare la funzionalità MDR durante l'installazione o l'upgrade di un'applicazione, si consiglia di utilizzare l'attività di installazione remota. Quando si crea un'attività di installazione remota, è necessario selezionare il componente MDR nelle impostazioni del pacchetto di installazione.

   È inoltre possibile eseguire l'applicazione con i seguenti metodi:

   - Tramite il servizio di aggiornamento di Kaspersky.
   - In locale, utilizzando l'Installazione guidata.

Kaspersky Endpoint Security supporta la selezione automatica dei componenti quando si effettua l'upgrade dell'applicazione in un computer con l'applicazione Kaspersky Endpoint Agent installata. La selezione automatica dei componenti dipende dalle autorizzazioni dell'account utente che sta effettuando l'upgrade dell'applicazione.

Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando il file EXE o MSI nell'account di sistema (SYSTEM), Kaspersky Endpoint Security ottiene l'accesso alle licenze correnti delle soluzioni Kaspersky. Pertanto, se nel computer è installato Kaspersky Endpoint Agent e la soluzione MDR è attivata, il programma di installazione di Kaspersky Endpoint Security configura automaticamente il set di componenti e seleziona il componente MDR. In questo modo, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent. L'esecuzione del programma di installazione MSI nell'account di sistema (SYSTEM) viene in genere eseguita quando si effettua l'upgrade tramite Kaspersky Update Service o quando si distribuisce un pacchetto di installazione tramite Kaspersky Security Center.

Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando un file MSI in un account utente senza privilegi, Kaspersky Endpoint Security non sarà in grado di accedere alle licenze correnti delle soluzioni Kaspersky. In questo caso, Kaspersky Endpoint Security seleziona automaticamente i componenti in base a un set di componenti di Kaspersky Endpoint Agent. A questo punto, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent.

Kaspersky Endpoint Security supporta l'upgrade senza riavviare il computer. È possibile selezionare la modalità di upgrade dell'applicazione nelle proprietà dei criteri.

5. **Verifica del funzionamento dell'applicazione**

   Se dopo l'installazione o l'upgrade il computer presenta lo stato *Critico* nella console di Kaspersky Security Center:

   - Accertarsi che nel computer sia installato Network Agent versione 13.2 o successiva.
   - Controllare lo stato operativo dell'agente integrato visualizzando *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non installato*, installare il componente tramite l'attività *Modifica i componenti dell'applicazione*. Se un componente presenta lo stato *Non incluso nella licenza*, verificare di aver attivato la funzionalità dell'agente integrata.
   - Accertarsi di accettare l'Informativa di Kaspersky Security Network nel nuovo criterio di Kaspersky Endpoint Security for Windows.

Endpoint Detection and Response



Kaspersky Endpoint Security for Windows include un agente integrato per la soluzione Kaspersky Endpoint Detection and Response Optimum (di seguito denominato anche "EDR Optimum"). A partire dalla versione 11.8.0, Kaspersky Endpoint Security for Windows include un agente integrato per la soluzione Kaspersky Endpoint Detection and Response Expert (di seguito denominata anche "EDR Expert"). *Kaspersky Endpoint Detection and Response* è una serie di soluzioni che consente di proteggere l'infrastruttura IT aziendale dalle minacce informatiche avanzate. La funzionalità delle soluzioni combina il rilevamento automatico delle minacce con la capacità di reagire a tali minacce per contrastare gli attacchi avanzati, inclusi nuovi exploit, ransomware, attacchi fileless, nonché metodi che utilizzano strumenti di sistemi legittimi. EDR Expert offre più funzionalità di monitoraggio e risposta delle minacce rispetto a EDR Optimal. Per informazioni dettagliate sulle soluzioni, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.

Strumenti di threat intelligence

Kaspersky Endpoint Detection and Response utilizza i seguenti strumenti Threat Intelligence:

- Integrazione con Kaspersky Threat Intelligence Portal, che contiene e mostra informazioni sulla reputazione di file e indirizzi Web.
- Database delle minacce di Kaspersky.
- L'infrastruttura di servizi cloud di Kaspersky Security Network (di seguito denominata anche "KSN"), che fornisce accesso ai file in tempo reale, siti Web e informazioni sulla reputazione del software dalla knowledge base di Kaspersky. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce risposte più rapide da parte delle applicazioni Kaspersky alle minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi positivi.
- Tecnologia Sandbox cloud che consente di eseguire file rilevati in un ambiente isolato e controllarne la reputazione.

Principio di funzionamento della soluzione

Kaspersky Endpoint Detection and Response esamina e analizza lo sviluppo delle minacce e fornisce *personale di sicurezza* o l'*Amministratore* con informazioni sul potenziale attacco necessarie per una risposta tempestiva. Kaspersky Endpoint Detection and Response mostra i dettagli degli avvisi in una finestra separata. Un *avviso* è un evento nell'infrastruttura IT aziendale che l'applicazione ha identificato come insolito o sospetto e che può rappresentare una minaccia per la sicurezza dell'infrastruttura IT aziendale. *Dettagli avviso* è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Per informazioni dettagliate sulla gestione dei dettagli degli avvisi, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.

Supporto per le versioni precedenti di Kaspersky Endpoint Security

Se si utilizza Kaspersky Endpoint Security 11.2.0-11.6.0 per l'interoperabilità con Kaspersky Endpoint Detection and Response Optimum, l'applicazione include Kaspersky Endpoint Agent. È possibile installare Kaspersky Endpoint Agent insieme a Kaspersky Endpoint Security. In Kaspersky Endpoint Security 11.9.0, il pacchetto di distribuzione di Kaspersky Endpoint Agent non fa più parte del kit di distribuzione di Kaspersky Endpoint Security.

La soluzione Kaspersky Endpoint Detection and Response Expert non supporta l'interoperabilità con Kaspersky Endpoint Agent. La soluzione Kaspersky Endpoint Detection and Response Expert utilizza Kaspersky Endpoint Security con agente integrato (versione 11.8.0 e successive).

Integrazione dell'agente integrato con EDR Optimum/EDR Expert

Per configurare l'integrazione con Kaspersky Endpoint Detection and Response, è necessario abilitare il componente Endpoint Detection and Response Optimum o il componente Endpoint Detection and Response Expert (cloud) e configurare Kaspersky Endpoint Security.

I componenti Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), e Endpoint Detection and Response Expert (on-premises) i non sono compatibili tra loro.

Per il corretto funzionamento di Endpoint Detection and Response, è necessario soddisfare le seguenti condizioni:

- Kaspersky Security Center versione 13.2 o successiva. Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità Endpoint Detection and Response.
- Plug-in di gestione di Kaspersky Endpoint Detection and Response.

  A partire da Kaspersky Endpoint Security versione 12.6, la visualizzazione dei dettagli degli avvisi è stata spostata dal plug-in di gestione di Kaspersky Endpoint Security al plug-in di gestione EDR. Il plug-in di gestione EDR è un plug-in singolo per l'utilizzo degli agenti nei sistemi operativi Windows, Mac e Linux. Ora, quando si utilizza EDR Optimum, sarà necessario il plug-in di gestione di Kaspersky Endpoint Security per creare attività di risposta alle minacce e il plug-in di gestione EDR per visualizzare i dettagli degli avvisi.
- Il componente Endpoint Detection and Response Optimum come parte di Kaspersky Endpoint Security supporta l'interazione con la soluzione Kaspersky Endpoint Detection and Response Optimum 2.0. L'interazione con Kaspersky Endpoint Detection and Response Optimum versione 1.0 non è supportata.
- EDR Optimum può essere gestito in Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console.

  EDR Expert può essere gestito solo utilizzando Kaspersky Security Center Cloud Console. Non è possibile gestire questa funzionalità tramite Administration Console (MMC).
- L'applicazione è attivata e la funzionalità è coperta dalla licenza.
- Il componente Endpoint Detection and Response è attivato.
- I componenti dell'applicazione da cui dipende Endpoint Detection and Response sono abilitati e operativi. Endpoint Detection and Response dipende dai seguenti componenti:
  - Protezione minacce file.
  - Protezione minacce web.
  - Protezione minacce di posta.
  - Prevenzione Exploit.
  - Rilevamento del Comportamento.
  - Prevenzione Intrusioni Host.

- Motore di Remediation.
- Controllo adattivo delle anomalie.

L'integrazione con Kaspersky Endpoint Detection and Response prevede i seguenti passaggi:

1. **Installazione dei componenti di Endpoint Detection and Response**

   È possibile selezionare il componente Endpoint Detection and Response Optimum o il componente Endpoint Detection and Response Expert (cloud) durante l'installazione o l'upgrade, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

   > È necessario riavviare il computer per completare l'aggiornamento dell'applicazione con i nuovi componenti.

2. **Attivazione di Kaspersky Endpoint Detection and Response**

   È possibile acquisire una licenza per l'uso di Kaspersky Endpoint Detection and Response nei seguenti modi:

   - La funzionalità Endpoint Detection and Response è inclusa nella licenza di Kaspersky Endpoint Security for Windows.

     La funzionalità è disponibile immediatamente dopo l'attivazione di Kaspersky Endpoint Security for Windows.

   - Acquisto di una licenza separata per EDR Optimum o EDR Expert (componente aggiuntivo di Kaspersky Endpoint Detection and Response).

     La funzionalità diventa disponibile dopo aver aggiunto una chiave separata per il componente aggiuntivo Kaspersky Endpoint Detection and Response. Di conseguenza, nel computer vengono aggiunte due chiavi: una per Kaspersky Endpoint Security e l'altra per Kaspersky Endpoint Detection and Response.

     La licenza per la funzionalità Endpoint Detection and Response standalone è la stessa della licenza di Kaspersky Endpoint Security.

   Verificare che la funzionalità EDR Optimum o EDR Expert sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

   Per ulteriori informazioni sul Contratto di licenza con l'utente finale di EDR Optimum, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum.

3. **Abilitazione dei componenti di Endpoint Detection and Response**

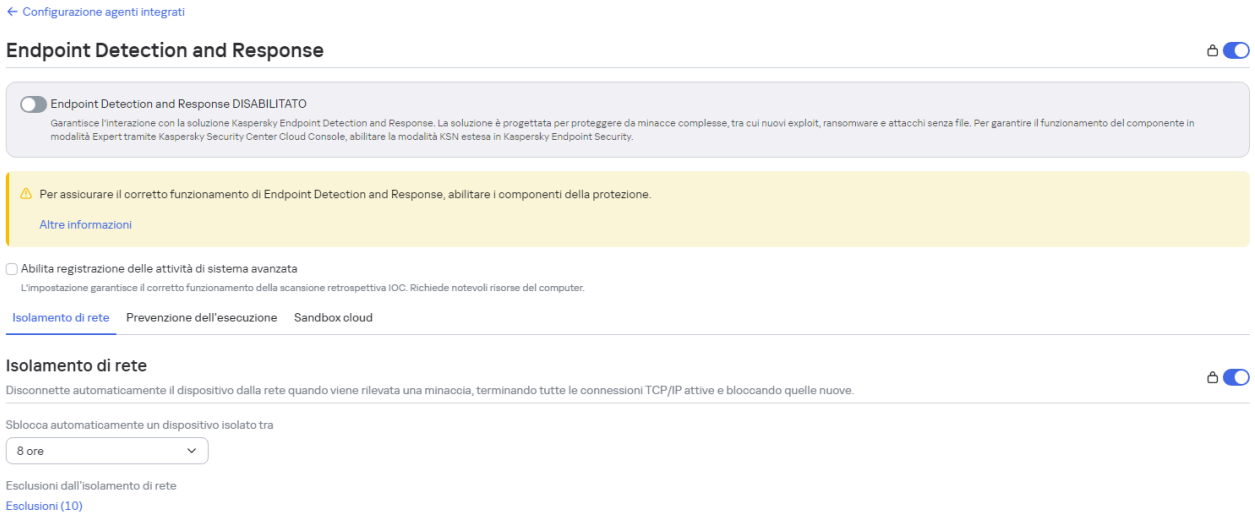
   È possibile abilitare o disabilitare il componente nelle impostazioni dei criteri di Kaspersky Endpoint Security for Windows.

   Come abilitare o disabilitare il componente Endpoint Detection and Response in Web Console

   1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
   2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

      Verrà visualizzata la finestra delle proprietà del criterio.
   3. Selezionare la scheda **Impostazioni applicazione**.
   4. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response**.
   5. Attivare l'interruttore **Endpoint Detection and Response ABILITATO**.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.



Impostazioni di integrazione di EDR

Il componente Kaspersky Endpoint Detection and Response è abilitato. Controllare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Endpoint Detection and Response Optimum** o **Endpoint Detection and Response Expert (cloud)** viene aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

4 Abilitazione del trasferimento dei dati ad Administration Server

Per abilitare tutte le funzionalità di Endpoint Detection and Response, è necessario abilitare il trasferimento dei dati per i seguenti tipi di dati:

- Dati dei file in quarantena.

  I dati sono necessari per ottenere informazioni sui file in quarantena in un computer tramite Web Console. Ad esempio, è possibile scaricare un file dalla quarantena per l'analisi in Web Console.

- Dati della catena di sviluppo delle minacce.

  I dati sono necessari per ottenere informazioni sulle minacce rilevate in un computer in Web Console. È possibile visualizzare i dettagli degli avvisi ed eseguire azioni di risposta in Web Console.

Come abilitare il trasferimento dei dati ad Administration Server in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Integrazione KSC**.
5. Nella sezione **Trasferimento dei dati ad Administration Server**, fare clic sul collegamento **Impostazioni avanzate**.

6. Nella finestra visualizzata, selezionare le seguenti caselle di controllo:

   - **Informazioni sui file in Quarantena**.
   - **Informazioni su una catena di sviluppo delle minacce**.

7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Scansione degli indicatori di compromissione (attività standard)

Un *indicatore di compromissione (IOC)* è una serie di dati su un oggetto o un'attività che indica un accesso non autorizzato al computer (compromissione dei dati). Ad esempio, molti tentativi non riusciti di accesso al sistema possono costituire un indicatore di compromissione. L'attività *Scansione IOC* consente di trovare indicatori di compromissione sul computer e di adottare misure di risposta alle minacce.

Kaspersky Endpoint Security ricerca gli indicatori di compromissione utilizzando i file IOC. I *file IOC* sono file che contengono le serie di indicatori che l'applicazione tenta di abbinare per eseguire un rilevamento. I file IOC devono essere conformi allo standard OpenIOC.

Modalità di esecuzione dell'attività Scansione IOC

Kaspersky Endpoint Detection and Response consente di creare attività di scansione IOC standard per rilevare dati compromessi. *Attività di scansione IOC standard* è un'attività locale o di gruppo creata e configurata manualmente in Web Console. Le attività vengono eseguite utilizzando i file IOC preparati dall'utente. Se si desidera aggiungere un indicatore di compromissione manualmente, leggere i requisiti dei file IOC.

Il file che è possibile scaricare facendo clic sul collegamento sottostante contiene una tabella con l'elenco completo dei termini IOC dello standard OpenIOC.

SCARICA IL FILE IOC_TERMS.XLSX

Kaspersky Endpoint Security supporta anche le attività di scansione IOC standalone quando l'applicazione viene utilizzata come parte della soluzione Kaspersky Sandbox.

Creazione del file IOC

A partire da Kaspersky Endpoint Security 12.10 for Windows, è possibile creare i file IOC direttamente nelle impostazioni dell'attività. Per creare un file IOC, è necessario preparare un file TXT con un elenco di indicatori di compromissione. È possibile aggiungere elenchi dei seguenti oggetti come indicatori di compromissione:

- Hash dei file (MD5/SHA256).

  L'applicazione prepara un file IOC con un ambito di scansione FileItem/Md5sum o FileItem/Sha256sum.

- Indirizzi IP (IPv4, IPv6).

  L'applicazione prepara un file IOC con un ambito di scansione PortItem/RemoteIP.

- Nomi DNS.

  L'applicazione prepara un file IOC con un ambito di scansione DnsEntryItem/RecordName.

Come creare un file IOC in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Attività**.

   Viene aperto l'elenco delle attività.

2. Selezionare l'attività **Scansione IOC**.

   Verrà visualizzata la finestra delle proprietà dell'attività. Se necessario, creare l'attività **Scansione IOC**.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare alla sezione **Scansione delle minacce**.

5. Fare clic su **Ridefinire i file IOC**.

6. Viene aperto il modulo per la creazione di un file IOC:

   a. In **Origine file IOC**, selezionare **Genera da file**.

   b. Immettere il nome del file IOC.

   c. Selezionare un file TXT con un elenco di indicatori di compromissione.

   d. Selezionare il tipo di file IOC: **Nomi DNS**, **Hash dei file**, **Indirizzi IP**.

   e. Fare clic su **Carica**.

   Kaspersky Endpoint Security aggiunge i file IOC alla raccolta di IOC. Se necessario, è possibile escludere temporaneamente i file IOC dall'ambito dell'attività.

7. Salvare le modifiche.

Creazione di un'attività Scansione IOC

È possibile creare attività *Scansione IOC* manualmente:

- Nei dettagli degli avvisi (solo per EDR Optimum).

  Dettagli avviso è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Per informazioni dettagliate sulla gestione dei dettagli degli avvisi, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.

- Utilizzo della Creazione guidata attività.

L'attività di gruppo *Scansione IOC* non può essere eseguita se nei computer da sottoporre a scansione è configurata l'integrazione con Kaspersky Endpoint Detection and Response Expert (on-premises) o Kaspersky Endpoint Detection and Response Expert (cloud). In questo caso, è consigliabile utilizzare l'azione di risposta *Scansione IOC* per cercare gli indicatori di compromissione. Per maggiori dettagli, consultare la guida di Kaspersky Endpoint Detection and Response Expert (on-premises).

È possibile configurare l'attività per EDR Optimum in Web Console e Cloud Console. Le impostazioni dell'attività per EDR Expert sono disponibili solo in Cloud Console.

Per creare un'attività Scansione IOC:

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Scansione IOC**.

   c. Nel campo **Nome attività**, immettere una breve descrizione.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Procedere con il passaggio successivo.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Procedere con il passaggio successivo.

   Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

L'account di sistema (SYSTEM) non dispone dell'autorizzazione necessaria per eseguire l'attività *Scansione IOC* nelle unità di rete. Se si desidera eseguire l'attività per un'unità di rete, selezionare l'account di un utente che ha accesso a tale unità.

Per le attività Scansione IOC standalone nelle unità di rete, nelle proprietà dell'attività è necessario selezionare manualmente l'accesso utente che ha accesso a tale unità.

6. Terminare la procedura guidata.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Fare clic sulla nuova attività.

   Verrà visualizzata la finestra delle proprietà dell'attività.

8. Selezionare la scheda **Impostazioni applicazione**.

9. Passare alla sezione **Scansione delle minacce**.

10. Caricare i file IOC per cercare gli indicatori di compromissione.

    Dopo aver caricato i file IOC, l'applicazione mostra informazioni di riepilogo sul file, incluso l'elenco degli indicatori che non hanno superato il controllo. Dopo il caricamento dei file IOC, è possibile modificare manualmente i file nell'editor integrato direttamente nelle proprietà dell'attività. Kaspersky Endpoint Security supporta la modifica di file IOC conformi allo standard OpenIOC 1.1. Non è possibile modificare il contenuto dei file IOC compatibili con OpenIOC versione 1.0.

    Kaspersky Endpoint Security aggiunge i file IOC alla raccolta di IOC. Se necessario, è possibile escludere temporaneamente i file IOC dall'ambito dell'attività.

    Si sconsiglia di aggiungere o rimuovere file IOC dopo l'esecuzione dell'attività, poiché può causare la visualizzazione errata dei risultati della scansione IOC per le esecuzioni dell'attività precedenti. Per cercare indicatori di compromissione da parte di nuovi file IOC, si consiglia di aggiungere nuove attività.

11. Se necessario, selezionare la casella di controllo **Scansione IOC retrospettiva**. *Scansione IOC retrospettiva* è una modalità dell'attività *Scansione IOC* in cui Kaspersky Endpoint Security esegue la scansione degli indicatori di compromissione utilizzando i dati per un determinato periodo di tempo. Questa modalità è destinata alla ricerca di indicatori di compromissione tramite la telemetria del computer protetto, ad esempio attività di rete, processi, file e altri dati di telemetria. Kaspersky Endpoint Security analizza i dati nei registri del sistema operativo e del browser nel computer. La scansione IOC retrospettiva analizza i registri dei seguenti browser: Google Chrome, Mozilla Firefox, Microsoft Edge (versione 79 o successiva).

12. Configurare le azioni se viene rilevato un indicatore di compromissione:

    - **Isola il dispositivo dalla rete**. Se questa opzione è selezionata, Kaspersky Endpoint Security isola il computer dalla rete per impedire la diffusione della minaccia. È possibile configurare la durata dell'isolamento nelle impostazioni del componente Endpoint Detection and Response.

      Se questa casella di controllo è deselezionata, è possibile isolare il computer dalla rete dopo aver eseguito manualmente l'attività. Se l'attività *Scansione IOC* rileva un file IOC, è possibile isolare il computer dalla rete direttamente dal file IOC (proprietà dell'attività *Scansione IOC* → **Impostazioni applicazione** → **Risultati scansione IOC**). Kaspersky Endpoint Security consente inoltre di gestire immediatamente impostazioni aggiuntive: periodo di disattivazione dell'isolamento della rete ed esclusioni dell'isolamento della rete.

- **Sposta la copia in Quarantena, elimina oggetto**. Se questa opzione è selezionata, Kaspersky Endpoint Security elimina l'oggetto dannoso trovato nel computer. Prima di eliminare l'oggetto, Kaspersky Endpoint Security crea una copia di backup nel caso in cui sia necessario ripristinare l'oggetto in un secondo momento. Kaspersky Endpoint Security sposta la copia di backup in Quarantena.

  Se questa casella di controllo è deselezionata, è possibile mettere manualmente in quarantena il file dopo aver eseguito manualmente l'attività. Se l'attività *Scansione IOC* rileva un file che può compromettere i dati, è possibile mettere in quarantena questo file direttamente dai risultati della scansione IOC (**Impostazioni applicazione → Risultati scansione IOC**). In seguito a questa operazione, Kaspersky Endpoint Security avvia la creazione guidata dell'attività con i dati preimpostati del file rilevato. È solo necessario gestire le impostazioni aggiuntive dell'attività, ad esempio impostare la pianificazione dell'attività.

  Se necessario, selezionare la casella di controllo **Applica a oggetti critici di sistema**. Gli System Critical Object (SCO) includono i file necessari per il funzionamento del sistema operativo.

  Non è consigliabile applicare azioni ai file SCO. Ciò può rendere instabile il sistema operativo o impedirne l'avvio.

- **Esegui scansione delle aree critiche**. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue l'attività *Scansione delle aree critiche*. Per impostazione predefinita, Kaspersky Endpoint Security esamina la memoria del kernel, i processi in esecuzione e i settori di avvio del disco.

13. Passare alla sezione **Avanzato**.

14. Selezionare i tipi di dati (documenti IOC) che devono essere analizzati come parte dell'attività.

    Kaspersky Endpoint Security seleziona automaticamente i tipi di dati (documenti IOC) per l'attività *Scansione IOC* in conformità con i contenuti dei file IOC caricati. Si sconsiglia di deselezionare i tipo di dati.

    È inoltre possibile configurare gli ambiti della scansione per i seguenti tipi di dati:

    - **File - FileItem**. Consente di impostare un ambito della scansione IOC nel computer in cui vengono utilizzati gli ambiti preimpostati.

      Per impostazione predefinita, Kaspersky Endpoint Security esamina gli IOC solo nelle aree importanti del computer, ad esempio la cartella Download, il desktop, la cartella con i file temporanei del sistema operativo ecc. È inoltre possibile aggiungere manualmente l'ambito della scansione.

    - **Registro eventi Windows - EventLogItem**. Immettere il periodo di tempo in cui gli eventi sono stati registrati. È inoltre possibile selezionare i registri eventi di Windows da utilizzare per la scansione IOC. Per impostazione predefinita, vengono selezionati i seguenti registri eventi: registro eventi delle applicazioni, registro eventi del sistema e registro eventi della sicurezza.

      Per il termine IOC EventLogItem\source, utilizzare il valore **Nome provider** dello schema XML dell'evento.

    - **Registro di sistema Windows - RegistryItem**. Configurare l'ambito di scansione IOC nel Registro di sistema.

      Per impostazione predefinita, Kaspersky Endpoint Security esamina una serie di chiavi del Registro di sistema.

15. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

16. Configurare la pianificazione dell'attività.

> Wake-on-LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

17. Salvare le modifiche.

18. Selezionare la casella di controllo accanto all'attività.

19. Fare clic su **Avvia**.

A questo punto, Kaspersky Endpoint Security esegue la ricerca degli indicatori di compromissione sul computer. È possibile visualizzare i risultati dell'attività nelle proprietà dell'attività nelle sezione **Risultati**. È possibile visualizzare le informazioni sugli indicatori di compromissione rilevati nelle proprietà dell'attività: **Impostazioni applicazione** → **Risultati scansione IOC**. Nei risultati di scansione IOC è possibile mettere in quarantena il file rilevato o isolare il computer dalla rete anche manualmente.

Kaspersky Endpoint Security cerca i duplicati tra i record creati per lo stesso file IOC e conserva solo i record univoci nei risultati delle attività. I duplicati sono record dello stesso tipo con gli stessi valori di tutti i campi confrontati. L'applicazione potrebbe inoltre non creare un record se non dispone di un valore in uno o più campi (vedere la tabella seguente).

Tipo	Campi confrontati	Condizione per non creare un record
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• Valore mancante dei campi FullPath, Md5sum, Sha256sum. • Valori mancanti del campo FullPath e valori identici dei campi Md5sum, Sha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Valore mancante di almeno uno dei seguenti campi: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	Valori mancanti dei campi startTime o PID.

> La finestra **Dettagli avviso** potrebbe visualizzare i record di RegistryItem con valori dei campi identici. Tali record non sono duplicati poiché hanno valori diversi del campo Testo, che non è visualizzato nell'interfaccia.

> I risultati della scansione IOC vengono conservati per 30 giorni. Al termine di questo periodo, Kaspersky Endpoint Security elimina automaticamente le voci meno recenti.

Telemetria estesa per la scansione IOC

È consigliabile abilitare la telemetria estesa nel computer per la scansione IOC retrospettiva. La telemetria estesa migliora la precisione del rilevamento IOC, ma utilizza più risorse del computer.

La telemetria estesa include il supporto dei seguenti termini aggiuntivi:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Se la telemetria estesa è disabilitata, Kaspersky Endpoint Security può ruotare le informazioni sugli indicatori di compromissione rilevati.

Per abilitare la telemetria estesa:

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response**.
5. Selezionare la casella di controllo **Abilita registrazione delle attività di sistema avanzata**.
6. Salvare le modifiche.

Sposta il file in Quarantena

Quando reagisce alle minacce, Kaspersky Endpoint Detection and Response può creare attività *Sposta file in Quarantena*. Ciò è necessario per ridurre al minimo le conseguenze della minaccia. *Quarantena* è una memoria locale speciale sul computer. L'utente può mettere in quarantena i file che considera pericolosi per il computer. I file in quarantena vengono archiviati in uno stato criptato e non minacciano la sicurezza del dispositivo. Kaspersky Endpoint Security utilizza la Quarantena solo quando è integrato con le soluzioni Kaspersky Detection and Response. In altri casi, Kaspersky Endpoint Security inserisce il file pertinente in Backup. Per ulteriori dettagli sulla gestione di Quarantena come parte delle soluzioni, consultare la Guida di Kaspersky Sandbox Help, la Guida di Kaspersky Endpoint Detection and Response Optimum, la Guida di Kaspersky Endpoint Detection and Response Expert, la Guida di Kaspersky Anti Targeted Attack Platform e la Guida di Kaspersky Endpoint Detection and Response Expert (on-premises).

È possibile creare attività *Sposta file in Quarantena* nei seguenti modi:

- Nei dettagli degli avvisi (solo per EDR Optimum).

  Dettagli avviso è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Per informazioni dettagliate sulla gestione dei dettagli degli avvisi, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.

- Utilizzo della Creazione guidata attività.

  È necessario immettere il percorso del file o l'hash (SHA256 o MD5) oppure sia il percorso del file che l'hash del file.

- Nelle impostazioni dell'attività *Scansione IOC*.

  Se l'attività *Scansione IOC* rileva un file che può compromettere i dati, è possibile mettere in quarantena questo file direttamente dai risultati della scansione IOC (**Impostazioni applicazione** → **Risultati scansione IOC**). In seguito a questa operazione, Kaspersky Endpoint Security avvia la creazione guidata dell'attività con i dati preimpostati del file rilevato. È solo necessario gestire le impostazioni aggiuntive dell'attività, ad esempio impostare la pianificazione dell'attività.

L'attività *Sposta file in Quarantena* ha le seguenti limitazioni:

1. La dimensione del file non deve superare i 100 MB.
2. Non è possibile eliminare i file necessari per il funzionamento di Kaspersky Endpoint Security for Windows:
   - File inclusi nell'ambito della tecnologia di autodifesa di Kaspersky Endpoint Security for Windows
   - File con firma digitale di Kaspersky
3. È possibile configurare l'attività per EDR Optimum in Web Console e Cloud Console. Le impostazioni dell'attività per EDR Expert sono disponibili solo in Cloud Console.
4. Non è possibile eseguire la scansione di un oggetto inserito in Quarantena a causa dell'attività *Sposta file in Quarantena*.

Per creare un'attività Sposta file in Quarantena:

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Sposta file in Quarantena**.

   c. Nel campo **Nome attività**, immettere una breve descrizione.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Fare clic su **Avanti**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

6. Terminare la procedura guidata facendo clic sul pulsante **Fine**.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Fare clic sulla nuova attività.

   Verrà visualizzata la finestra delle proprietà dell'attività.

8. Selezionare la scheda **Impostazioni applicazione**.

9. Se necessario, selezionare la casella di controllo **Applica a oggetti critici di sistema**.

   Gli System Critical Object (SCO) includono i file necessari per il funzionamento del sistema operativo.

   Non è consigliabile applicare azioni ai file SCO. Ciò può rendere instabile il sistema operativo o impedirne l'avvio.

10. Nell'elenco dei file, fare clic su **Aggiungi**.

    Viene avviata la procedura guidata per l'aggiunta di file.

11. Per aggiungere il file, è necessario immettere il percorso completo del file oppure sia l'hash che il percorso del file.

    Se il file si trova su un'unità di rete, immettere il percorso del file che inizia con `\\`, non la lettera dell'unità. Ad esempio, `\\server\shared_folder\file.exe`. Se il percorso del file contiene una lettera di unità di rete, è possibile che venga restituito un errore *File non trovato*.

12. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

13. Configurare la pianificazione dell'attività.

    Wake-on-LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

14. Salvare le modifiche.

15. Selezionare la casella di controllo accanto all'attività.

16. Fare clic su **Avvia**.

    A questo punto, Kaspersky Endpoint Security sposta il file in Quarantena.

Se il file è bloccato da un altro processo, l'attività viene visualizzata come Fine, ma il file stesso viene messo in quarantena solo dopo il riavvio del computer. Dopo aver riavviato il computer, verificare che il file sia stato eliminato.

Se il file è bloccato da un processo diverso, l'attività viene visualizzata come *Completata*, ma il file stesso viene messo in quarantena solo dopo il riavvio del computer. Dopo aver riavviato il computer, verificare che il file sia stato eliminato.

L'attività *Sposta file in Quarantena* può terminare con l'errore *Accesso negato* se si sta tentando di mettere in quarantena un file eseguibile attualmente in esecuzione. Creare un'attività Termina processo per il file e riprovare.

L'attività *Sposta file in Quarantena* può terminare con l'errore *Spazio insufficiente nell'archivio Quarantena* se si sta tentando di mettere in quarantena un file di dimensioni eccessive. Svuotare la Quarantena o aumentare lo spazio della Quarantena, quindi riprovare.

È possibile ripristinare un file dalla Quarantena o svuotare la Quarantena tramite Web Console. È possibile ripristinare gli oggetti in locale sul computer utilizzando la riga di comando.

Ottieni file

È possibile ottenere file dai computer degli utenti. Ad esempio, è possibile configurare l'acquisizione di un file di registro eventi creato da un'applicazione di terzi. Come risultato dell'esecuzione dell'attività, una copia del file viene salvata in Quarantena. *Quarantena* è una memoria locale speciale sul computer. È possibile scaricare questo file dalla Quarantena sul computer tramite Web Console (**Operazioni** → **Archivi** → **Quarantena**). Sul computer dell'utente, il file rimane nella cartella originale.

La dimensione del file non deve superare i 2 GB.

È possibile configurare l'attività per EDR Optimum in Web Console e Cloud Console. Le impostazioni dell'attività per EDR Expert sono disponibili solo in Cloud Console.

Per creare un'attività Ottieni file:

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Ottieni file**.

   c. Nel campo **Nome attività**, immettere una breve descrizione.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Fare clic su **Avanti**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

6. Terminare la procedura guidata facendo clic sul pulsante **Fine**.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Fare clic sulla nuova attività.

   Verrà visualizzata la finestra delle proprietà dell'attività.

8. Selezionare la scheda **Impostazioni applicazione**.

9. Nell'elenco dei file, fare clic su **Aggiungi**.

   Viene avviata la procedura guidata per l'aggiunta di file.

10. Per aggiungere il file, è necessario immettere il percorso completo del file oppure sia l'hash che il percorso del file.

    Se il file si trova su un'unità di rete, immettere il percorso del file che inizia con `\\`, non la lettera dell'unità. Ad esempio, `\\server\shared_folder\file.exe`. Se il percorso del file contiene una lettera di unità di rete, è possibile che venga restituito un errore *File non trovato*.

11. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

12. Configurare la pianificazione dell'attività.

    Wake-on-LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

13. Salvare le modifiche.

14. Selezionare la casella di controllo accanto all'attività.

15. Fare clic su **Avvia**.

    Di conseguenza, Kaspersky Endpoint Security crea una copia del file e sposta tale copia nella Quarantena. È possibile scaricare il file dalla Quarantena in Web Console.

Elimina file

È possibile eliminare i file da remoto tramite l'attività *Elimina il file*. Ad esempio, è possibile eliminare da remoto un file quando si risponde alle minacce.

Non è possibile eliminare i file necessari per il funzionamento di Kaspersky Endpoint Security for Windows:

- File inclusi nell'ambito della tecnologia di autodifesa di Kaspersky Endpoint Security for Windows
- File con firma digitale di Kaspersky

È possibile configurare l'attività per EDR Optimum in Web Console e Cloud Console. Le impostazioni dell'attività per EDR Expert sono disponibili solo in Cloud Console.

Per creare un'attività Elimina il file:

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Elimina il file**.

   c. Nel campo **Nome attività**, immettere una breve descrizione.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Fare clic su **Avanti**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

6. Terminare la procedura guidata facendo clic sul pulsante **Fine**.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Fare clic sulla nuova attività.

   Verrà visualizzata la finestra delle proprietà dell'attività.

8. Selezionare la scheda **Impostazioni applicazione**.

9. Per aggiungere il file, è necessario immettere il percorso completo del file oppure sia l'hash che il percorso del file.

   Se il file si trova su un'unità di rete, immettere il percorso del file che inizia con `\\`, non la lettera dell'unità. Ad esempio, `\\server\shared_folder\file.exe`. Se il percorso del file contiene una lettera di unità di rete, è possibile che venga restituito un errore *File non trovato*.

10. Se necessario, selezionare la casella di controllo **Applica a oggetti critici di sistema**.

    Gli System Critical Object (SCO) includono i file necessari per il funzionamento del sistema operativo.

    Non è consigliabile applicare azioni ai file SCO. Ciò può rendere instabile il sistema operativo o impedirne l'avvio.

11. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

12. Configurare la pianificazione dell'attività.

    Wake-on-LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

13. Salvare le modifiche.

14. Selezionare la casella di controllo accanto all'attività.

15. Fare clic su **Avvia**.

    A questo punto, Kaspersky Endpoint Security elimina il file dal computer. Se il file è bloccato da un processo diverso, l'attività viene visualizzata come *Fine*, ma il file stesso viene eliminato solo dopo il riavvio del computer. Dopo aver riavviato il computer, verificare che il file sia stato eliminato.

L'attività *Elimina il file* può terminare con l'errore *Accesso negato o file non trovato* se si sta tentando di eliminare un file eseguibile attualmente in esecuzione. Creare un'attività Termina processo per il file e riprovare.

Avvio del processo

È possibile eseguire i file da remoto tramite l'attività *Avvio del processo*. Ad esempio, è possibile eseguire da remoto un'utilità che crea il file di configurazione del computer. Successivamente, è possibile utilizzare l'attività *Ottieni file* per ricevere il file creato in Kaspersky Security Center Web Console.

È possibile configurare l'attività per EDR Optimum in Web Console e Cloud Console. Le impostazioni dell'attività per EDR Expert sono disponibili solo in Cloud Console.

Per creare un'attività Avvio del processo:

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Avvio del processo**.

c. Nel campo **Nome attività**, immettere una breve descrizione.

d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Fare clic su **Avanti**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

6. Terminare la procedura guidata facendo clic sul pulsante **Fine**.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Fare clic sulla nuova attività.

8. Verrà visualizzata la finestra delle proprietà dell'attività.

9. Selezionare la scheda **Impostazioni applicazione**.

10. Immettere il comando di avvio del processo.

    Si supponga di voler eseguire un'utilità (`utility.exe`) che salvi le informazioni sulla configurazione del computer in un file denominato `conf.txt` nella cartella corrente (per impostazione predefinita). L'utilità si trova nella cartella `C:\Users\admin\Diagnostic\`. È necessario salvare il file di configurazione nella cartella `C:\Users\admin\Documents\Configuration`. Immettere i seguenti valori:

    - **Comando eseguibile** - `C:\Users\admin\Diagnostic\utility.exe`
    - **Argomenti della riga di comando (facoltativo)** - `/R conf.txt`
    - **Percorso della cartella di lavoro (non obbligatorio)** - `C:\Users\admin\Documents\Configuration`

11. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

12. Configurare la pianificazione dell'attività.

    Wake-on-LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

13. Salvare le modifiche.

14. Selezionare la casella di controllo accanto all'attività.

15. Fare clic su **Avvia**.

Di conseguenza, Kaspersky Endpoint Security esegue il comando in modalità invisibile e avvia il processo. È possibile visualizzare i risultati dell'attività nelle proprietà dell'attività nelle sezione **Risultati dell'esecuzione**.

Termina processo

È possibile terminare i processi da remoto tramite l'attività *Termina processo*. Ad esempio, è possibile terminare da remoto un'utilità di test della velocità di Internet avviata tramite l'attività *Esegui processo*.

Se si desidera impedire l'esecuzione di un file, è possibile configurare il componente Prevenzione dell'esecuzione. È possibile vietare l'esecuzione di file eseguibili, script, file in formato Office.

L'attività *Termina processo* ha le seguenti limitazioni:

Non è possibile terminare i processi dei file necessari per il funzionamento di Kaspersky Endpoint Security for Windows:

- File inclusi nell'ambito della tecnologia di autodifesa di Kaspersky Endpoint Security for Windows
- File con firma digitale di Kaspersky

È possibile configurare l'attività per EDR Optimum in Web Console e Cloud Console. Le impostazioni dell'attività per EDR Expert sono disponibili solo in Cloud Console.

Per creare un'attività Termina processo:

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata attività.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Endpoint Security for Windows 14.2**.

   b. Nell'elenco a discesa **Tipo di attività**, selezionare **Termina processo**.

   c. Nel campo **Nome attività**, immettere una breve descrizione.

   d. Nel blocco **Dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Fare clic su **Avanti**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (SYSTEM).

6. Terminare la procedura guidata facendo clic sul pulsante **Fine**.

   Verrà visualizzata una nuova attività nell'elenco delle attività.

7. Fare clic sulla nuova attività.

   Verrà visualizzata la finestra delle proprietà dell'attività.

8. Selezionare la scheda **Impostazioni applicazione**.

9. Se necessario, selezionare la casella di controllo **Applica a oggetti critici di sistema**.

   Gli System Critical Object (SCO) includono i file necessari per il funzionamento del sistema operativo.

   > Non è consigliabile applicare azioni ai file SCO. Ciò può rendere instabile il sistema operativo o impedirne l'avvio.

10. Per completare il processo, è necessario selezionare il file che si desidera terminare. È possibile selezionare un file in uno dei seguenti modi:

    - Immettere il nome completo del file.
    - Immettere l'hash e il percorso del file.
    - Immettere il PID del processo (solo per le attività locali).
    - Se il file si trova su un'unità di rete, immettere il percorso del file che inizia con `\\`, non la lettera dell'unità. Ad esempio, `\\server\shared_folder\file.exe`. Se il percorso del file contiene una lettera di unità di rete, è possibile che venga restituito un errore *File non trovato*.

    > Se il file si trova su un'unità di rete, immettere il percorso del file che inizia con `\\`, non la lettera dell'unità. Ad esempio, `\\server\shared_folder\file.exe`. Se il percorso del file contiene una lettera di unità di rete, è possibile che venga restituito un errore *Impossibile trovare il file*.

11. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

12. Configurare la pianificazione dell'attività.

    > Wake-on-LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

13. Fare clic su **Salva**.

14. Selezionare la casella di controllo accanto all'attività.

15. Fare clic su **Avvia**.

A questo punto, Kaspersky Endpoint Security termina il processo sul computer. Ad esempio, se un'applicazione GAME è in esecuzione e si termina il processo game.exe, l'applicazione viene chiusa senza salvare i dati. È possibile visualizzare i risultati dell'attività nelle proprietà dell'attività nelle sezione **Risultati**.

Prevenzione dell'esecuzione

Prevenzione dell'esecuzione consente di gestire l'esecuzione dei file eseguibili e degli script, nonché di aprire i file in formato Office. In questo modo, è possibile, ad esempio, impedire l'esecuzione di applicazioni non considerate sicure. Di conseguenza, la diffusione della minaccia può essere arrestata. Prevenzione dell'esecuzione supporta una serie di estensioni di file Office e una serie di interpreti di script.

Regola di prevenzione dell'esecuzione

Prevenzione dell'esecuzione gestisce l'accesso degli utenti ai file con regole di prevenzione dell'esecuzione. *Regola di prevenzione dell'esecuzione* è un insieme di criteri che l'applicazione prende in considerazione quando reagisce all'esecuzione di un oggetto, ad esempio quando blocca l'esecuzione di un oggetto. L'applicazione identifica i file in base ai loro percorsi o checksum calcolati utilizzando gli algoritmi di hash MD5 e SHA256.

È possibile creare regole di prevenzione dell'esecuzione:

- Nei dettagli degli avvisi (solo per EDR Optimum).

  Dettagli avviso è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Per informazioni dettagliate sulla gestione dei dettagli degli avvisi, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.

- Tramite un criterio di gruppo o impostazioni delle applicazioni locali.

  È necessario immettere il percorso o l'hash del file (SHA256 o MD5) oppure il percorso della cartella e l'hash del file.

È inoltre possibile gestire Prevenzione dell'esecuzione in locale tramite la riga di comando.

La prevenzione dell'esecuzione presenta le seguenti limitazioni:

1. Le regole di prevenzione non vengono applicate ai file su CD o nelle immagini ISO. L'applicazione non blocca l'esecuzione o l'apertura di tali file.

2. Non è possibile applicare una regola di prevenzione ai file necessari per il funzionamento di Kaspersky Endpoint Security for Windows:

   - File inclusi nell'ambito della tecnologia di autodifesa di Kaspersky Endpoint Security for Windows

   - File con firma digitale di Kaspersky

3. Si sconsiglia di creare più di 5000 regole di prevenzione delle esecuzioni, per evitare di causare instabilità di sistema.

Modalità delle regole di prevenzione dell'esecuzione

Il componente Prevenzione dell'esecuzione può funzionare in due modalità:

- **Statistics only**

  In questa modalità, Kaspersky Endpoint Security pubblica un evento sui tentativi di esecuzione di oggetti eseguibili o apertura di documenti che corrispondono ai criteri della regola di prevenzione nel registro eventi di Windows e in Kaspersky Security Center, ma non blocca il tentativo di esecuzione o apertura dell'oggetto o del documento. Questa modalità è selezionata per impostazione predefinita.

- **Active**

  In questa modalità, l'applicazione blocca l'esecuzione di oggetti o l'apertura di documenti che soddisfano i criteri della regola di prevenzione. L'applicazione pubblica anche un evento sui tentativi di esecuzione di oggetti o apertura di documenti nel registro eventi di Windows e nel registro eventi di Kaspersky Security Center.

Gestione della prevenzione dell'esecuzione

È possibile configurare le impostazioni del componente solo in Web Console.

Per impedire l'esecuzione:

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response**.
5. Selezionare la scheda **Prevenzione dell'esecuzione**.
6. Attivare l'interruttore **Prevenzione dell'esecuzione ABILITATA**.
7. Nel blocco **Azione in caso di esecuzione o apertura di un oggetto vietato**, selezionare la modalità operativa del componente:

   - **Blocca e aggiungi al registro eventi**. In questa modalità, l'applicazione blocca l'esecuzione di oggetti o l'apertura di documenti che soddisfano i criteri della regola di prevenzione. L'applicazione pubblica anche un evento sui tentativi di esecuzione di oggetti o apertura di documenti nel registro eventi di Windows e nel registro eventi di Kaspersky Security Center.

     Se necessario, selezionare la casella di controllo **Applica a oggetti critici di sistema**. Gli System Critical Object (SCO) includono i file necessari per il funzionamento del sistema operativo.

Non è consigliabile applicare azioni ai file SCO. Ciò può rendere instabile il sistema operativo o impedirne l'avvio.

- **Aggiungi al registro eventi**. In questa modalità, Kaspersky Endpoint Security pubblica un evento sui tentativi di esecuzione di oggetti eseguibili o apertura di documenti che corrispondono ai criteri della regola di prevenzione nel registro eventi di Windows e in Kaspersky Security Center, ma non blocca il tentativo di esecuzione o apertura dell'oggetto o del documento. Questa modalità è selezionata per impostazione predefinita.

8. Creare un elenco di regole di prevenzione dell'esecuzione:

   a. Fare clic su **Aggiungi**.

   b. Si apre una finestra; in questa finestra, immettere il nome della regola di prevenzione dell'esecuzione (ad esempio, *Applicazione A*).

   c. Nell'elenco a discesa **Tipo**, selezionare l'oggetto che si desidera bloccare: **File eseguibile**, **Script**, **Documento di Microsoft Office**.

   Se si seleziona un tipo di oggetto errato, Kaspersky Endpoint Security non blocca il file o lo script.

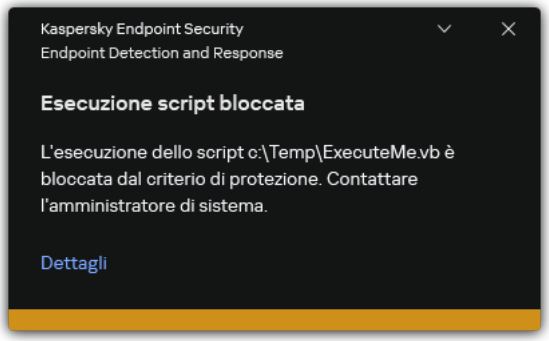
   d. Per aggiungere il file, è necessario immettere l'hash del file (SHA256 o MD5), il percorso completo del file oppure l'hash e il percorso della cartella.

   Se il file si trova su un'unità di rete, immettere il percorso del file che inizia con `\\`, non la lettera dell'unità. Ad esempio, `\\server\shared_folder\file.exe`. Se il percorso file contiene una lettera di unità di rete, Kaspersky Endpoint Security non blocca il file o lo script.

   Prevenzione dell'esecuzione supporta una serie di estensioni di file Office e una serie di interpreti di script.

9. Salvare le modifiche.

Di conseguenza, Kaspersky Endpoint Security blocca l'esecuzione degli oggetti: esecuzione di file eseguibili e script, apertura di file in formato Office. È tuttavia possibile, ad esempio, aprire un file di script in un editor di testo anche se l'esecuzione dello script è stata impedita. Quando si blocca l'esecuzione di un oggetto, Kaspersky Endpoint Security mostra una notifica standard (vedere la figura riportata di seguito) se le notifiche sono abilitate nelle impostazioni dell'applicazione.



Notifica di Prevenzione dell'esecuzione

Isolamento di rete del computer

L'isolamento di rete del computer consente di isolare automaticamente un computer dalla rete in risposta al rilevamento di un indicatore di compromissione (IOC): questa è la *modalità automatica*. È possibile attivare Isolamento di rete manualmente mentre si effettuano indagini sulla minaccia rilevata: questa è la *modalità manuale*.

Quando l'opzione Isolamento di rete è attivata, l'applicazione interrompe tutte le connessioni attive e blocca tutte le nuove connessioni alle reti TCP/IP sul computer, ad eccezione delle seguenti connessioni:

- Connessioni elencate in Esclusioni dall'isolamento di rete.
- Connessioni avviate dai servizi di Kaspersky Endpoint Security.
- Connessioni avviate da Kaspersky Security Center Network Agent.
- Connessioni alla SVM e al server di integrazione, se l'applicazione è utilizzata in modalità Light Agent.
- Connessioni a KSN durante l'integrazione dell'applicazione con Kaspersky Managed Detection and Response.

È possibile configurare le impostazioni del componente solo in Web Console.

Modalità Isolamento di rete automatica

È possibile configurare l'attivazione automatica di Isolamento di rete in risposta a un rilevamento di IOC. È possibile configurare la modalità Isolamento di rete automatica con un criterio di gruppo.

Come configurare l'attivazione automatica di Isolamento di rete in risposta a un rilevamento di IOC

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Scansione IOC** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

   Se necessario, creare l'attività *Scansione IOC*.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Selezionare la sezione **Impostazioni di risposta**.

5. Nel blocco **Configura le azioni di risposta al rilevamento IOC**, selezionare **Avviso e risposta** e selezionare la casella di controllo **Isola il dispositivo dalla rete**.

6. Salvare le modifiche.

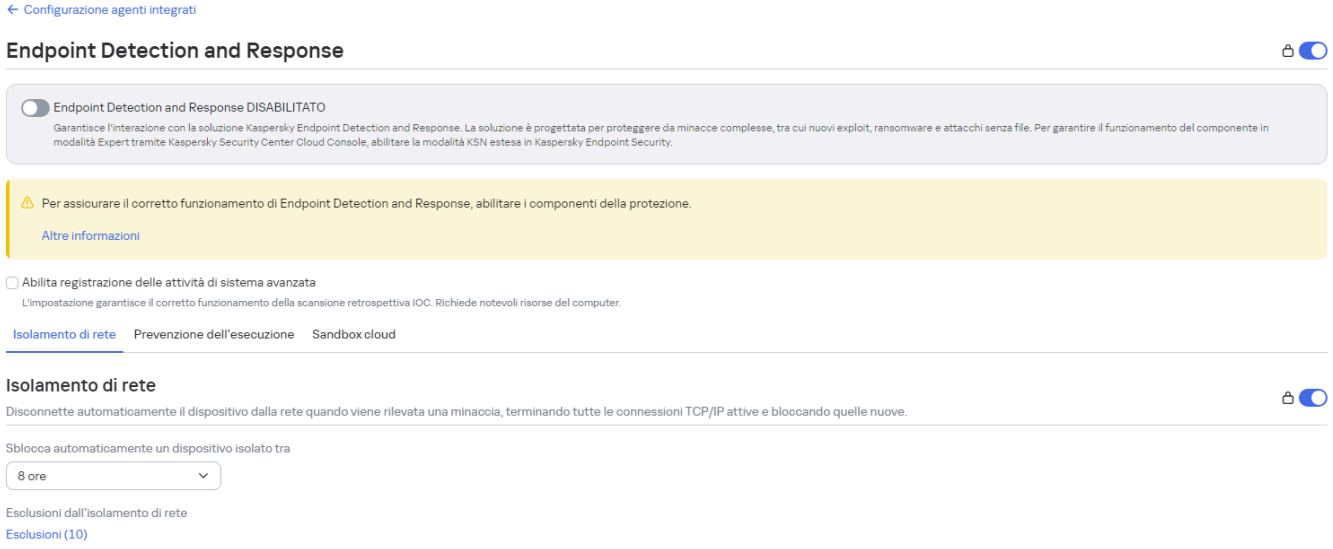
Di conseguenza, quando viene rilevato un IOC, l'applicazione isola il computer dalla rete per impedire la diffusione della minaccia.

È possibile configurare l'isolamento della rete automatico per la disabilitazione dopo un determinato periodo di tempo. Per impostazione predefinita, l'applicazione disattiva Isolamento di rete dopo 8 ore dalla sua attivazione. È anche possibile disattivare Isolamento di rete manualmente (vedere le istruzioni di seguito). Dopo aver disattivato Isolamento di rete, il computer può utilizzare la rete senza limitazioni.

Come configurare il ritardo per la disattivazione di Isolamento di rete di un computer in modalità automatica

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati → Endpoint Detection and Response**.
5. Selezionare la scheda **Isolamento di rete**.
6. Selezionare il ritardo per la disattivazione dell'Isolamento di rete.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.



Impostazioni di integrazione di EDR

Modalità Isolamento di rete manuale

È possibile attivare e disattivare Isolamento di rete manualmente. È possibile configurare la modalità Isolamento di rete manuale utilizzando le proprietà del computer nella console di Kaspersky Security Center.

È possibile attivare Isolamento di rete:

- Nei dettagli degli avvisi (solo per EDR Optimum).

  Dettagli avviso è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Per informazioni dettagliate sulla gestione dei dettagli degli avvisi, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.
- Utilizzo delle impostazioni locali dell'applicazione.

- Nelle impostazioni dell'attività *Scansione IOC*.

  Se l'attività *Scansione IOC* rileva un file IOC, è possibile isolare il computer dalla rete direttamente dal file IOC (proprietà dell'attività *Scansione IOC* → **Impostazioni applicazione** → **Risultati scansione IOC**). Kaspersky Endpoint Security consente inoltre di gestire immediatamente impostazioni aggiuntive: periodo di disattivazione dell'isolamento della rete ed esclusioni dell'isolamento della rete.

Come attivare manualmente l'isolamento di rete di un computer

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Selezionare il computer per cui si desidera configurare le impostazioni locali dell'applicazione.

   Verranno visualizzate le proprietà del computer.
3. Selezionare la scheda **Applicazioni**.
4. Fare clic su **Kaspersky Endpoint Security for Windows 14.2**.

   Verranno visualizzate le impostazioni locali dell'applicazione.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Passare a **Detection and Response** → **Endpoint Detection and Response**.
7. Nel blocco **Isolamento di rete**, fare clic su **Isola il computer dalla rete**.

È possibile configurare l'isolamento della rete automatico per la disabilitazione dopo un determinato periodo di tempo. Per impostazione predefinita, l'applicazione disattiva Isolamento di rete dopo 8 ore dalla sua attivazione. Dopo aver disattivato Isolamento di rete, il computer può utilizzare la rete senza limitazioni.

Come configurare il ritardo per la disattivazione di Isolamento di rete di un computer in modalità manuale

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Selezionare il computer per cui si desidera configurare le impostazioni locali dell'applicazione.

   Verranno visualizzate le proprietà del computer.
3. Selezionare la scheda **Attività**.

   Viene visualizzato l'elenco delle attività disponibili nel computer.
4. Selezionare l'attività **Isolamento di rete**.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Viene visualizzata una finestra, in cui è possibile selezionare il ritardo per la disattivazione di Isolamento di rete.
7. Salvare le modifiche.

Come disattivare manualmente l'isolamento di rete di un computer

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Selezionare il computer per cui si desidera configurare le impostazioni locali dell'applicazione.

   Verranno visualizzate le proprietà del computer.
3. Selezionare la scheda **Applicazioni**.

4. Fare clic su **Kaspersky Endpoint Security for Windows 14.2**.

   Verranno visualizzate le impostazioni locali dell'applicazione.

5. Selezionare la scheda **Impostazioni applicazione**.

6. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response**.

7. Nel blocco **Isolamento di rete**, fare clic su **Sblocca il computer isolato dalla rete**.

È inoltre possibile disabilitare Isolamento di rete in locale tramite la riga di comando.

A partire da Kaspersky Endpoint Security 12.10 for Windows, è possibile gestire Isolamento di rete nei dettagli degli avvisi. Nei dettagli degli avvisi è inoltre possibile specificare il periodo di isolamento della rete del computer. Per informazioni dettagliate sulla gestione dei dettagli degli avvisi, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.

Esclusioni dall'isolamento di rete

È possibile configurare le esclusioni dall'isolamento di rete. Le connessioni di rete che soddisfano le regole non vengono bloccate sul computer quando Isolamento di rete è attivato.

Per configurare le esclusioni dall'isolamento di rete, è possibile utilizzare un elenco di *profili di rete standard*. Per impostazione predefinita, le esclusioni includono i profili di rete che contengono regole che garantiscono il funzionamento costante dei dispositivi con il server DNS/DHCP e i ruoli client DNS/DHCP. È inoltre possibile modificare le impostazioni dei profili di rete standard o definire esclusioni manualmente (vedere le istruzioni riportate di seguito).

Le esclusioni specificate nelle proprietà dei criteri vengono applicate solo se Isolamento di rete viene attivato automaticamente in risposta a una minaccia rilevata. Le esclusioni specificate nelle proprietà del computer vengono applicate solo se Isolamento di rete è attivato manualmente nelle proprietà del computer in Kaspersky Security Center Console o nei dettagli degli avvisi.

Un criterio attivo non impedisce l'applicazione delle esclusioni dall'isolamento di rete configurate nelle proprietà del computer poiché tali parametri presentano scenari di utilizzo diversi.

Come aggiungere un'esclusione di Isolamento di rete in modalità automatica

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response**.

5. Selezionare la scheda **Isolamento di rete**.

6. Nel blocco **Esclusioni dall'isolamento di rete**, fare clic su **Esclusioni**.

7. Si apre una finestra; in questa finestra, fare clic su **Aggiungi** → **Aggiungi dal profilo** e selezionare i profili di rete standard per la configurazione delle esclusioni.

   Le esclusioni dall'isolamento di rete dal profilo vengono aggiunte all'elenco delle esclusioni dall'isolamento della rete. È possibile visualizzare le proprietà delle connessioni di rete. Se necessario, è possibile modificare le impostazioni delle connessioni di rete.

8. Se necessario, aggiungere un'esclusione dall'isolamento di rete manualmente. A tale scopo, nella finestra con l'elenco delle esclusioni, fare clic su **Aggiungi** → **Aggiungi** e modificare manualmente le impostazioni delle connessioni di rete.

9. Salvare le modifiche.

Come aggiungere un'esclusione di Isolamento di rete in modalità manuale

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.

2. Selezionare il computer per cui si desidera configurare le impostazioni locali dell'applicazione.

   Verranno visualizzate le proprietà del computer.

3. Selezionare la scheda **Attività**.

   Viene visualizzato l'elenco delle attività disponibili nel computer.

4. Selezionare l'attività **Isolamento di rete**.

5. Selezionare la scheda **Impostazioni applicazione**.

6. Viene visualizzata una finestra, in cui è possibile fare clic su **Esclusioni**.

7. Si apre una finestra; in questa finestra, fare clic su **Aggiungi dal profilo** e selezionare i profili di rete standard per la configurazione delle esclusioni.

   Le esclusioni dall'isolamento di rete dal profilo vengono aggiunte all'elenco delle esclusioni dall'isolamento della rete. È possibile visualizzare le proprietà delle connessioni di rete. Se necessario, è possibile modificare le impostazioni delle connessioni di rete.

8. Se necessario, aggiungere un'esclusione dall'isolamento di rete manualmente. A tale scopo, nella finestra con l'elenco delle esclusioni, fare clic su **Aggiungi** e modificare manualmente le impostazioni delle connessioni di rete.

9. Salvare le modifiche.

È inoltre possibile visualizzare l'elenco delle esclusioni dall'isolamento di rete in locale tramite la riga di comando. In questo caso, il computer deve essere isolato.

A partire da Kaspersky Endpoint Security 12.10 for Windows, è possibile aggiungere le esclusioni dell'isolamento della rete nei dettagli degli avvisi. Per informazioni dettagliate sulla gestione dei dettagli degli avvisi, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.

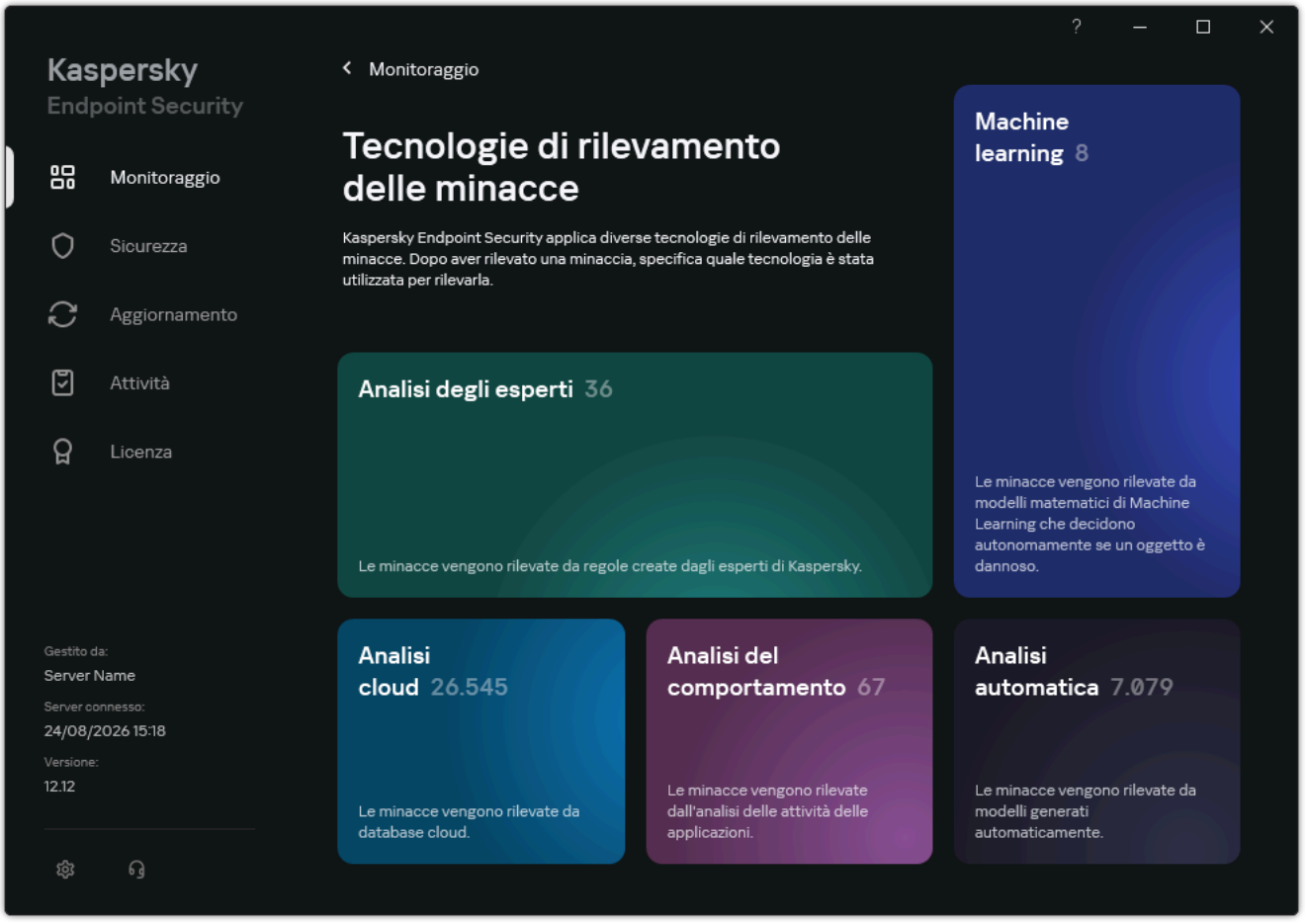
Sandbox cloud

Sandbox cloud è una tecnologia che consente di rilevare le minacce avanzate in un computer. Kaspersky Endpoint Security inoltra automaticamente i file rilevati a Sandbox cloud per l'analisi. Sandbox cloud esegue questi file in un ambiente isolato per identificare le attività dannose e prendere decisioni sulla loro reputazione. I dati contenuti in questi file vengono quindi inviati a Kaspersky Security Network. Pertanto, se Sandbox cloud rileva un file dannoso, Kaspersky Endpoint Security eseguirà l'azione appropriata per eliminare questa minaccia in tutti i computer in cui viene rilevato tale file.

Affinché Sandbox cloud possa funzionare, è necessario abilitare l'uso di Kaspersky Security Network.

Se si utilizza Kaspersky Private Security Network, la tecnologia Sandbox cloud non è disponibile.

La tecnologia Sandbox cloud è sempre abilitata ed è disponibile per tutti gli utenti di Kaspersky Security Network indipendentemente dal tipo di licenza in uso. Se la soluzione Endpoint Detection and Response Optimum è già stata distribuita, è possibile abilitare un contatore separato per le minacce rilevate dalla sandbox cloud. È possibile utilizzare questo contatore per compilare statistiche durante l'analisi delle minacce rilevate. Kaspersky Endpoint Security indica la tecnologia di rilevamento delle minacce sandbox cloud nel *Rapporto sulle minacce* nella console Kaspersky Security Center.



Contatori di minacce

Per abilitare il contatore di Sandbox cloud:

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response**.
5. Selezionare la scheda **Sandbox cloud**.
6. Attivare l'interruttore **Sandbox cloud ABILITATA**.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Ogni volta che viene rilevata una minaccia, Kaspersky Endpoint Security attiva il contatore delle minacce rilevate utilizzando Sandbox cloud nella finestra principale dell'applicazione in **Tecnologie di rilevamento delle minacce**. Kaspersky Endpoint Security indicherà anche la tecnologie di rilevamento delle minacce Sandbox cloud nel *Rapporto sulle minacce* nella console Kaspersky Security Center.

Sezione dei criteri di Endpoint Detection and Response

Guida alla migrazione da KEA a KES per EDR Optimum

Kaspersky Endpoint Security for Windows include un agente integrato per la soluzione Kaspersky Endpoint Detection and Response Optimum. Non è più necessaria un'applicazione Kaspersky Endpoint Agent separata per utilizzare EDR Optimum. Tutte le funzioni di Kaspersky Endpoint Agent verranno eseguite da Kaspersky Endpoint Security.

Quando si distribuisce Kaspersky Endpoint Security nei computer in cui è installato Kaspersky Endpoint Agent, le soluzioni Kaspersky Endpoint Detection and Response Optimum continueranno a funzionare con Kaspersky Endpoint Security. Inoltre, Kaspersky Endpoint Agent verrà rimosso dal computer. Lo stesso comportamento nel sistema si verificherà quando si aggiorna Kaspersky Endpoint Security alla versione 11.7.0 o successiva.

Kaspersky Endpoint Security non è compatibile con Kaspersky Endpoint Agent. Non è possibile installare entrambe queste applicazioni nello stesso computer.

Le seguenti condizioni devono essere soddisfatte affinché Kaspersky Endpoint Security funzioni come parte di Kaspersky Endpoint Detection and Response Optimum:

- Kaspersky Endpoint Detection and Response Optimum 2.0 o versione successiva.
- Kaspersky Security Center versione 13.2 o successiva (incluso Network Agent). Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità EDR Optimum.
- EDR Optimum può essere gestito solo utilizzando Kaspersky Security Center Web Console.

- Il trasferimento dei dati ad Administration Server è abilitato. I dati sono necessari per ottenere informazioni sui file in quarantena in un computer tramite Web Console.

- Viene stabilita una connessione in background tra Kaspersky Security Center Web Console e Administration Server. Affinché EDR Optimum funzioni con Administration Server tramite Kaspersky Security Center Web Console, è necessario stabilire una nuova connessione sicura: una *connessione in background*.

Passaggi per la migrazione della configurazione [KES+KEA] a [KES+agente integrato] per EDR Optimum

1. **Upgrade del plug-in Web di Kaspersky Endpoint Security**

   Il componente EDR Optimum può essere gestito utilizzando il plug-in Web di Kaspersky Endpoint Security versione 11.7.0 o successiva.

2. **Migrazione di criteri e attività**

   Trasferire le impostazioni di Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows. A tale scopo, utilizzare la migrazione guidata da Kaspersky Endpoint Agent in Web Console.

   Come eseguire la migrazione delle impostazioni di criteri e attività da Kaspersky Endpoint Agent a Kaspersky Endpoint Security in Web Console

   Nella finestra principale di Web Console, fare clic su **Operazioni** → **Migrazione da Kaspersky Endpoint Agent**.

   Viene eseguita la migrazione guidata di criteri e attività. Attenersi alle istruzioni della procedura guidata.

   Passaggio 1. Migrazione dei criteri

   La migrazione guidata crea un nuovo criterio che unisce le impostazioni dei criteri di Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Nell'elenco dei criteri, selezionare i criteri di Kaspersky Endpoint Agent di cui si desidera unire le impostazioni con il criterio di Kaspersky Endpoint Security. Fare clic sul criterio di Kaspersky Endpoint Agent per selezionare il criterio di Kaspersky Endpoint Security con cui unire le impostazioni. Verificare di aver selezionato i criteri corretti, quindi procedere con il passaggio successivo.

   Passaggio 2. Migrazione delle attività

   La migrazione guidata crea nuove attività per Kaspersky Endpoint Security. Nell'elenco delle attività, selezionare le attività di Kaspersky Endpoint Agent che si desidera creare per il criterio di Kaspersky Endpoint Security. Procedere con il passaggio successivo.

   Passaggio 3. Completamento della procedura guidata

   Terminare la procedura guidata. Di conseguenza, la procedura guidata esegue le seguenti operazioni:

   - Crea un nuovo criterio di Kaspersky Endpoint Security.

Il criterio unisce le impostazioni da Kaspersky Endpoint Security e Kaspersky Endpoint Agent Il criterio è denominato *<Nome del criterio di Kaspersky Endpoint Security> e <Nome del criterio di Kaspersky Endpoint Agent>*. Il nuovo criterio presenta lo stato *Inattivo*. Per continuare, modificare gli stati dei criteri di Kaspersky Endpoint Agent e Kaspersky Endpoint Security in *Inattivo* e attivare il nuovo criterio unito.

Dopo aver eseguito la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows, accertarsi che la funzionalità di trasferimento dei dati ad Administration Server (dati dei file in quarantena e dati della catena di sviluppo delle minacce) sia configurata. I valori del parametro di trasferimento dei dati non vengono migrati dal criterio di Kaspersky Endpoint Agent.

- Crea nuove attività di Kaspersky Endpoint Security.

  Le nuove attività sono copie delle attività di Kaspersky Endpoint Agent. Allo stesso tempo, la procedura guidata lascia le attività Kaspersky Endpoint Agent immutate.

3. **Licenza della funzionalità EDR Optimum**

   Se si utilizza una licenza comune di Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security per attivare Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Agent, la funzionalità EDR Optimum verrà attivata automaticamente dopo l'upgrade dell'applicazione alla versione 11.7.0 o successiva. Non è necessario eseguire altre operazioni.

   Se si utilizza una licenza del componente aggiuntivo standalone di Kaspersky Endpoint Detection and Response Optimum per attivare la funzionalità EDR Optimum, è necessario accertarsi che la chiave di EDR Optimum sia aggiunta al repository di Kaspersky Security Center e che la funzionalità di distribuzione della chiave di licenza automatica sia abilitata. Dopo aver eseguito l'upgrade dell'applicazione alla versione 11.7.0 o successiva, la funzionalità EDR Optimum viene attivata automaticamente.

   Se si utilizza una licenza di Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security per attivare Kaspersky Endpoint Agent e una licenza diversa per attivare Kaspersky Endpoint Security for Windows, è necessario sostituire la chiave di Kaspersky Endpoint Security con la chiave comune di Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security. È possibile sostituire la chiave tramite l'attività *Aggiungi chiave*.

4. **Installazione/upgrade dell'applicazione Kaspersky Endpoint Security**

   Per migrare la funzionalità EDR Optimum durante l'installazione o l'upgrade di un'applicazione, si consiglia di utilizzare l'attività di installazione remota. Quando si crea un'attività di installazione remota, è necessario selezionare il componente EDR Optimum nelle impostazioni del pacchetto di installazione.

   È inoltre possibile eseguire l'applicazione con i seguenti metodi:

   - Tramite il servizio di aggiornamento di Kaspersky.
   - In locale, utilizzando l'Installazione guidata.

   Kaspersky Endpoint Security supporta la selezione automatica dei componenti quando si effettua l'upgrade dell'applicazione in un computer con l'applicazione Kaspersky Endpoint Agent installata. La selezione automatica dei componenti dipende dalle autorizzazioni dell'account utente che sta effettuando l'upgrade dell'applicazione.

   Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando il file EXE o MSI nell'account di sistema (SYSTEM), Kaspersky Endpoint Security ottiene l'accesso alle licenze correnti delle soluzioni Kaspersky. Pertanto, se nel computer è installato Kaspersky Endpoint Agent e la soluzione EDR Optimum è attivata, il programma di installazione di Kaspersky Endpoint Security configura automaticamente il set di componenti e seleziona il componente EDR Optimum. In questo modo, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent. L'esecuzione del programma di installazione MSI nell'account di sistema (SYSTEM) viene in genere eseguita quando si effettua l'upgrade tramite Kaspersky Update Service o quando si distribuisce un pacchetto di installazione tramite Kaspersky Security Center.

Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando un file MSI in un account utente senza privilegi, Kaspersky Endpoint Security non sarà in grado di accedere alle licenze correnti delle soluzioni Kaspersky. In questo caso, Kaspersky Endpoint Security seleziona automaticamente i componenti in base alla configurazione di Kaspersky Endpoint Agent. A questo punto, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent.

Kaspersky Endpoint Security supporta l'upgrade senza riavviare il computer. È possibile selezionare la modalità di upgrade dell'applicazione nelle proprietà dei criteri.

5. **Verifica del funzionamento dell'applicazione**

   Se dopo l'installazione o l'upgrade il computer presenta lo stato *Critico* nella console di Kaspersky Security Center:

   - Accertarsi che nel computer sia installato Network Agent versione 13.2 o successiva.
   - Controllare lo stato operativo dell'agente integrato visualizzando *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non installato*, installare il componente tramite l'attività *Modifica i componenti dell'applicazione*. Se un componente presenta lo stato *Non incluso nella licenza*, verificare di aver attivato la funzionalità dell'agente integrata.
   - Accertarsi di accettare l'Informativa di Kaspersky Security Network nel nuovo criterio di Kaspersky Endpoint Security for Windows.

Kaspersky Sandbox



Kaspersky Endpoint Security for Windows include un agente integrato per l'integrazione con la soluzione Kaspersky Sandbox. Il componente *Sandbox* rileva e blocca automaticamente le minacce avanzate sui computer. Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Sandbox). Per informazioni dettagliate sulla soluzione, consultare la Guida di Kaspersky Sandbox Help e la Guida di Kaspersky Anti Targeted Attack Platform.

Integrazione dell'agente integrato con Kaspersky Sandbox

L'aggiunta del componente Sandbox è necessaria per l'integrazione con il componente Kaspersky Sandbox. È possibile selezionare il componente Sandbox durante l'installazione o l'upgrade, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

Per utilizzare il componente, è necessario che le seguenti condizioni siano soddisfatte:

- Kaspersky Security Center 13.2. Le versioni precedenti di Kaspersky Security Center non consentono la creazione di attività Scansione IOC standalone per la risposta alle minacce.
- Il componente può essere gestito solo utilizzando Web Console. Non è possibile gestire questo componente tramite Administration Console (MMC).
- L'applicazione è attivata e la funzionalità è coperta dalla licenza.
- Il trasferimento dei dati ad Administration Server è abilitato.

Per utilizzare tutte le funzionalità di Kaspersky Sandbox, verificare che il trasferimento dei file in quarantena sia abilitato. I dati sono necessari per ottenere informazioni sui file in quarantena in un computer tramite Web Console. Ad esempio, è possibile scaricare un file dalla quarantena per l'analisi in Web Console.

Come abilitare il trasferimento dei dati ad Administration Server in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Integrazione KSC**.
5. Nella sezione **Trasferimento dei dati ad Administration Server** selezionare la casella di controllo **Informazioni sui file in Quarantena**.
6. Salvare le modifiche.

- Viene stabilita una connessione in background tra Kaspersky Security Center Web Console e Administration Server

  Affinché Kaspersky Sandbox funzioni con Administration Server tramite Kaspersky Security Center Web Console, è necessario stabilire una nuova connessione sicura: una *connessione in background*. Per ulteriori dettagli sull'integrazione di Kaspersky Security Center con altre soluzioni Kaspersky, consultare la Guida di Kaspersky Security Center.

  Stabilire una connessione in background in Web Console

  1. Nella finestra principale di Web Console, fare clic su **Impostazioni** → **Integrazione**.
  2. Passare alla sezione **Integrazione**.
  3. Attivare l'interruttore **Connessione in background per l'integrazione Abilitato**.
  4. Salvare le modifiche.

  Se non viene stabilita una connessione in background tra Kaspersky Security Center Web Console e Administration Server, non è possibile creare le attività di scansione IOC autonome come parte dell'attività di risposta alle minacce.

- Per configurare una connessione attendibile con il server Sandbox, è necessario preparare un certificato TLS. È quindi necessario aggiungere il certificato nel computer utilizzando un criterio. È inoltre necessario aggiungere il certificato al server Sandbox.

  > L'autenticazione bidirezionale tramite un contenitore crittografico non è disponibile per Kaspersky Sandbox.

  È possibile aggiungere un certificato TLS in Web Console o in locale tramite la riga di comando.

- Il componente Kaspersky Sandbox è abilitato.

- I componenti dell'applicazione che garantiscono il funzionamento di Sandbox sono abilitati e operativi. I seguenti componenti assicurano il funzionamento di Sandbox:
  - Protezione minacce file.
  - Prevenzione Intrusioni Host.
  - Firewall.
  - Protezione AMSI.
  - Scansione in background.

Per abilitare e disabilitare l'integrazione con Kaspersky Sandbox:

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Sandbox**.
5. Utilizzare l'interruttore **Integrazione con Sandbox ABILITATA** per abilitare o disabilitare il componente.
6. Nel blocco **Modalità di integrazione**, selezionare la modalità operativa del componente: **Kaspersky Sandbox**.
7. Fare clic sul collegamento **Impostazioni di connessione**.

   Si apre la finestra Impostazioni della connessione al server di Sandbox.
8. Nel blocco **Certificato TLS del server**, fare clic su **Carica** e selezionare il file del certificato TLS.

   Kaspersky Endpoint Security può disporre di un solo certificato TLS per un server di Sandbox. Se in precedenza è stato aggiunto un certificato TLS, tale certificato viene revocato. Viene utilizzato solo l'ultimo certificato aggiunto.
9. Configurare le impostazioni di connessione avanzate per i server di Kaspersky Sandbox:
   - **Timeout (msec)**. Timeout della connessione per il server Sandbox. Allo scadere del timeout configurato, Kaspersky Endpoint Security invia una richiesta al server successivo. È possibile aumentare il timeout della connessione per il server se la velocità di connessione è lenta o se la connessione è instabile. Il timeout della richiesta consigliato è di 0,5 secondi o meno.
   - **Coda richieste**. Dimensione della cartella della coda di richieste. Quando si inviano più oggetti per la scansione in Sandbox, Kaspersky Endpoint Security crea una coda di richieste. Per impostazione predefinita, la dimensione della cartella della coda di richieste è limitata a 100 MB. Una volta raggiunta la dimensione massima, Sandbox interrompe l'aggiunta di nuove richieste alla coda e invia l'evento corrispondente a Kaspersky Security Center. È possibile configurare la dimensione della cartella della coda delle richieste in base alla configurazione del server.
10. Nel blocco **Connessione ai server Sandbox**, fare clic sul pulsante **Aggiungi**.

11. Si apre una finestra; nella finestra, immettere l'indirizzo e la porta del server di Sandbox (IPv4, IPv6, DNS).

    Per ulteriori dettagli sulla distribuzione di immagini virtuali e sulla configurazione dei server di Sandbox, consultare la Guida di Kaspersky Sandbox.

12. Salvare le modifiche.

    A questo punto, Kaspersky Endpoint Security verifica il certificato TLS. Se il certificato viene verificato correttamente, Kaspersky Endpoint Security carica il certificato nel computer durante la successiva sincronizzazione con Kaspersky Security Center. Se sono stati aggiunti due certificati TLS, Kaspersky Sandbox utilizzerà il certificato più recente per stabilire una connessione attendibile. Controllare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Sandbox** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

    È possibile abilitare o disabilitare l'integrazione con Kaspersky Sandbox in Web Console o in locale con la riga di comando.

Kaspersky Endpoint Security salva le informazioni sul funzionamento del componente Kaspersky Sandbox in un rapporto. Il rapporto contiene anche informazioni sugli errori. Se si riceve un errore con una descrizione che corrisponde a `Error code: XXX` formato (ad esempio, `0xa67b01f4`), contattare l'Assistenza tecnica.

Scansione degli indicatori di compromissione (attività standalone)

Un *indicatore di compromissione (IOC)* è una serie di dati su un oggetto o un'attività che indica un accesso non autorizzato al computer (compromissione dei dati). Ad esempio, molti tentativi non riusciti di accesso al sistema possono costituire un indicatore di compromissione. L'attività *Scansione IOC* consente di trovare indicatori di compromissione sul computer e di adottare misure di risposta alle minacce.

Kaspersky Endpoint Security ricerca gli indicatori di compromissione utilizzando i file IOC. I *file IOC* sono file che contengono le serie di indicatori che l'applicazione tenta di abbinare per eseguire un rilevamento. I file IOC devono essere conformi allo standard OpenIOC. Kaspersky Endpoint Security genera automaticamente i file IOC per Kaspersky Sandbox.

Modalità di esecuzione dell'attività Scansione IOC

L'applicazione crea attività di scansione IOC autonome per Kaspersky Sandbox. *Attività di scansione IOC autonoma* è un'attività di gruppo che viene creata automaticamente quando si reagisce a una minaccia rilevata da Kaspersky Sandbox. Kaspersky Endpoint Security genera automaticamente il file IOC. I file IOC personalizzati non sono supportati. Le attività vengono eliminate automaticamente 30 giorni dopo l'ora di creazione. Per altri dettagli sulle attività di scansione IOC autonome, consultare la Guida di Kaspersky Sandbox.

Impostazioni attività di Scansione IOC

Kaspersky Sandbox può creare ed eseguire automaticamente attività *Scansione IOC* quando reagisce alle minacce.

È possibile configurare le impostazioni solo in Web Console.

Affinché tutte le attività di scansione IOC standalone di Kaspersky Sandbox vengano eseguite correttamente, è necessario Kaspersky Security Center 13.2.

Per modificare le impostazioni dell'attività Scansione IOC:

1. Nella finestra principale di Web Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Scansione IOC** di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà dell'attività.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare alla sezione **Impostazioni di scansione IOC**.

5. Configurare le azioni se viene rilevato un indicatore di compromissione:

   - **Sposta la copia in Quarantena, elimina oggetto**. Se questa opzione è selezionata, Kaspersky Endpoint Security elimina l'oggetto dannoso trovato nel computer. Prima di eliminare l'oggetto, Kaspersky Endpoint Security crea una copia di backup nel caso in cui sia necessario ripristinare l'oggetto in un secondo momento. Kaspersky Endpoint Security sposta la copia di backup in Quarantena.

   - **Esegui scansione delle aree critiche**. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue l'attività *Scansione delle aree critiche*. Per impostazione predefinita, Kaspersky Endpoint Security esamina la memoria del kernel, i processi in esecuzione e i settori di avvio del disco.

   - **Esegui solo quando il computer è inattivo**. Avvio posticipato dell'attività quando le risorse del computer sono occupate. Kaspersky Endpoint Security avvia l'attività di scansione se il computer è bloccato o se lo screensaver è attivo. Se l'esecuzione dell'attività è stata interrotta, ad esempio sbloccando il computer, Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui era stata interrotta. Questa opzione di pianificazione consente di conservare le risorse del computer durante l'utilizzo del computer.

6. Salvare le modifiche.

È possibile visualizzare i risultati dell'attività nelle proprietà dell'attività nelle sezione **Risultati**. È possibile visualizzare le informazioni sugli indicatori di compromissione rilevati nelle proprietà dell'attività: **Impostazioni applicazione → Risultati scansione IOC**.

I risultati della scansione IOC vengono conservati per 30 giorni. Al termine di questo periodo, Kaspersky Endpoint Security elimina automaticamente le voci meno recenti.

Guida alla migrazione da KEA a KES per Kaspersky Sandbox

Kaspersky Endpoint Security for Windows include un agente integrato per la soluzione Kaspersky Sandbox. Non è più necessaria un'applicazione Kaspersky Endpoint Agent separata per utilizzare Kaspersky Sandbox. Tutte le funzioni di Kaspersky Endpoint Agent verranno eseguite da Kaspersky Endpoint Security.

Quando si distribuisce Kaspersky Endpoint Security nei computer in cui è installato Kaspersky Endpoint Agent, la soluzione Kaspersky Sandbox continuerà a funzionare con Kaspersky Endpoint Security. Inoltre, Kaspersky Endpoint Agent verrà rimosso dal computer. Lo stesso comportamento nel sistema si verificherà quando si aggiorna Kaspersky Endpoint Security alla versione 11.7.0 o successiva.

Kaspersky Endpoint Security non è compatibile con Kaspersky Endpoint Agent. Non è possibile installare entrambe queste applicazioni nello stesso computer.

Le seguenti condizioni devono essere soddisfatte affinché Kaspersky Endpoint Security funzioni come parte di Kaspersky Sandbox:

- Kaspersky Sandbox versione 2.0 o successiva.
- Kaspersky Security Center versione 13.2 o successiva (incluso Network Agent). Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità Kaspersky Sandbox.
- Kaspersky Sandbox può essere gestito solo utilizzando Kaspersky Security Center Web Console.
- Il trasferimento dei dati ad Administration Server è abilitato. I dati sono necessari per ottenere informazioni sui file in quarantena in un computer tramite Web Console.
- Viene stabilita una connessione in background tra Kaspersky Security Center Web Console e Administration Server. Affinché Kaspersky Sandbox funzioni con Administration Server tramite Kaspersky Security Center Web Console, è necessario stabilire una nuova connessione sicura: una *connessione in background*.

Passaggi per la migrazione della configurazione [KES+KEA] a [KES+agente integrato] per Kaspersky Sandbox

1. **Upgrade del plug-in Web di Kaspersky Endpoint Security**

   Il componente Kaspersky Sandbox può essere gestito utilizzando il plug-in Web di Kaspersky Endpoint Security versione 11.7.0 o successiva.

2. **Migrazione di criteri e attività**

   Trasferire le impostazioni di Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows. A tale scopo, utilizzare la migrazione guidata da Kaspersky Endpoint Agent in Web Console.

   Come eseguire la migrazione delle impostazioni di criteri e attività da Kaspersky Endpoint Agent a Kaspersky Endpoint Security in Web Console

   Nella finestra principale di Web Console, fare clic su **Operazioni → Migrazione da Kaspersky Endpoint Agent**.

   Viene eseguita la migrazione guidata di criteri e attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Migrazione dei criteri

La migrazione guidata crea un nuovo criterio che unisce le impostazioni dei criteri di Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Nell'elenco dei criteri, selezionare i criteri di Kaspersky Endpoint Agent di cui si desidera unire le impostazioni con il criterio di Kaspersky Endpoint Security. Fare clic sul criterio di Kaspersky Endpoint Agent per selezionare il criterio di Kaspersky Endpoint Security con cui unire le impostazioni. Verificare di aver selezionato i criteri corretti, quindi procedere con il passaggio successivo.

Passaggio 2. Migrazione delle attività

La migrazione guidata crea nuove attività per Kaspersky Endpoint Security. Nell'elenco delle attività, selezionare le attività di Kaspersky Endpoint Agent che si desidera creare per il criterio di Kaspersky Endpoint Security. Procedere con il passaggio successivo.

Passaggio 3. Completamento della procedura guidata

Terminare la procedura guidata. Di conseguenza, la procedura guidata esegue le seguenti operazioni:

- Crea un nuovo criterio di Kaspersky Endpoint Security.

  Il criterio unisce le impostazioni da Kaspersky Endpoint Security e Kaspersky Endpoint Agent Il criterio è denominato *<Nome del criterio di Kaspersky Endpoint Security> e <Nome del criterio di Kaspersky Endpoint Agent>*. Il nuovo criterio presenta lo stato *Inattivo*. Per continuare, modificare gli stati dei criteri di Kaspersky Endpoint Agent e Kaspersky Endpoint Security in *Inattivo* e attivare il nuovo criterio unito.

  Dopo aver eseguito la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows, accertarsi che la funzionalità di trasferimento dei dati ad Administration Server (dati dei file in quarantena e dati della catena di sviluppo delle minacce) sia configurata. I valori del parametro di trasferimento dei dati non vengono migrati dal criterio di Kaspersky Endpoint Agent.

- Crea nuove attività di Kaspersky Endpoint Security.

  Le nuove attività sono copie delle attività di Kaspersky Endpoint Agent. Allo stesso tempo, la procedura guidata lascia le attività Kaspersky Endpoint Agent immutate.

3. **Gestione della licenza della funzionalità Kaspersky Sandbox**

   Per attivare Kaspersky Endpoint Security come parte della soluzione Kaspersky Sandbox, è necessaria una licenza separata per il componente aggiuntivo Kaspersky Sandbox. È possibile aggiungere la chiave tramite l'attività *Aggiungi chiave*. Di conseguenza, verranno aggiunte due chiavi all'applicazione: *Kaspersky Endpoint Security* e *Kaspersky Sandbox*.

4. **Installazione/upgrade dell'applicazione Kaspersky Endpoint Security**

   Per migrare la funzionalità Kaspersky Sandbox durante l'installazione o l'upgrade di un'applicazione, si consiglia di utilizzare l'attività di installazione remota. Quando si crea un'attività di installazione remota, è necessario selezionare il componente Kaspersky Sandbox nelle impostazioni del pacchetto di installazione.

È inoltre possibile eseguire l'applicazione con i seguenti metodi:

- Tramite il servizio di aggiornamento di Kaspersky.
- In locale, utilizzando l'Installazione guidata.

Kaspersky Endpoint Security supporta la selezione automatica dei componenti quando si effettua l'upgrade dell'applicazione in un computer con l'applicazione Kaspersky Endpoint Agent installata. La selezione automatica dei componenti dipende dalle autorizzazioni dell'account utente che sta effettuando l'upgrade dell'applicazione.

Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando il file EXE o MSI nell'account di sistema (SYSTEM), Kaspersky Endpoint Security ottiene l'accesso alle licenze correnti delle soluzioni Kaspersky. Pertanto, se nel computer è installato Kaspersky Endpoint Agent e la soluzione Kaspersky Sandbox è attivata, il programma di installazione di Kaspersky Endpoint Security configura automaticamente il set di componenti e seleziona il componente Kaspersky Sandbox. In questo modo, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent. L'esecuzione del programma di installazione MSI nell'account di sistema (SYSTEM) viene in genere eseguita quando si effettua l'upgrade tramite Kaspersky Update Service o quando si distribuisce un pacchetto di installazione tramite Kaspersky Security Center.

Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando un file MSI in un account utente senza privilegi, Kaspersky Endpoint Security non sarà in grado di accedere alle licenze correnti delle soluzioni Kaspersky. In questo caso, Kaspersky Endpoint Security seleziona automaticamente i componenti in base alla configurazione di Kaspersky Endpoint Agent. A questo punto, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent.

Kaspersky Endpoint Security supporta l'upgrade senza riavviare il computer. È possibile selezionare la modalità di upgrade dell'applicazione nelle proprietà dei criteri.

5 Verifica del funzionamento dell'applicazione

Se dopo l'installazione o l'upgrade il computer presenta lo stato *Critico* nella console di Kaspersky Security Center:

- Accertarsi che nel computer sia installato Network Agent versione 13.2 o successiva.
- Controllare lo stato operativo dell'agente integrato visualizzando *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non installato*, installare il componente tramite l'attività *Modifica i componenti dell'applicazione*. Se un componente presenta lo stato *Non incluso nella licenza*, verificare di aver attivato la funzionalità dell'agente integrata.
- Accertarsi di accettare l'Informativa di Kaspersky Security Network nel nuovo criterio di Kaspersky Endpoint Security for Windows.

Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Security for Windows supporta l'utilizzo della soluzione Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* è una soluzione progettata per il rilevamento tempestivo di minacce sofisticate come attacchi mirati, minacce APT (Advanced Persistent Threat), attacchi zero-day e di altro tipo. Kaspersky Anti Targeted Attack Platform include tre unità funzionali:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

È possibile acquistare tutte le unità funzionali o le singole unità funzionali separatamente. Per informazioni dettagliate sulla soluzione, consultare la Guida di Kaspersky Anti Targeted Attack Platform. L'applicazione include agenti predefiniti per i componenti EDR e NDR. L'applicazione supporta anche l'utilizzo del componente Sandbox, che fa parte di KATA.

Strumenti di threat intelligence

Kaspersky Endpoint Detection and Response utilizza i seguenti strumenti Threat Intelligence:

- Integrazione con Kaspersky Threat Intelligence Portal, che contiene e mostra informazioni sulla reputazione di file e indirizzi Web.
- Database delle minacce di Kaspersky.
- L'infrastruttura di servizi cloud di Kaspersky Security Network (di seguito denominata anche "KSN"), che fornisce accesso ai file in tempo reale, siti Web e informazioni sulla reputazione del software dalla knowledge base di Kaspersky. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce risposte più rapide da parte delle applicazioni Kaspersky alle minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi positivi.

Principio di funzionamento della soluzione

L'applicazione Kaspersky Endpoint Security viene installata nei singoli computer dell'infrastruttura IT aziendale e monitora continuamente i processi, le connessioni di rete aperte e i file modificati. Le informazioni sugli eventi nel computer (dati di telemetria) vengono inviate al server di Kaspersky Anti Targeted Attack Platform. In questo caso, Kaspersky Endpoint Security invia anche informazioni al server di Kaspersky Anti Targeted Attack Platform sulle minacce rilevate dall'applicazione, nonché informazioni sull'elaborazione dei risultati di tali minacce.

L'integrazione di EDR (KATA) e NDR (KATA) è configurata nella console di Kaspersky Security Center. L'agente integrato viene quindi gestito tramite la console di Kaspersky Anti Targeted Attack Platform, inclusa l'esecuzione delle attività, la gestione degli oggetti in quarantena, la visualizzazione dei rapporti e altre azioni.

Configurazioni di Kaspersky Endpoint Security per l'utilizzo con EDR / NDR (KATA)

Per l'utilizzo con EDR / NDR (KATA), è possibile utilizzare le seguenti configurazioni:

- **[KES+agente integrato]**. In questa configurazione, Kaspersky Endpoint Security funge sia da applicazione che garantisce la sicurezza del computer sia da applicazione per l'utilizzo con EDR / NDR (KATA). L'agente integrato per EDR (KATA) è disponibile in Kaspersky Endpoint Security 12.1 for Windows o versioni successive. L'agente integrato per NDR (KATA) è disponibile in Kaspersky Endpoint Security 12.7 for Windows o versioni successive.

- **[EPP di terzi+EDR Agent]**. In questa configurazione, la sicurezza dell'infrastruttura IT è garantita da Endpoint Protection Platform (EPP) di terzi. L'interazione con EDR / NDR (KATA) è fornita da Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent (EDR Agent). In questa configurazione, EDR Agent è compatibile con le applicazioni PPE di terzi. EDR Agent per EDR (KATA) è disponibile in Kaspersky Endpoint Security 12.3 for Windows o versioni successive. EDR Agent per NDR (KATA) è disponibile in Kaspersky Endpoint Security 12.7 for Windows o versioni successive.

Supporto per le versioni precedenti di Kaspersky Endpoint Security

Se si utilizza Kaspersky Endpoint Security 11.2.0-11.8.0 per l'interoperabilità con Kaspersky Anti Targeted Attack Platform (EDR), l'applicazione include Kaspersky Endpoint Agent. È possibile installare Kaspersky Endpoint Agent insieme a Kaspersky Endpoint Security.

Se si utilizza Kaspersky Endpoint Security 11.9.0-12.0, è necessario installare Kaspersky Endpoint Agent separatamente perché a partire da Kaspersky Endpoint Security 11.9.0 il pacchetto di distribuzione di Kaspersky Endpoint Agent non fa più parte del kit di distribuzione di Kaspersky Endpoint Security.

Integrazione dell'agente integrato con EDR / NDR (KATA)

Per l'integrazione con EDR/NDR (KATA), è necessario aggiungere il componente pertinente: Endpoint Detection and Response (KATA) o Network Detection and Response (KATA). È possibile selezionare i componenti per l'integrazione con EDR / NDR (KATA) durante l'installazione o l'upgrade dell'applicazione, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

A partire dalla versione 12.11 di Kaspersky Endpoint Security for Windows, il componente EDR (KATA) è stato rinominato in **Endpoint Detection and Response Expert (versione 8.0 o successiva)**. In questa versione dell'applicazione, il componente è compatibile con Kaspersky Anti Targeted Attack Platform 7.1 e versioni precedenti, nonché con Kaspersky Endpoint Detection and Response Expert (on-premises).

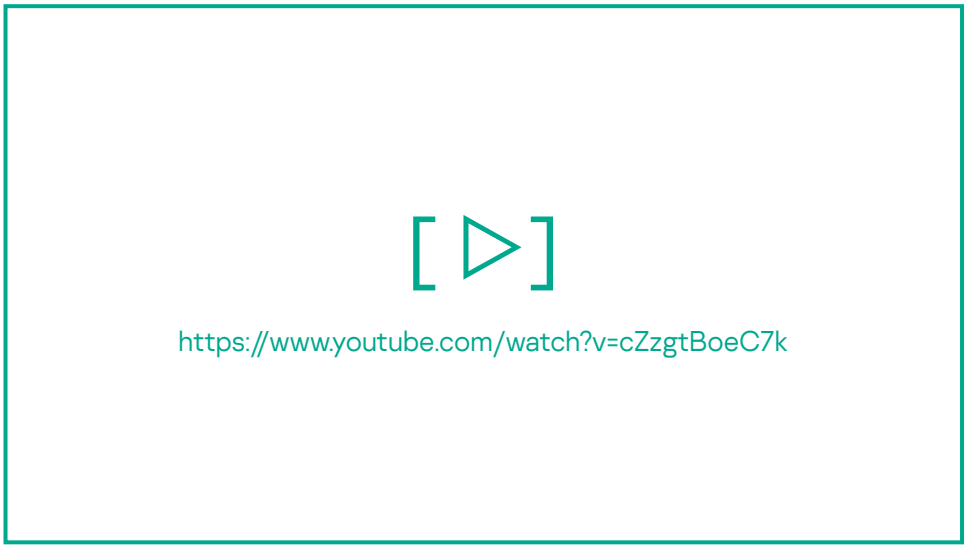
I componenti Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), e Endpoint Detection and Response Expert (on-premises) i non sono compatibili tra loro.

Per utilizzare EDR / NDR (KATA), è necessario che le seguenti condizioni siano soddisfatte:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform versioni 5.0-7.1.

- NDR (KATA): Kaspersky Anti Targeted Attack Platform versione 7.0 o successiva.

- EDR (KATA): Kaspersky Endpoint Security for Windows 12.1 o versioni successive. Per ulteriori dettagli sulla compatibilità di KATA con le diverse versioni di Kaspersky Endpoint Security, fare riferimento alla Guida di Kaspersky Anti Targeted Attack Platform.
- NDR (KATA): Kaspersky Endpoint Security for Windows 12.7 o versioni successive.
- Kaspersky Security Center versione 14.2 o successiva. Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità di EDR / NDR (KATA).
- L'applicazione è attivata e la funzionalità è coperta dalla licenza.
- I componenti Endpoint Detection and Response (KATA) e Network Detection and Response (KATA) sono abilitati.
- I componenti dell'applicazione che garantiscono il funzionamento di EDR / NDR (KATA) sono abilitati e operativi. I seguenti componenti assicurano il funzionamento di EDR / NDR (KATA):
  - Protezione minacce file.
  - Protezione minacce web.
  - Protezione minacce di posta.
  - Prevenzione Exploit.
  - Rilevamento del Comportamento.
  - Prevenzione Intrusioni Host.
  - Protezione AMSI.
  - Scansione in background.
  - Kaspersky Security Network.



https://www.youtube.com/watch?v=gd-rySv0ThQ

L'integrazione con Endpoint Detection and Response (KATA) prevede i seguenti passaggi:

1. **Installazione dei componenti Endpoint Detection and Response (KATA) e Network Detection and Response (KATA)**

   È possibile selezionare i componenti EDR (KATA) e NDR (KATA) durante l'installazione o l'upgrade, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

   > È necessario riavviare il computer per completare l'aggiornamento dell'applicazione con i nuovi componenti.

2. **Attivazione di Endpoint Detection and Response (KATA) e Network Detection and Response (KATA)**

   È necessario acquistare una licenza separata per EDR (KATA) e NDR (KATA) (ad esempio, il componente aggiuntivo Kaspersky Endpoint Detection and Response (KATA)).

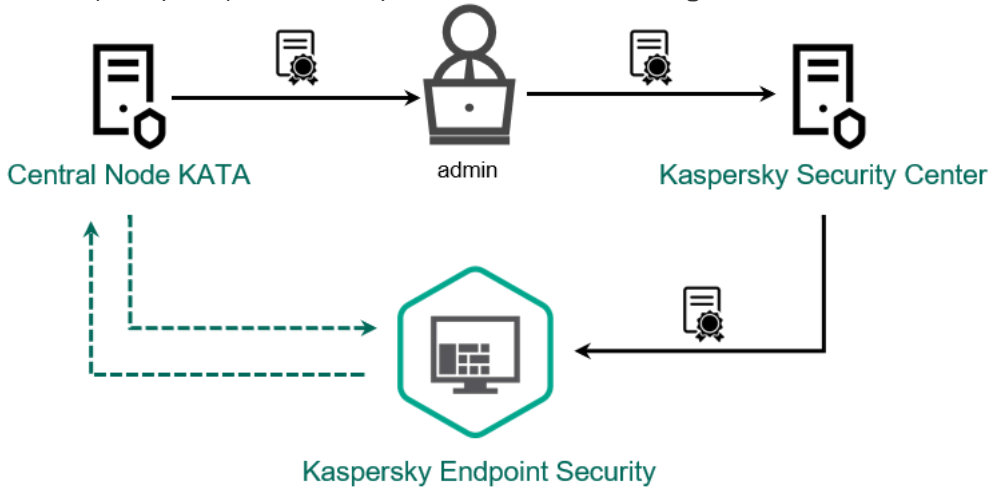
   La funzionalità diventa disponibile dopo l'aggiunta di una chiave separata che copre le funzionalità EDR (KATA) e NDR (KATA). Di conseguenza, nel computer vengono aggiunte più chiavi: una chiave per Kaspersky Endpoint Security e altre chiavi per Kaspersky Endpoint Detection and Response (KATA) e Network Detection and Response (KATA).

   La licenza per la funzionalità EDR (KATA) e NDR (KATA) autonoma è la stessa della licenza di Kaspersky Endpoint Security.

   Verificare che sia la funzionalità EDR (KATA) che NDR (KATA) sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

3. **Connessione a Central Node**

   Kaspersky Anti Targeted Attack Platform richiede di stabilire una connessione attendibile tra Kaspersky Endpoint Security e il componente Central Node. Per configurare una connessione attendibile, è necessario utilizzare un certificato TLS. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Quindi è necessario aggiungere il certificato TLS a Kaspersky Endpoint Security (vedere le istruzioni di seguito).



Aggiunta di un certificato TLS a Kaspersky Endpoint Security

Per impostazione predefinita, Kaspersky Endpoint Security controlla solo il certificato TLS di Central Node. Per rendere la connessione più sicura, è inoltre possibile abilitare la verifica del computer in Central Node (autenticazione a due vie). Per abilitare questa verifica, è necessario attivare l'autenticazione a due vie nelle impostazioni di Central Node e Kaspersky Endpoint Security. Per utilizzare l'autenticazione a due vie, è necessario anche un contenitore crittografico. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform).

Come connettere un computer Kaspersky Endpoint Security a Central Node tramite Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Detection and Response**, quindi selezionare il componente che si desidera configurare: **Endpoint Detection and Response Expert (on-premises)** o **Network Detection and Response (KATA)**.
5. Selezionare la casella di controllo corrispondente: **Endpoint Detection and Response Expert (versione 7.1 o precedente)** o **Network Detection and Response (KATA)**.
6. Fare clic su **Impostazioni della connessione al server**.
7. Configurare la connessione al server:
   - **Timeout (sec)**. Timeout massimo di risposta del server di Central Node. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server Central Node.
   - **Certificato TLS del server**. Certificato TLS per stabilire una connessione attendibile con il server di Central Node. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform).
   - **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

     Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.
8. Fare clic su **OK**.
9. Aggiungere i server di Central Node. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.

   È possibile aggiungere più indirizzi server di Central Node. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

10. Se necessario, configurare la telemetria.

11. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come connettere un computer Kaspersky Endpoint Security a Central Node tramite Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare alla sezione **Configurazione agenti integrati** e selezionare il componente che si desidera configurare: **Endpoint Detection and Response Expert (on-premises)** o **Network Detection and Response (KATA)**.

5. Attivare l'interruttore corrispondente: **Endpoint Detection and Response Expert (on-premises) ABILITATO** o **Network Detection and Response (KATA) ABILITATO**.

6. Per configurare EDR (KATA), selezionare **Endpoint Detection and Response Expert (versione 7.1 o precedente)** dall'elenco delle soluzioni.

7. Fare clic su **Impostazioni di connessione**.

8. Configurare la connessione al server:

   - **Timeout (sec)**. Timeout massimo di risposta del server di Central Node. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server Central Node.

   - **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server di Central Node. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform).

   - **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

     Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

9. Fare clic su **OK**.

10. Aggiungere i server di Central Node. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.

    È possibile aggiungere più indirizzi server di Central Node. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

11. Se necessario, configurare la telemetria.

12. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

È inoltre possibile aggiungere un certificato TLS in locale tramite la riga di comando.

Di conseguenza, il computer viene aggiunto alla console di Kaspersky Anti Targeted Attack Platform. Controllare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo dei componenti nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. I componenti **Endpoint Detection and Response Expert (versione 8.0 o successiva)** e **Network Detection and Response (KATA)** verranno aggiunti all'elenco dei componenti di Kaspersky Endpoint Security.

> È possibile verificare lo stato dei componenti nella console di Kaspersky Security Center nelle proprietà del computer nella sezione **Componenti**. Considerare quanto segue durante il controllo dello stato del componente nella console. Se il componente non è installato e la funzionalità non è coperta dalla licenza, la console mostra lo stato **Non supportato dalla licenza** anziché **Non installato**.

A partire da Kaspersky Endpoint Security 12.6 for Windows, è possibile monitorare lo stato del componente EDR (KATA) in Kaspersky Security Center Administration Console (MMC). Lo stato corrente del componente viene visualizzato nelle proprietà del computer nella colonna **Stato Endpoint Sensor** (*In esecuzione*, *Avvio in corso*, *Arrestata*, *Sospesa*, *Non riuscito*, *Sconosciuto*). Web Console non mostra lo stato di Endpoint Sensor.

Configurazione della telemetria EDR (KATA).

Telemetria è un elenco di eventi che si sono verificati nel computer protetto. Kaspersky Endpoint Security analizza i dati di telemetria e li invia a Kaspersky Anti Targeted Attack Platform durante la sincronizzazione. Gli eventi di telemetria arrivano sul server quasi continuamente. Kaspersky Endpoint Security avvia la sincronizzazione con il server quando viene soddisfatta una delle seguenti condizioni:

- L'intervallo di sincronizzazione è scaduto.
- Il numero di eventi nel buffer supera il limite massimo.

Pertanto, per impostazione predefinita, l'applicazione esegue la sincronizzazione ogni 30 secondi oppure ogni volta che il buffer contiene 1024 eventi. È possibile configurare il comportamento di sincronizzazione nella policy di Kaspersky Endpoint Security e selezionare i valori ottimali in base al carico di rete (vedere le istruzioni di seguito).

Se non è presente alcuna connessione tra Kaspersky Endpoint Security e il server, l'applicazione accoda i nuovi eventi. Quando la connessione viene ripristinata, Kaspersky Endpoint Security invia gli eventi in coda al server nell'ordine corretto. Per evitare di sovraccaricare il server, Kaspersky Endpoint Security potrebbe ignorare alcuni eventi. Per abilitare questo, è possibile ottimizzare le impostazioni di trasmissione degli eventi, ad esempio, per impostare un valore massimo di eventi all'ora (vedere le istruzioni di seguito).

Se si utilizza Kaspersky Anti Targeted Attack Platform insieme a un'altra soluzione che usa anch'essa la telemetria, è possibile disattivare la telemetria per KATA (EDR) (vedere le istruzioni riportate di seguito). Ciò consente di ottimizzare il carico del server per queste soluzioni. Ad esempio, se è stata distribuita la soluzione Managed Detection and Response e KATA (EDR), è possibile utilizzare la telemetria MDR e creare attività Risposta alle minacce in KATA (EDR).

Come configurare la telemetria in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella struttura della console, selezionare **Criteri**.

3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

4. Nella finestra del criterio, selezionare **Detection and Response**, quindi selezionare il componente che si desidera configurare: **Endpoint Detection and Response Expert (on-premises)** o **Network Detection and Response (KATA)**.

5. Configurare l'impostazione **Invia richiesta di sincronizzazione al server KATA ogni (min.)**. Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security invia informazioni sulle attività e le impostazioni dell'applicazione modificate.

6. Verificare che la casella di controllo **Invia telemetria a KATA** sia selezionata.

7. Se necessario, configurare la sincronizzazione con le impostazioni del server nel blocco **Impostazioni trasmissione dati**:

   - **Ritardo di trasmissione eventi massimo (sec)**. L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione. L'impostazione predefinita è 30 secondi.

   - **Numero massimo di pacchetti eventi**. L'applicazione si sincronizza con il server quando il buffer si riempie di eventi. L'impostazione predefinita è 1024 eventi.

8. Se necessario, selezionare la casella di controllo **Abilita limitazione delle richieste** nel blocco **Limitazione delle richieste**.

   Questa funzionalità consente di ottimizzare il carico sul server. Se questa funzionalità è abilitata, l'applicazione limita la trasmissione degli eventi. Se il numero di eventi supera i limiti configurati, Kaspersky Endpoint Security interrompe l'invio degli eventi.

9. Configurare le impostazioni di ottimizzazione per l'invio degli eventi al server:

   - **Numero massimo di eventi all'ora**. L'applicazione analizza il flusso di dati di telemetria e limita l'invio degli eventi se il flusso di eventi supera il limite di eventi all'ora configurato. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora. L'impostazione predefinita è 3000 eventi all'ora. Se l'applicazione è installata in un server, il flusso di dati di telemetria è maggiore. Per i server, è consigliabile aumentare il valore a 60.000 eventi all'ora.

   - **Percentuale di eccedenza limite eventi**. L'applicazione ordina gli eventi in base al tipo (ad esempio, eventi di "Modifiche nel Registro di sistema") e limita la trasmissione degli eventi se il rapporto tra eventi dello stesso tipo e il numero totale di eventi supera il limite percentuale configurato. Kaspersky Endpoint Security riprende l'invio degli eventi quando il rapporto tra altri eventi e il numero totale di eventi diventa di nuovo sufficientemente elevato. L'impostazione predefinita è 15%.

10. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare la telemetria in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Configurazione agenti integrati → Endpoint Detection and Response Expert (on-premises)**.

5. Per configurare EDR (KATA), selezionare **Endpoint Detection and Response Expert (versione 7.1 o precedente)** dall'elenco delle soluzioni.

6. Assicurarsi che la casella di controllo **Invia telemetria ai server KATA** sia selezionata nel blocco **Impostazioni trasmissione dati**.

7. Configurare l'impostazione **Invia richiesta di sincronizzazione al server ogni (min)**. Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security invia informazioni sulle attività e le impostazioni dell'applicazione modificate.

8. Verificare che la casella di controllo **Invia telemetria ai server KATA** sia selezionata.

9. Se necessario, configurare la sincronizzazione con le impostazioni del server nel blocco **Impostazioni trasmissione dati**:

   - **Ritardo di trasmissione eventi massimo (sec)**. L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione. L'impostazione predefinita è 30 secondi.

   - **Numero massimo di pacchetti eventi**. L'applicazione si sincronizza con il server quando il buffer si riempie di eventi. L'impostazione predefinita è 1024 eventi.

10. Se necessario, selezionare la casella di controllo **Abilita limitazione delle richieste** nel blocco **Limitazione delle richieste**.

    Questa funzionalità consente di ottimizzare il carico sul server. Se questa funzionalità è abilitata, l'applicazione limita la trasmissione degli eventi. Se il numero di eventi supera i limiti configurati, Kaspersky Endpoint Security interrompe l'invio degli eventi.

11. Configurare le impostazioni di ottimizzazione per l'invio degli eventi al server:

    - **Numero massimo di eventi all'ora**. L'applicazione analizza il flusso di dati di telemetria e limita l'invio degli eventi se il flusso di eventi supera il limite di eventi all'ora configurato. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora. L'impostazione predefinita è 3000 eventi all'ora. Se l'applicazione è installata in un server, il flusso di dati di telemetria è maggiore. Per i server, è consigliabile aumentare il valore a 60.000 eventi all'ora.

    - **Percentuale di eccedenza limite eventi**. L'applicazione ordina gli eventi in base al tipo (ad esempio, eventi di "Modifiche nel Registro di sistema") e limita la trasmissione degli eventi se il rapporto tra eventi dello stesso tipo e il numero totale di eventi supera il limite percentuale configurato. Kaspersky Endpoint Security riprende l'invio degli eventi quando il rapporto tra altri eventi e il numero totale di eventi diventa di nuovo sufficientemente elevato. L'impostazione predefinita è 15%.

12. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare alla sezione **Integrazione KATA** → **Esclusioni di telemetria**.

5. In **Impostazioni trasmissione dati**, selezionare la casella di controllo **Usa esclusioni**.

6. Fare clic su **Aggiungi** e configurare le esclusioni:

I criteri sono combinati con la logica *AND*.

- **Percorso**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. Affinché l'esclusione funzioni, è necessario specificare il percorso del file.
- **Riga di comando**. Comando utilizzato per eseguire l'oggetto.
- **Descrizione**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo).

  Per ulteriori informazioni sulla risorsa VersionInfo, visitare il sito Web di Microsoft.
- **Nome originale del file**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo).
- **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo).
- **MD5**. Hash MD5 del file.
- **SHA256**. Hash SHA256 del file.
- **Tipi di evento**. Affinché l'esclusione funzioni, è necessario selezionare almeno un tipo di evento.

7. Salvare le modifiche.

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Attività**.

   Viene aperto l'elenco delle attività.
2. Fare clic su **Nuova attività**.

Verrà avviata la Creazione guidata attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione del tipo di attività

1. Selezionare **Kaspersky Endpoint Security for Windows (14.2)** → **Rollback degli aggiornamenti**.

Passaggio 2. Selezione dei dispositivi a cui assegnare l'attività

Selezionare i computer in cui verrà eseguita l'attività. Sono disponibili le seguenti opzioni:

- Assegnare l'attività a un gruppo di amministrazione. In questo caso l'attività viene assegnata a computer inclusi in un gruppo di amministrazione creato in precedenza.
- Selezionare i computer rilevati da Administration Server nella rete – *dispositivi non assegnati*. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco. È possibile specificare nomi NetBIOS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Passaggio 3. Configurazione di una pianificazione di avvio dell'attività

Ad esempio, configurare manualmente la pianificazione dell'attività.

Passaggio 4. Definizione del nome dell'attività

Immettere un nome per l'attività.

Passaggio 7. Completamento della creazione dell'attività

Terminare la procedura guidata. Se necessario, selezionare la casella di controllo **&Esegui l'attività al termine della procedura guidata**. È possibile monitorare lo stato di avanzamento dell'attività nelle proprietà dell'attività.

Esclusioni della telemetria EDR (KATA)

Per migliorare le prestazioni e ottimizzare la trasmissione dei dati al server di telemetria, è possibile configurare le esclusioni della telemetria. È ad esempio possibile scegliere di non inviare i dati sulle comunicazioni di rete per le singole applicazioni.

Come creare un'esclusione di telemetria in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.
4. Nel blocco **Impostazioni di telemetria** → **Telemetria EDR (KATA)/NDR (KATA)**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, configurare le esclusioni di telemetria (vedere la tabella di seguito).

   L'applicazione combina le condizioni di esclusione con l'operatore logico AND. Per creare una regola, è necessario specificare un valore nel campo **Percorso completo** e selezionare almeno un tipo di evento nell'elenco **Usa per i seguenti tipi di eventi**.
6. Salvare le modifiche.

Come creare un'esclusione di telemetria in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali → Impostazioni di telemetria**.

5. Selezionare la scheda **Telemetria EDR (KATA)/NDR (KATA)**.

6. Nella finestra visualizzata, configurare le esclusioni di telemetria (vedere la tabella di seguito).

   L'applicazione combina le condizioni di esclusione con l'operatore logico AND. Per creare una regola, è necessario specificare un valore nel campo **Percorso completo** e selezionare almeno un tipo di evento.

7. Salvare le modifiche.

Parametri di esclusione di telemetria

Parametro	Descrizione
Processi esclusi	**Ottimizza le dimensioni della telemetria da inviare**. Kaspersky Endpoint Security consente di ottimizzare la quantità di dati trasmessi ed escludere gli eventi con determinati codici dalla telemetria: codice 102 (comunicazioni di base) e 8 (attività di rete del processo) per il protocollo Microsoft SMB, il servizio WinRM e il processo klnagent.exe di Network Agent, nonché informazioni estese sui tipi di pacchetti di rete per tutti i tipi di protocolli di rete. Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico. **Processo** e **Processo entità superiore**: • **Percorso completo**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. • **Testo riga di comando**. Comando utilizzato per eseguire il file. • **Descrizione**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo). • **Nome file originale**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo). • **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo). • **Checksum file**. MD5 e SHA256. È anche possibile selezionare un file manualmente e l'applicazione compilerà automaticamente i campi del file selezionato. Nei sistemi operativi a 64 bit, è necessario immettere manualmente i parametri della versione a 64 bit del file eseguibile di un processo dalla cartella `C:\windows\system32` poiché l'applicazione compila i campi dei parametri del file eseguibile con i dati delle proprietà del file della versione a 32 bit dello stesso file eseguibile nella cartella `C:\windows\syswow64`. Ad esempio, se si seleziona `C:\windows\system32\cmd.exe`, il plug-in mostra i parametri di `C:\windows\syswow64\cmd.exe`. Tale comportamento è dettato dalle peculiarità del sistema operativo. **Usa per i seguenti tipi di eventi**: • **Modifica del file**. • **Eventi rete**. • **Processo: input interattivo nella console**. • **Modulo caricato**. • **Registro di sistema modificato**. • **Registri DNS**. • **Accesso ai processi**. • **Inoculazione di codice**. • **Query WMI**. • **Pipe**. • **LDAP**. • **AMSI**.

Parametro	Descrizione
Comunicazioni di rete escluse	**Nome regola**. **Direzione**. **Protocollo**. **Socket non elaborato**. **Numero di protocollo**. **Certificato TLS**. **Porta locale o intervallo**. **Porta remota o intervallo**. **Indirizzo locale**. L'indirizzo di rete del computer per cui Kaspersky Endpoint Security esclude la telemetria dal traffico di rete. **Indirizzo remoto**. L'indirizzo di rete del computer per cui Kaspersky Endpoint Security esclude la telemetria dal traffico di rete. Per gli indirizzi IP è supportato solo il formato IPv4. **Applicazioni**. Elenco dei file eseguibili delle applicazioni per cui Kaspersky Endpoint Security esclude la telemetria EDR dal traffico di rete.
Operazioni sui file escluse	**Nome regola**. **Nome file o maschera**. Nome o maschera di un file o di una cartella; Kaspersky Endpoint Security applica la regola di esclusione quando si accede a questo file o cartella. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce una maschera: **Tipo di operazione**. **Percorso precedente**. Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico. **Processo** e **Processo entità superiore**: • **Percorso completo**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. • **Testo riga di comando**. Comando utilizzato per eseguire il file. • **Descrizione**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo). • **Nome file originale**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo). • **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo). • **Checksum file**. MD5 e SHA256. È anche possibile selezionare un file manualmente e l'applicazione compilerà automaticamente i campi del file selezionato. Nei sistemi operativi a 64 bit, è necessario immettere manualmente i parametri della versione a 64 bit del file eseguibile di un processo dalla cartella `C:\windows\system32` poiché l'applicazione compila i campi dei parametri del file eseguibile con i dati delle proprietà del file della versione a 32 bit dello stesso file eseguibile nella cartella `C:\windows\syswow64`. Ad esempio, se si seleziona `C:\windows\system32\cmd.exe`, il plug-in mostra i parametri di `C:\windows\syswow64\cmd.exe`. Tale comportamento è dettato dalle peculiarità del sistema operativo.

Parametro	Descrizione
Operazioni DNS escluse	**Nome regola**. Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico. **Processo** e **Processo entità superiore**: • **Percorso completo**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. • **Testo riga di comando**. Comando utilizzato per eseguire il file. • **Descrizione**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo). • **Nome file originale**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo). • **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo). • **Checksum file**. MD5 e SHA256. È anche possibile selezionare un file manualmente e l'applicazione compilerà automaticamente i campi del file selezionato. Nei sistemi operativi a 64 bit, è necessario immettere manualmente i parametri della versione a 64 bit del file eseguibile di un processo dalla cartella `C:\windows\system32` poiché l'applicazione compila i campi dei parametri del file eseguibile con i dati delle proprietà del file della versione a 32 bit dello stesso file eseguibile nella cartella `C:\windows\syswow64`. Ad esempio, se si seleziona `C:\windows\system32\cmd.exe`, il plug-in mostra i parametri di `C:\windows\syswow64\cmd.exe`. Tale comportamento è dettato dalle peculiarità del sistema operativo. **DNS**: • **Indirizzo IP server DNS**. • **Opzioni query**. • **Stato**. • **Nome di dominio**. • **ID tipo impostazioni**. • **Dati risposta**.
Operazioni LDAP escluse	**Nome regola**. **Ambito di ricerca LDAP**. **Filtro**. **Nome distinto per la ricerca degli oggetti LDAP**. **Attributi degli oggetti**. Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico. **Processo** e **Processo entità superiore**: • **Percorso completo**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. • **Testo riga di comando**. Comando utilizzato per eseguire il file. • **Descrizione**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo). • **Nome file originale**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo). • **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo). • **Checksum file**. MD5 e SHA256. È anche possibile selezionare un file manualmente e l'applicazione compilerà automaticamente i campi del file selezionato. Nei sistemi operativi a 64 bit, è necessario immettere manualmente i parametri della versione a 64 bit del file eseguibile di un processo dalla cartella `C:\windows\system32` poiché l'applicazione compila i campi dei parametri del file eseguibile con i dati delle proprietà del file della versione a 32 bit dello stesso file eseguibile nella cartella `C:\windows\syswow64`. Ad esempio, se si seleziona `C:\windows\system32\cmd.exe`, il plug-in mostra i parametri di `C:\windows\syswow64\cmd.exe`. Tale comportamento è dettato dalle peculiarità del sistema operativo.

Parametro	Descrizione
Query di accesso al processo escluse	**Nome regola**. **Tipo di operazione**. **Accesso richiesto al processo**. **Traccia stack di chiamate**. Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico. **Processo**, **Processo entità superiore**, **File del processo di destinazione**, **Handle del processo di origine** e **Gestire il processo di destinazione**. • **Percorso completo**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. • **Testo riga di comando**. Comando utilizzato per eseguire il file. • **Specificare i criteri di attivazione della regola e i tipi di eventi per cui utilizzare questa regola**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo). • **Nome file originale**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo). • **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo). • **Checksum file**. MD5 e SHA256. È anche possibile selezionare un file manualmente e l'applicazione compilerà automaticamente i campi del file selezionato. Nei sistemi operativi a 64 bit, è necessario immettere manualmente i parametri della versione a 64 bit del file eseguibile di un processo dalla cartella `C:\windows\system32` poiché l'applicazione compila i campi dei parametri del file eseguibile con i dati delle proprietà del file della versione a 32 bit dello stesso file eseguibile nella cartella `C:\windows\syswow64`. Ad esempio, se si seleziona `C:\windows\system32\cmd.exe`, il plug-in mostra i parametri di `C:\windows\syswow64\cmd.exe`. Tale comportamento è dettato dalle peculiarità del sistema operativo.
Inoculazioni di codice escluse	**Nome regola**. **Metodo di accesso**. **Stack di chiamate**. **Riga di comando modificata**. **Indirizzo inoculazione**. **Nome DLL inoculato**. Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico. **Processo** e **Processo entità superiore**: • **Percorso completo**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. • **Testo riga di comando**. Comando utilizzato per eseguire il file. • **Descrizione**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo). • **Nome file originale**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo). • **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo). • **Checksum file**. MD5 e SHA256. È anche possibile selezionare un file manualmente e l'applicazione compilerà automaticamente i campi del file selezionato. Nei sistemi operativi a 64 bit, è necessario immettere manualmente i parametri della versione a 64 bit del file eseguibile di un processo dalla cartella `C:\windows\system32` poiché l'applicazione compila i campi dei parametri del file eseguibile con i dati delle proprietà del file della versione a 32 bit dello stesso file eseguibile nella cartella `C:\windows\syswow64`. Ad esempio, se si seleziona `C:\windows\system32\cmd.exe`, il plug-in mostra i parametri di `C:\windows\syswow64\cmd.exe`. Tale comportamento è dettato dalle peculiarità del sistema operativo.

Parametro	Descrizione
Query WMI escluse	**Nome regola**. **Tipo di operazione WMI**. **Query remota**. **Nome di un computer che ha eseguito un comando WMI**. **Account utente WMI**. **Comando WMI eseguito**. **Spazio dei nomi WMI**. **Filtro consumer eventi WMI**. **Nome del consumer di eventi WMI creato**. **Codice sorgente di un consumer di eventi WMI**. Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico. **Processo** e **Processo entità superiore**: • **Percorso completo**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. • **Testo riga di comando**. Comando utilizzato per eseguire il file. • **Descrizione**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo). • **Nome file originale**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo). • **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo). • **Checksum file**. MD5 e SHA256. È anche possibile selezionare un file manualmente e l'applicazione compilerà automaticamente i campi del file selezionato. Nei sistemi operativi a 64 bit, è necessario immettere manualmente i parametri della versione a 64 bit del file eseguibile di un processo dalla cartella `C:\windows\system32` poiché l'applicazione compila i campi dei parametri del file eseguibile con i dati delle proprietà del file della versione a 32 bit dello stesso file eseguibile nella cartella `C:\windows\syswow64`. Ad esempio, se si seleziona `C:\windows\system32\cmd.exe`, il plug-in mostra i parametri di `C:\windows\syswow64\cmd.exe`. Tale comportamento è dettato dalle peculiarità del sistema operativo.
Operazioni pipe escluse	**Nome regola**. **Nome pipe**. **Tipo di operazione**. Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico. **Processo** e **Processo entità superiore**: • **Percorso completo**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. • **Testo riga di comando**. Comando utilizzato per eseguire il file. • **Descrizione**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo). • **Nome file originale**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo). • **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo). • **Checksum file**. MD5 e SHA256. È anche possibile selezionare un file manualmente e l'applicazione compilerà automaticamente i campi del file selezionato. Nei sistemi operativi a 64 bit, è necessario immettere manualmente i parametri della versione a 64 bit del file eseguibile di un processo dalla cartella `C:\windows\system32` poiché l'applicazione compila i campi dei parametri del file eseguibile con i dati delle proprietà del file della versione a 32 bit dello stesso file eseguibile nella cartella `C:\windows\syswow64`. Ad esempio, se si seleziona `C:\windows\system32\cmd.exe`, il plug-in mostra i parametri di `C:\windows\syswow64\cmd.exe`. Tale comportamento è dettato dalle peculiarità del sistema operativo.

Parametro	Descrizione
Modifiche al Registro di sistema escluse	**Nome regola**. **Tipo di operazione**. **Percorso**. **Nome valore**. **Valore**. **Nome completo di un file del Registro di sistema**. Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico. **Processo** e **Processo entità superiore**: • **Percorso completo**. Percorso completo del file, inclusi il nome e l'estensione. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. • **Testo riga di comando**. Comando utilizzato per eseguire il file. • **Descrizione**. Valore del parametro FileDescription da una risorsa RT_VERSION (VersionInfo). • **Nome file originale**. Valore del parametro OriginalFilename da una risorsa RT_VERSION (VersionInfo). • **Versione**. Valore del parametro FileVersion da una risorsa RT_VERSION (VersionInfo). • **Checksum file**. MD5 e SHA256. È anche possibile selezionare un file manualmente e l'applicazione compilerà automaticamente i campi del file selezionato. Nei sistemi operativi a 64 bit, è necessario immettere manualmente i parametri della versione a 64 bit del file eseguibile di un processo dalla cartella `C:\windows\system32` poiché l'applicazione compila i campi dei parametri del file eseguibile con i dati delle proprietà del file della versione a 32 bit dello stesso file eseguibile nella cartella `C:\windows\syswow64`. Ad esempio, se si seleziona `C:\windows\system32\cmd.exe`, il plug-in mostra i parametri di `C:\windows\syswow64\cmd.exe`. Tale comportamento è dettato dalle peculiarità del sistema operativo.
Operazioni escluse con i dispositivi	**Nome regola**. **Tipo di dispositivo**. **ID dispositivo**. **Nome dispositivo**.

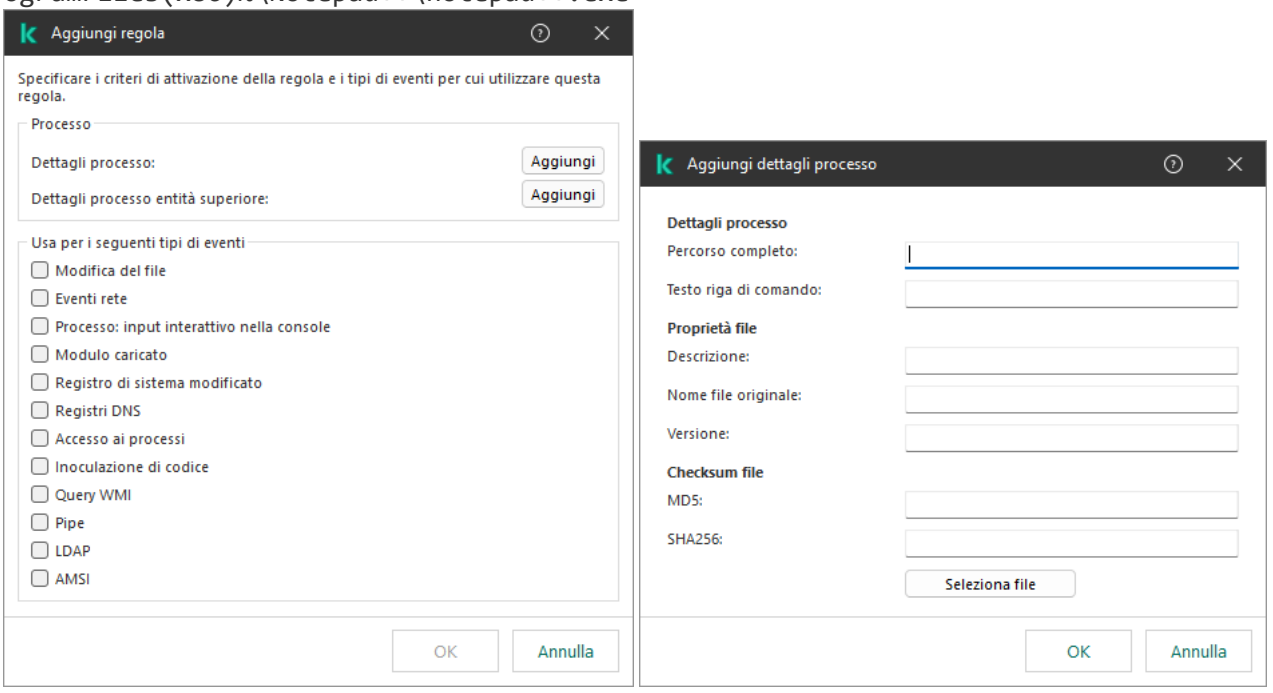
Esempio 1. Processi esclusi

Per escludere gli eventi di applicazioni (processo) di terze parti dalla telemetria, aprire la finestra Esclusioni della telemetria EDR nella scheda **Processi esclusi** e aggiungere il file eseguibile dell'applicazione.

Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico.

Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. Ad esempio:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Esclusione di un processo

Esempio 1. Modifica ai file

Se si modificano spesso gli script nell'applicazione Notepad++ e si desidera escludere gli eventi di modifica per gli script corrispondenti, aggiungere il file eseguibile Notepad++ alle esclusioni di telemetria.

Specificare le impostazioni come segue:

- **Percorso completo**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Usa per i seguenti tipi di eventi**: Modifica del file.

Esempio 2. Eventi di rete

Se si utilizza l'applicazione WinSCP per gestire i file in un server remoto e si desidera escludere eventi di rete, aggiungere il file eseguibile WinSCP alle esclusioni di telemetria.

Specificare le impostazioni come segue:

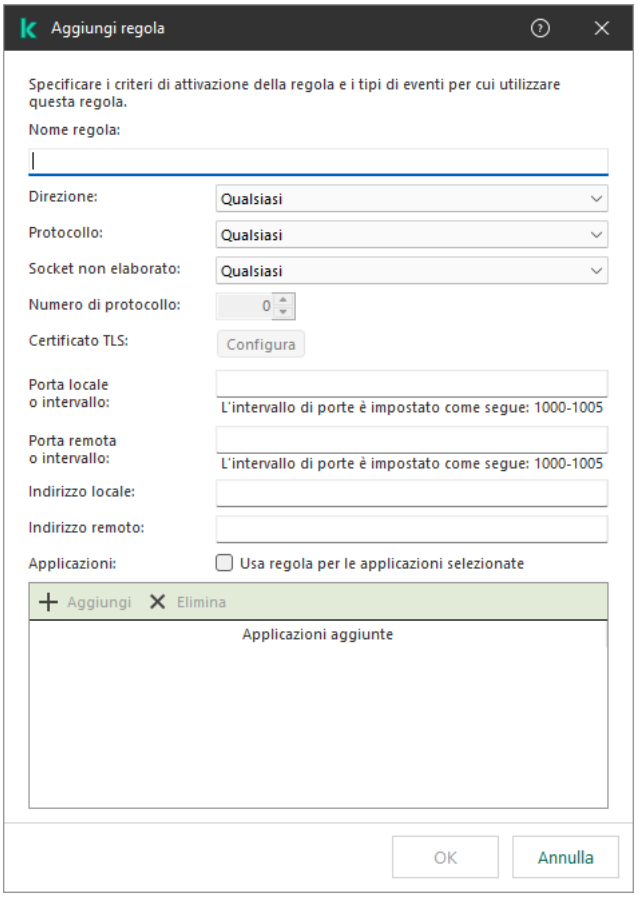
- **Percorso completo**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (optional).
- **Usa per i seguenti tipi di eventi**: Eventi rete.

Esempio 2. Comunicazioni di rete escluse

Per escludere gli eventi di connessione al servizio remoto dalla telemetria, aprire la finestra Esclusioni della telemetria EDR nella scheda **Comunicazioni di rete escluse** e aggiungere le impostazioni di connessione: protocollo, porta, direzione, indirizzo IP, certificato TLS e altro.

Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico.

Non è possibile specificare un indirizzo di subnet (ad esempio 10.28.0.0/24). L'applicazione consente di specificare un solo indirizzo IP (ad esempio 10.28.0.105).



Esclusione della comunicazione di rete

Se si utilizza un server Web aziendale e si desidera escludere gli eventi del browser durante la connessione a tale server Web, aggiungere l'indirizzo IP del server e il file eseguibile del browser alle esclusioni di telemetria.

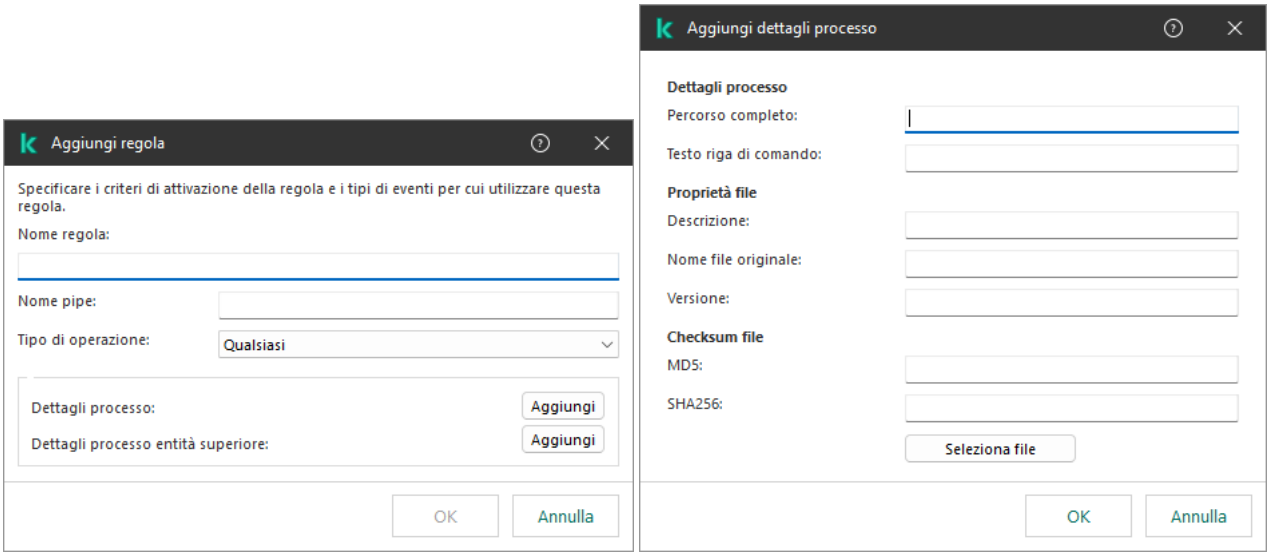
Specificare le impostazioni come segue:

- **Protocollo**: TCP.
- **Porta remota o intervallo**: 443.
- **Indirizzo remoto**: 10.28.0.105.
- **Applicazioni**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Esempio 3. Operazioni sui file escluse

Per escludere dalla telemetria gli eventi che implicano operazioni con file attendibili, aprire la finestra Esclusioni della telemetria EDR nella scheda **Operazioni sui file escluse** e aggiungere il file attendibile.

Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico.



Esclusione delle operazioni sui file

Se un'applicazione scrive in un registro e si desidera escludere gli eventi di modifica del file di registro, aggiungere il file di registro e il file eseguibile dell'applicazione dalla telemetria.

Specificare le impostazioni come segue:

- **Nome file o maschera**: `C:\Apache24\logs\error.log`.
- **Tipo di operazione**: Modifica dei file.
- **Percorso completo**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Esempio 4. Modifiche al Registro di sistema escluse

Per escludere gli eventi di modifica del registro di sistema dalla telemetria, aprire la finestra Esclusioni della telemetria EDR nella scheda **Modifiche al Registro di sistema escluse** e aggiungere una chiave del registro di sistema.

Kaspersky Endpoint Security combina i criteri di attivazione delle regole con un AND logico.

Se un'applicazione modifica frequentemente i propri valori del registro di sistema e si desidera escludere questi eventi di modifica del registro di sistema dalla telemetria, aggiungere la chiave del registro di sistema e il file eseguibile dell'applicazione alle esclusioni di telemetria.

Specificare le impostazioni come segue:

- **Tipo di operazione**: Modifica.
- **Percorso**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Percorso completo**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform include il componente Sandbox (KATA Sandbox). *Sandbox* è una tecnologia che consente di rilevare le minacce avanzate in un computer. Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Sandbox). Per informazioni dettagliate sulla soluzione, consultare la Guida di Kaspersky Anti Targeted Attack Platform.

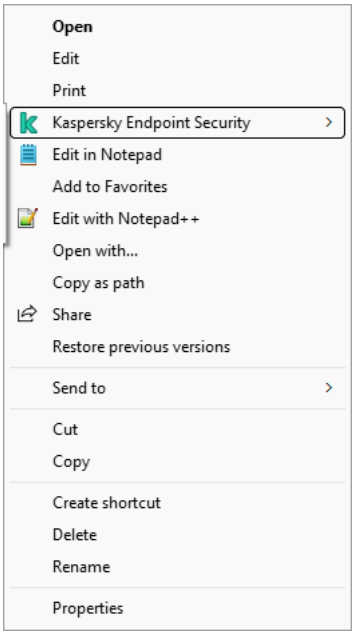
Per attivare KATA Sandbox, è necessaria una chiave di licenza che includa funzionalità KATA o KEDR. Per ulteriori dettagli sulle funzionalità disponibili, consultare la Guida di Kaspersky Anti Targeted Attack Platform.

KATA Sandbox consente di eseguire la scansione dei file nelle seguenti modalità:

- *Manualmente*. L'utente invia manualmente il file per la scansione dal menu di scelta rapida (**Invia a Sandbox**). Quando si invia un file a Sandbox, l'applicazione esegue la scansione del file utilizzando i database anti-virus.
- *Automaticamente*. L'applicazione rileva automaticamente gli oggetti e li invia a Sandbox per la scansione.

Dopo l'invio del file a Sandbox, il file rimane accessibile per l'utente. Kaspersky Endpoint Security registra l'evento corrispondente e invia l'evento a Kaspersky Security Center e alla console Kaspersky Anti Targeted Attack Platform. Se Sandbox rileva attività dannose, Kaspersky Endpoint Security esegue automaticamente un'azione di risposta alle minacce (ad esempio, elimina l'oggetto e avvia un'attività Scansione delle Aree Critiche).

Per il funzionamento di KATA Sandbox in modalità manuale, è necessario distribuire Kaspersky Anti Targeted Attack Platform 7.0 o versioni successive. Per il funzionamento di KATA Sandbox in modalità automatica, è necessario distribuire Kaspersky Anti Targeted Attack Platform 8.0 o versioni successive.



Scansione in KATA Sandbox dal menu di scelta rapida

Integrazione dell'agente integrato con KATA Sandbox

L'aggiunta del componente Sandbox è necessaria per l'integrazione con il componente KATA Sandbox. È possibile selezionare il componente Sandbox durante l'installazione o l'upgrade, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

Per inviare i file per la scansione, è necessario abilitare l'integrazione con KATA Sandbox e aggiungere un server Central Node distribuito all'interno della soluzione. Il componente può essere gestito solo utilizzando Kaspersky Security Center Web Console. Non è possibile gestire questo componente tramite Administration Console (MMC).

Per abilitare e disabilitare l'integrazione con KATA Sandbox:

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Sandbox**.
5. Utilizzare l'interruttore **Integrazione con Sandbox ABILITATA** per abilitare o disabilitare il componente.

6. Selezionare la modalità operativa KATA Sandbox:

   - **Manualmente**. L'utente invia manualmente il file per la scansione dal menu di scelta rapida (**Invia a Sandbox**).
   - **Automaticamente**. L'applicazione rileva automaticamente gli oggetti e li invia a Sandbox per la scansione.
   - **Combinato**.

7. Fare clic sul collegamento **Impostazioni di connessione**.

8. Configurare le impostazioni di connessione al server di Central Node:

   - **Timeout (msec)**. Timeout della connessione per il server Central Node. Allo scadere del timeout configurato, Kaspersky Endpoint Security invia una richiesta al server successivo. È possibile aumentare il timeout della connessione per il server se la velocità di connessione è lenta o se la connessione è instabile. Il timeout della richiesta consigliato è di 0,5 secondi o meno.
   - **Coda richieste**. Dimensione della cartella della coda di richieste. Quando si inviano più oggetti per la scansione in Sandbox, Kaspersky Endpoint Security crea una coda di richieste. Per impostazione predefinita, la dimensione della cartella della coda di richieste è limitata a 100 MB. Una volta raggiunta la dimensione massima, Sandbox interrompe l'aggiunta di nuove richieste alla coda e invia l'evento corrispondente a Kaspersky Security Center. È possibile configurare la dimensione della cartella della coda delle richieste in base alla configurazione del server.
   - **Certificato TLS del server**. Per configurare una connessione attendibile con il server Central Node, è necessario preparare un certificato TLS. È quindi necessario aggiungere il certificato nel computer utilizzando un criterio. È inoltre necessario aggiungere il certificato al server Central Node.
   - **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

9. Nel blocco **Connessione ai server Sandbox**, fare clic sul pulsante **Aggiungi**.

10. Si apre una finestra; nella finestra, immettere l'indirizzo e la porta del server di Central Node (IPv4, IPv6, DNS).

    Per ulteriori dettagli sulla distribuzione di immagini virtuali e sulla configurazione dei server di Central Node, consultare la Guida di Kaspersky Anti Targeted Attack Platform.

11. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

A questo punto, il componente Sandbox è abilitato. Controllare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Sandbox** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

Configurazione delle azioni di risposta alle minacce

Se Sandbox rileva attività dannose, Kaspersky Endpoint Security esegue automaticamente un'azione di risposta alle minacce (ad esempio, elimina l'oggetto e avvia un'attività Scansione delle Aree Critiche).

Per configurare le azioni di risposta alle minacce:

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Sandbox**.
5. Selezionare l'azione attinente nella sezione **Azione se viene rilevata una minaccia**:

   - **Sposta la copia in Quarantena, elimina oggetto**. Se questa opzione è selezionata, Kaspersky Endpoint Security elimina l'oggetto dannoso trovato nel computer. Prima di eliminare l'oggetto, Kaspersky Endpoint Security crea una copia di backup nel caso in cui sia necessario ripristinare l'oggetto in un secondo momento. Kaspersky Endpoint Security sposta la copia di backup in Quarantena.
   - **Esegui scansione delle aree critiche**. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue l'attività *Scansione delle aree critiche*. Per impostazione predefinita, Kaspersky Endpoint Security esamina la memoria del kernel, i processi in esecuzione e i settori di avvio del disco.
   - **Crea attività di scansione IOC**. Se questa opzione è selezionata, Kaspersky Endpoint Security crea automaticamente l'attività *Scansione IOC (attività di scansione IOC autonoma)*. Per questa attività, è possibile configurare la modalità di esecuzione, l'ambito della scansione e l'azione al rilevamento IOC (*Sposta la copia in Quarantena, elimina oggetto* o *Esegui scansione delle aree critiche*). Per modificare altre impostazioni dell'attività di *Scansione IOC*, passare alle impostazioni dell'attività.
6. Se necessario, configurare le impostazioni dell'attività *Scansione IOC* nel blocco **Ambito della scansione IOC**.

   - **Aree dei file critiche**. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue una scansione IOC solo nelle aree dei file critiche del computer: memoria del kernel e settori di avvio.
   - **Aree dei file nell'unità di sistema del computer**. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue una scansione IOC sull'unità di sistema del computer.
7. Se necessario, configurare le impostazioni dell'attività *Scansione IOC* nel blocco **Esegui attività di scansione IOC**.

   - **Manualmente**. Modalità di esecuzione in cui è possibile avviare l'attività *Scansione IOC* manualmente nel momento più opportuno.
   - **Automaticamente**. Modalità di esecuzione in cui Kaspersky Endpoint Security esegue automaticamente l'attività di *Scansione IOC* dopo il rilevamento di una minaccia.
   - **Esegui solo quando il computer è inattivo**. Modalità di esecuzione in cui Kaspersky Endpoint Security esegue l'attività di *Scansione IOC* se lo screensaver è attivo o lo schermo è bloccato. Se l'utente sblocca il computer, Kaspersky Endpoint Security sospende l'attività. Ciò significa che il completamento dell'attività può richiedere diversi giorni.
8. Configurare le impostazioni avanzate delle attività per *Scansione IOC*.
9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Guida alla migrazione da KEA a KES per EDR (KATA)

A partire dalla versione 12.1, Kaspersky Endpoint Security for Windows include un agente integrato per la gestione del componente Kaspersky Endpoint Detection and Response come parte della soluzione Kaspersky Anti Targeted Attack Platform. Non è più necessaria un'applicazione Kaspersky Endpoint Agent separata per utilizzare EDR (KATA). Tutte le funzioni di Kaspersky Endpoint Agent verranno eseguite da Kaspersky Endpoint Security. Il carico sui server di Kaspersky Anti Targeted Attack Platform rimarrà lo stesso.

Quando si distribuisce Kaspersky Endpoint Security nei computer in cui è installato Kaspersky Endpoint Agent, la soluzione Kaspersky Anti Targeted Attack Platform (EDR) continuerà a funzionare con Kaspersky Endpoint Security. Inoltre, Kaspersky Endpoint Agent verrà rimosso dal computer. Lo stesso comportamento nel sistema si verificherà quando si aggiorna Kaspersky Endpoint Security alla versione 12.1 o successiva.

Kaspersky Endpoint Security non è compatibile con Kaspersky Endpoint Agent. Non è possibile installare entrambe queste applicazioni nello stesso computer.

Le seguenti condizioni devono essere soddisfatte affinché Kaspersky Endpoint Security funzioni come parte di Endpoint Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform versione 5.0 o successiva.
- Kaspersky Security Center versione 14.2 o successiva (incluso Network Agent). Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità Endpoint Detection and Response (KATA).

Passaggi per la migrazione della configurazione [KES+KEA] a [KES+agente integrato] per EDR (KATA)

1. **Upgrade del plug-in di gestione di Kaspersky Endpoint Security**

   Il componente EDR (KATA) può essere gestito utilizzando il plug-in di gestione di Kaspersky Endpoint Security versione 12.1 o successiva. A seconda del tipo di console di Kaspersky Security Center in uso, aggiornare il plug-in di gestione in Administration Console (MMC) o il plug-in Web in Web Console.

2. **Migrazione di criteri e attività**

   Trasferire le impostazioni di Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows. Sono disponibili le seguenti opzioni:

   - Una migrazione guidata da Kaspersky Endpoint Agent a Kaspersky Endpoint Security. Una migrazione guidata da Kaspersky Endpoint Agent a Kaspersky Endpoint Security funziona solo in Web Console

     Come eseguire la migrazione delle impostazioni di criteri e attività da Kaspersky Endpoint Agent a Kaspersky Endpoint Security in Web Console

     Nella finestra principale di Web Console, fare clic su **Operazioni** → **Migrazione da Kaspersky Endpoint Agent**.

     Viene eseguita la migrazione guidata di criteri e attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Migrazione dei criteri

La migrazione guidata crea un nuovo criterio che unisce le impostazioni dei criteri di Kaspersky Endpoint Security e Kaspersky Endpoint Agent. Nell'elenco dei criteri, selezionare i criteri di Kaspersky Endpoint Agent di cui si desidera unire le impostazioni con il criterio di Kaspersky Endpoint Security. Fare clic sul criterio di Kaspersky Endpoint Agent per selezionare il criterio di Kaspersky Endpoint Security con cui unire le impostazioni. Verificare di aver selezionato i criteri corretti, quindi procedere con il passaggio successivo.

Passaggio 2. Migrazione delle attività

La migrazione guidata non supporta le attività di EDR (KATA). Ignorare questo passaggio.

Passaggio 3. Completamento della procedura guidata

Terminare la procedura guidata. Come risultato della procedura guidata, verrà creato un nuovo criterio di Kaspersky Endpoint Security. Il criterio unisce le impostazioni da Kaspersky Endpoint Security e Kaspersky Endpoint Agent Il criterio è denominato *<Nome del criterio di Kaspersky Endpoint Security> e <Nome del criterio di Kaspersky Endpoint Agent>*. Il nuovo criterio presenta lo stato *Inattivo*. Per continuare, modificare gli stati dei criteri di Kaspersky Endpoint Agent e Kaspersky Endpoint Security in *Inattivo* e attivare il nuovo criterio unito.

Questa migrazione guidata in Web Console ignora le seguenti impostazioni dei criteri e non le migra:

- Divieto di modifica delle impostazioni **Impostazioni di connessione** ("lucchetto").

  Per impostazione predefinita, le impostazioni possono essere modificate (il "lucchetto" è aperto). Pertanto, le impostazioni non vengono applicate al computer. È necessario vietare la modifica delle impostazioni e chiudere il "lucchetto".

- Contenitore crittografico.

  Se si utilizza l'autenticazione a due vie per la connessione ai server di Central Node, è necessario aggiungere di nuovo il contenitore crittografico.

Poiché la migrazione guidata non esegue la migrazione di queste impostazioni, è possibile che si verifichino errori durante la connessione del computer ai server di Central Node. Per correggere gli errori, è necessario accedere alle proprietà del criterio e configurare le impostazioni di connessione.

- Una Conversione guidata di criteri e attività in batch standard. La Conversione guidata di criteri e attività in batch è disponibile solo in Administration Console (MMC). Per ulteriori dettagli su Conversione guidata di criteri e attività in batch, consultare la Guida di Kaspersky Security Center.

Per assicurarsi che Kaspersky Endpoint Security funzioni correttamente sui server, si consiglia di aggiungere i file importanti per il funzionamento del server all'area attendibile. Per i server SQL, è necessario aggiungere file di database MDF e LDF. Per i server Microsoft Exchange, è necessario aggiungere i file CHK, EDB, JRS, LOG e JSL. È possibile utilizzare anche maschere, ad esempio, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A partire da Kaspersky Endpoint Security 12.6 for Windows, le esclusioni dalle scansioni e le applicazioni attendibili vengono aggiunte all'area attendibile. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server.

Le esclusioni della telemetria EDR non vengono migrate dal criterio di Kaspersky Endpoint Agent al criterio di Kaspersky Endpoint Security. Kaspersky Endpoint Security dispone dei propri strumenti di esclusione: le applicazioni attendibili. Il funzionamento di Kaspersky Endpoint Security è ottimizzato in modo che l'assenza di singole esclusioni della telemetria EDR non provochi alcun carico aggiuntivo sul computer rispetto a Kaspersky Endpoint Agent. Kaspersky Endpoint Security utilizza la telemetria non solo per EDR (KATA), ma anche per il funzionamento dei componenti di protezione delle applicazioni. Pertanto, non è necessario trasferire singole esclusioni della telemetria EDR. Se si riscontra una diminuzione delle prestazioni del computer, verificare il funzionamento dell'applicazione (vedere il passaggio 7 Controllo delle prestazioni).

3. **Licenza della funzionalità EDR (KATA)**

   Per attivare Kaspersky Endpoint Security come parte della soluzione Kaspersky Anti Targeted Attack Platform, è necessaria una licenza separata per il componente aggiuntivo Kaspersky Endpoint Detection and Response (KATA). È possibile aggiungere la chiave tramite l'attività *Aggiungi chiave*. Di conseguenza, verranno aggiunte due chiavi all'applicazione: *Kaspersky Endpoint Security* e *Kaspersky Endpoint Detection and Response (KATA)*.

   La concessione di una licenza del componente aggiuntivo Kaspersky Endpoint Detection and Response (KATA) nel computer con funzionalità EDR Optimum o EDR Expert precedentemente attivate comporta le seguenti considerazioni speciali:

   - Se si sta utilizzando un *file chiave* per la licenza di Kaspersky Endpoint Security con le funzionalità EDR Optimum o EDR Expert, non è possibile aggiungere una chiave separata per il componente aggiuntivo Kaspersky Endpoint Detection and Response (KATA). È possibile passare all'utilizzo di un codice di attivazione per la licenza oppure contattare il provider di servizi per ottenere un nuovo file chiave per l'attivazione delle funzionalità di Kaspersky Endpoint Security ed EDR. Il provider di servizi fornirà uno o più file chiave per la licenza.

   - Se si sta utilizzando un *file chiave* per la licenza di Kaspersky Endpoint Security senza le funzionalità EDR Optimum o EDR Expert, è possibile aggiungere una chiave separata per il componente aggiuntivo Kaspersky Endpoint Detection and Response (KATA) senza un nuovo rilascio dei file chiave.

   - Se si sta utilizzando un *codice di attivazione* per la licenza, il server di attivazione di Kaspersky rilascerà automaticamente le chiavi e le funzionalità EDR (KATA) diventeranno automaticamente disponibili. In questo caso, EDR Optimum ed EDR Expert saranno disabilitati.

   - Kaspersky Endpoint Security consente di aggiungere fino a due chiavi attive: chiave di Kaspersky Endpoint Security e chiave del tipo di componente aggiuntivo. È possibile aggiungere inoltre fino a due chiavi di riserva. Una chiave di riserva di Kaspersky Endpoint Security e una chiave di riserva del tipo Componente aggiuntivo.

4. **Installazione/upgrade dell'applicazione Kaspersky Endpoint Security**

   Per migrare la funzionalità EDR (KATA) durante l'installazione o l'upgrade di un'applicazione, si consiglia di utilizzare l'attività di installazione remota. Quando si crea un'attività di installazione remota, è necessario selezionare il componente EDR (KATA) nelle impostazioni del pacchetto di installazione.

   È inoltre possibile eseguire l'applicazione con i seguenti metodi:

   - Tramite il servizio di aggiornamento di Kaspersky.

   - In locale, utilizzando l'Installazione guidata.

Kaspersky Endpoint Security supporta la selezione automatica dei componenti quando si effettua l'upgrade dell'applicazione in un computer con l'applicazione Kaspersky Endpoint Agent installata. La selezione automatica dei componenti dipende dalle autorizzazioni dell'account utente che sta effettuando l'upgrade dell'applicazione.

Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando il file EXE o MSI nell'account di sistema (SYSTEM), Kaspersky Endpoint Security ottiene l'accesso alle licenze correnti delle soluzioni Kaspersky. Pertanto, se nel computer è installato Kaspersky Endpoint Agent e la soluzione EDR (KATA) è attivata, il programma di installazione di Kaspersky Endpoint Security configura automaticamente il set di componenti e seleziona il componente EDR (KATA). In questo modo, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent. L'esecuzione del programma di installazione MSI nell'account di sistema (SYSTEM) viene in genere eseguita quando si effettua l'upgrade tramite Kaspersky Update Service o quando si distribuisce un pacchetto di installazione tramite Kaspersky Security Center.

Se si effettua l'upgrade di Kaspersky Endpoint Security utilizzando un file MSI in un account utente senza privilegi, Kaspersky Endpoint Security non sarà in grado di accedere alle licenze correnti delle soluzioni Kaspersky. In questo caso, Kaspersky Endpoint Security seleziona automaticamente i componenti in base a un set di componenti di Kaspersky Endpoint Agent. A questo punto, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent.

Kaspersky Endpoint Security supporta l'upgrade senza riavviare il computer. È possibile selezionare la modalità di upgrade dell'applicazione nelle proprietà dei criteri.

5 Verifica del funzionamento dell'applicazione

Se dopo l'installazione o l'upgrade il computer presenta lo stato *Critico* nella console di Kaspersky Security Center:

- Accertarsi che nel computer sia installato Network Agent versione 13.2 o successiva.
- Controllare lo stato operativo dell'agente integrato visualizzando *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non installato*, installare il componente tramite l'attività *Modifica i componenti dell'applicazione*. Se un componente presenta lo stato *Non incluso nella licenza*, verificare di aver attivato la funzionalità dell'agente integrata.
- Accertarsi di accettare l'Informativa di Kaspersky Security Network nel nuovo criterio di Kaspersky Endpoint Security for Windows.

6 Verifica della connessione al server di Kaspersky Anti Targeted Attack Platform

Verificare la connessione al server di Kaspersky Anti Targeted Attack Platform. A tale scopo:

1. Verificare di disporre di un certificato valido.
2. Verificare le impostazioni di connessione al server.
3. Verificare il registro degli eventi.

   Se viene stabilita una connessione al server, l'applicazione invia l'evento *Connessione al server di EDR Expert riuscita*. Se non si verificano eventi di connessione riusciti e non sono presenti eventi con errori di connessione, verificare le impostazioni del registro degli eventi e abilitare l'invio di eventi per Endpoint Detection and Response (KATA).

Lo stato della connessione al server non influisce sullo stato del computer nella console di Kaspersky Security Center. Pertanto, se non è presente alcuna connessione al server, il computer può comunque presentare lo stato *OK*. Verificare il registro degli eventi per controllare la connessione al server.

7 Verifica delle prestazioni

Se le prestazioni del computer sono rallentate dopo l'installazione o l'aggiornamento di un'applicazione, è possibile ottimizzare il trasferimento dei dati. A tale scopo:

1. Disabilitare il componente EDR (KATA) e verificare che il deterioramento delle prestazioni sia dovuto all'EDR (KATA).
2. Per applicazioni attendibili, disattivare la raccolta dei dati di telemetria nelle operazioni di input della console (abilitata per impostazione predefinita).
3. Aggiungere applicazioni che riducono le prestazioni del computer all'elenco di applicazioni attendibili.
4. Contattare l'Assistenza tecnica di Kaspersky. Gli esperti dell'assistenza aiuteranno l'utente a configurare il filtraggio della telemetria in Kaspersky Anti Targeted Attack Platform. Questo ridurrà la quantità di traffico. Se le prestazioni del computer sono influenzate da una determinata applicazione, allegare alla richiesta il pacchetto di distribuzione di tale applicazione.

Endpoint Detection and Response Expert (on-premises)



Kaspersky Endpoint Security for Windows supporta l'integrazione con la soluzione Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* è una soluzione di sicurezza informatica aziendale che include le applicazioni Kaspersky che consentono a un'organizzazione di difendersi dalla maggior parte dei tipi di rischi informatici e coprire i più importanti scenari di propagazione delle minacce. I componenti di EDR Expert (on-premises) vengono distribuiti in Open Single Management Platform (OSMP). Questa piattaforma esegue scenari multipiattaforma in un'unica interfaccia e consente di integrare le applicazioni Kaspersky con applicazioni di terze parti in un sistema di protezione completo.

Uno degli elementi centrali della soluzione è *SIEM*. SIEM monitora gli eventi provenienti da tutti i componenti e correla questi eventi tra loro utilizzando regole definite dal fornitore e dall'utente. EDR Expert (on-premises) esamina i registri e la telemetria ricevuti dall'infrastruttura aziendale per rilevare automaticamente gli attacchi e consente di indagare sugli incidenti utilizzando un grafico di indagine unificato che combina tutti gli eventi raccolti in EDR Expert (on-premises), inclusi gli eventi delle applicazioni Kaspersky e prodotti di terze parti per la sicurezza delle informazioni.

Per la risposta a incidenti avanzati, EDR Expert (on-premises) utilizza scenari preimpostati e definiti dall'utente. È inoltre possibile utilizzare le azioni di reazione di applicazioni di terze parti e gli scenari di reazione che coinvolgono più applicazioni.

Strumenti di threat intelligence

Kaspersky Endpoint Detection and Response utilizza i seguenti strumenti Threat Intelligence:

- Integrazione con Kaspersky Threat Intelligence Portal, che contiene e mostra informazioni sulla reputazione di file e indirizzi Web.
- Database delle minacce di Kaspersky.
- L'infrastruttura di servizi cloud di Kaspersky Security Network (di seguito denominata anche "KSN"), che fornisce accesso ai file in tempo reale, siti Web e informazioni sulla reputazione del software dalla knowledge base di Kaspersky. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce risposte più rapide da parte delle applicazioni Kaspersky alle minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi positivi.

Principio di funzionamento della soluzione

L'applicazione Kaspersky Endpoint Security viene installata nei singoli computer dell'infrastruttura IT aziendale e monitora continuamente i processi, le connessioni di rete aperte e i file modificati.

Se installato in modalità standard nell'infrastruttura VDI, Kaspersky Endpoint Security supporta l'integrazione con EDR Expert (on-premises). Tuttavia, l'operabilità delle altre funzionalità dell'applicazione non è garantita. Per proteggere le macchine virtuali nell'infrastruttura VDI, è consigliabile utilizzare Kaspersky Endpoint Security in modalità Light Agent.

Le informazioni sugli eventi nel computer (telemetria) vengono inviate al server di EDR Expert (on-premises). In questo caso, Kaspersky Endpoint Security invia anche informazioni sulle minacce rilevate dall'applicazione, nonché informazioni sull'elaborazione dei risultati di tali minacce ai server di raccolta della telemetria.

L'integrazione di EDR Expert (on-premises) è configurata nella console di Kaspersky Security Center. L'agente integrato viene quindi gestito tramite Open Single Management Platform (OSMP), inclusa l'esecuzione delle attività, la gestione degli oggetti in quarantena, la visualizzazione dei rapporti e altre azioni.

Configurazioni di Kaspersky Endpoint Security per l'utilizzo con EDR Expert (on-premises)

Per l'utilizzo con EDR Expert (on-premises), è possibile utilizzare le seguenti configurazioni:

- **[KES+agente integrato]**. In questa configurazione, Kaspersky Endpoint Security funge sia da applicazione che garantisce la sicurezza del computer sia da applicazione per l'utilizzo con EDR Expert (on-premises). L'agente integrato per EDR Expert (on-premises) è disponibile in Kaspersky Endpoint Security 12.11 for Windows o versioni successive.
- **[EPP di terzi+EDR Agent]**. In questa configurazione, la sicurezza dell'infrastruttura IT è garantita da Endpoint Protection Platform (EPP) di terze parti. L'interazione con EDR Expert (on-premises) è fornita da Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent (EDR Agent). In questa configurazione, EDR Agent è compatibile con le applicazioni PPE di terzi. EDR Agent per EDR Expert (on-premises) è disponibile in Kaspersky Endpoint Security 12.11 for Windows o versioni successive.

Integrazione dell'agente integrato con EDR Expert (on-premises)

Per l'integrazione con la soluzione Kaspersky Endpoint Detection and Response Expert (on-premises), è necessario aggiungere il componente Endpoint Detection and Response Expert (on-premises) e configurare Kaspersky Endpoint Security.

I componenti Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), e Endpoint Detection and Response Expert (on-premises) i non sono compatibili tra loro.

Per il corretto funzionamento di Endpoint Detection and Response Expert (on-premises), è necessario soddisfare le seguenti condizioni:

- OSMP (Open Single Management Platform) è installato.
- L'applicazione è attivata e la funzionalità è coperta dalla licenza.
- Il componente Endpoint Detection and Response Expert (on-premises) è attivato.
- I componenti dell'applicazione che garantiscono il funzionamento di EDR Expert (on-premises) sono abilitati e operativi. I seguenti componenti assicurano il funzionamento di EDR Expert (on-premises):
  - Protezione minacce file.
  - Protezione minacce web.
  - Protezione minacce di posta.
  - Prevenzione Exploit.
  - Rilevamento del Comportamento.
  - Prevenzione Intrusioni Host.
  - Motore di Remediation.
  - Controllo adattivo delle anomalie.

La configurazione dell'integrazione di EDR Expert (on-premises) prevede i passaggi seguenti:

1. **Installazione del componente EDR Expert (on-premises).**

   È possibile selezionare il componente EDR Expert (on-premises) durante l'installazione o l'upgrade, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

   > È necessario riavviare il computer per completare l'aggiornamento dell'applicazione con il nuovo componente.

2. **Attivazione di Kaspersky Endpoint Detection and Response Expert (on-premises)**

   È necessario acquistare una licenza separata per EDR Expert (on-premises) (componente aggiuntivo Kaspersky Endpoint Detection and Response Expert (on-premises)).

   La funzionalità diventa disponibile dopo aver aggiunto una chiave separata per Kaspersky Endpoint Detection and Response Expert (on-premises). Di conseguenza, nel computer vengono aggiunte due chiavi: una per Kaspersky Endpoint Security e l'altra per Kaspersky Endpoint Detection and Response Expert (on-premises).

   La licenza per la funzionalità Endpoint Detection and Response Expert (on-premises) autonoma è la stessa della licenza di Kaspersky Endpoint Security.

   Verificare che la funzionalità EDR Expert (on-premises) sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

3. **Connessione al server di raccolta della telemetria e al server di risposta**

Kaspersky Endpoint Detection and Response Expert (on-premises) richiede una connessione attendibile tra Kaspersky Endpoint Security e due server:

- Un *server di raccolta della telemetria* è un server che fa parte di una soluzione SIEM che raccoglie, normalizza, correla, analizza e archivia le informazioni sugli eventi che si verificano nel computer.
- Un *server di risposta* è un server per la ricezione e la scansione dei dati, lo studio del comportamento degli oggetti e la pubblicazione dei risultati di tali studi.

Per configurare una connessione attendibile, è necessario utilizzare un certificato TLS. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). Quindi è necessario aggiungere il certificato TLS a Kaspersky Endpoint Security (vedere le istruzioni di seguito).

Per impostazione predefinita, Kaspersky Endpoint Security controlla solo il certificato TLS dei server. Per rendere la connessione più sicura, è inoltre possibile abilitare la verifica del computer nel server (autenticazione a due vie). Per abilitare questa verifica, è necessario attivare l'autenticazione a due vie nelle impostazioni del server e Kaspersky Endpoint Security. Per utilizzare l'autenticazione a due vie, è necessario anche un contenitore crittografico. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un cripto-contenitore nella piattaforma Open Single Management (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)).

Come connettere un computer Kaspersky Endpoint Security a EDR Expert (on-premises) tramite Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati → Endpoint Detection and Response Expert (on-premises)**.
5. Attivare l'interruttore **Endpoint Detection and Response Expert (on-premises) ABILITATO**.
6. Per configurare EDR Expert (on-premises), selezionare **Endpoint Detection and Response Expert (versione 8.0 o successiva)** dall'elenco delle soluzioni.
7. Configurare la connessione ai *server di raccolta della telemetria*:
   a. Nella sezione **Connessione ai server di raccolta della telemetria**, fare clic sul collegamento **Impostazioni di connessione**.
   b. Configurare la connessione ai server di raccolta della telemetria:
      - **Timeout (sec)**. Timeout massimo del server di KUMA. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server.
      - **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un cripto-contenitore nella piattaforma Open Single Management (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). Dopo aver configurato le impostazioni del server, è necessario abilitare anche l'autenticazione a due vie nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

  Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

c. Fare clic su **OK**.

d. Aggiungere i server di raccolta della telemetria. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.

   È possibile aggiungere più indirizzi di server di raccolta della telemetria. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

e. Se necessario, configurare la telemetria.

8. Configurare la connessione ai *server di risposta*:

   a. Nel blocco **Connessione ai server di risposta**, configurare l'impostazione **Invia richiesta di sincronizzazione al server ogni (min)**. Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security riceve le attività di risposta alle minacce e invia i risultati delle attività.

   b. Fare clic sul collegamento **Impostazioni di connessione**.

   c. Configurare la connessione ai server di risposta:

   - **Timeout (sec)**. Timeout massimo del server di KUMA. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server.

   - **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un cripto-contenitore nella piattaforma Open Single Management (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). Dopo aver configurato le impostazioni del server, è necessario abilitare anche l'autenticazione a due vie nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.

  Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

d. Fare clic su **OK**.

e. Aggiungere i server di risposta. A tale scopo, specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al server.

   È possibile aggiungere più indirizzi server di risposta. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

È possibile verificare lo stato del componente utilizzando *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Endpoint Detection and Response Expert (on-premises)** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

Configurazione delle impostazioni di telemetria EDR Expert (on-premises)

Telemetria è un elenco di eventi che si sono verificati nel computer protetto. Kaspersky Endpoint Security analizza i dati di telemetria e li invia ai server di raccolta della telemetria durante la sincronizzazione. Per ulteriori informazioni sugli eventi di telemetria trasmessi, consultare la Guida di Kaspersky Endpoint Detection and Response Expert (on-premises).

Gli eventi di telemetria arrivano sul server quasi continuamente. Kaspersky Endpoint Security avvia la sincronizzazione con il server quando viene soddisfatta una delle seguenti condizioni:

- L'intervallo di sincronizzazione è scaduto.
- Il numero di eventi nel buffer supera il limite massimo.

Pertanto, per impostazione predefinita, l'applicazione esegue la sincronizzazione ogni 30 secondi oppure ogni volta che il buffer contiene 1024 eventi. È possibile configurare il comportamento di sincronizzazione nella policy di Kaspersky Endpoint Security e selezionare i valori ottimali in base al carico di rete (vedere le istruzioni di seguito).

Se non è presente alcuna connessione tra Kaspersky Endpoint Security e il server, l'applicazione accoda i nuovi eventi. Quando la connessione viene ripristinata, Kaspersky Endpoint Security invia gli eventi in coda al server nell'ordine corretto. Per evitare di sovraccaricare il server, Kaspersky Endpoint Security potrebbe ignorare alcuni eventi. Per abilitare questo, è possibile ottimizzare le impostazioni di trasmissione degli eventi, ad esempio, per impostare un valore massimo di eventi all'ora (vedere le istruzioni di seguito).

Per configurare le impostazioni di telemetria, procedere come segue:

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati → Endpoint Detection and Response Expert (on-premises)**.
5. Per configurare EDR Expert (on-premises), selezionare **Endpoint Detection and Response Expert (versione 8.0 o successiva)** dall'elenco delle soluzioni.
6. Assicurarsi che la casella di controllo **Invia telemetria ai server di raccolta della telemetria** sia selezionata nel blocco **Impostazioni trasmissione dati**.
7. Se necessario, selezionare la casella di controllo **Invia telemetria solo con IOA**. *Indicatore di attacco (IOA)* è una regola che contiene una descrizione di un comportamento sospetto nel sistema che potrebbe indicare un attacco mirato. L'applicazione confronta il comportamento in corso nel sistema con queste regole e registra gli eventi indicativi di un attacco mirato. L'applicazione utilizza la tecnologia di *scansione in streaming*, che consente il monitoraggio in tempo reale di tali eventi.
8. Se necessario, configurare la sincronizzazione con le impostazioni del server nel blocco **Impostazioni trasmissione dati**:

   - **Ritardo di trasmissione eventi massimo (sec)**. L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione. L'impostazione predefinita è 30 secondi.
   - **Numero massimo di pacchetti eventi**. L'applicazione si sincronizza con il server quando il buffer si riempie di eventi. L'impostazione predefinita è 1024 eventi.
9. Se necessario, deselezionare la casella di controllo **Abilita limitazione delle richieste** nel blocco **Limitazione delle richieste**.

   Questa funzionalità consente di ottimizzare il carico sul server. Se questa funzionalità è abilitata, l'applicazione limita la trasmissione degli eventi. Se il numero di eventi supera i limiti configurati, Kaspersky Endpoint Security interrompe l'invio degli eventi. Questa opzione è abilitata per impostazione predefinita.
10. Configurare le impostazioni di ottimizzazione per l'invio degli eventi al server:

    - **Numero massimo di eventi all'ora**. L'applicazione analizza il flusso di dati di telemetria e limita l'invio degli eventi se il flusso di eventi supera il limite di eventi all'ora configurato. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora. L'impostazione predefinita è 3000 eventi all'ora. Se l'applicazione è installata in un server, il flusso di dati di telemetria è maggiore. Per i server, è consigliabile aumentare il valore a 60.000 eventi all'ora.
    - **Percentuale di eccedenza limite eventi**. L'applicazione ordina gli eventi in base al tipo (ad esempio, eventi di "Modifiche nel Registro di sistema") e limita la trasmissione degli eventi se il rapporto tra eventi dello stesso tipo e il numero totale di eventi supera il limite percentuale configurato. Kaspersky Endpoint Security riprende l'invio degli eventi quando il rapporto tra altri eventi e il numero totale di eventi diventa di nuovo sufficientemente elevato. L'impostazione predefinita è 15%.
11. Nel blocco **Connessione ai server di risposta**, immettere un valore per il parametro **Invia richiesta di sincronizzazione al server ogni (min)**.

12. Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security invia informazioni sulle attività e le impostazioni dell'applicazione modificate.

13. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Esclusioni della telemetria EDR Expert (on-premises)

Per migliorare le prestazioni e ottimizzare la trasmissione dei dati al server di raccolta della telemetria, è possibile aggiungere le esclusioni della telemetria. È ad esempio possibile scegliere di non inviare i dati sulle comunicazioni di rete per le singole applicazioni.

L'utilizzo di un numero eccessivo di regole può aumentare il carico sul server di raccolta della telemetria e ridurre le prestazioni del computer. È consigliabile aggiungere solo le regole necessarie.

Per creare un'esclusione di telemetria in Web Console e Cloud Console:

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Impostazioni di telemetria**.

5. Selezionare la scheda **Telemetria EDR Expert (on-premises)**.

6. Nel blocco **Esclusioni generali**, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Aggiungi regola di esclusione**.

7. Se necessario, modificare lo stato della regola. La regola è abilitata per impostazione predefinita.

8. Immettere un nome per la regola.

9. Selezionare l'azione da eseguire quando viene attivata la regola:

   - **Non raccogliere**. L'evento filtrato verrà escluso dalla telemetria inviata.

   - **Escludi IOA**. L'evento di attivazione della regola IOA verrà escluso dalla telemetria inviata.

10. Se l'opzione **Escludi IOA** è selezionata, specificare le regole IOA da aggiungere alle esclusioni:

    - **Escludi tutto**. Quando la condizione specificata viene soddisfatta, l'applicazione escluderà gli eventi generati in base a tutte le regole IOA dalla telemetria.

    - **Escludi in base a GUID**. Specificare il GUID della regola IOA. È possibile specificare più GUID utilizzando `,`. Per maggiori dettagli sulle regole IOA, fare riferimento alla Guida di EDR Expert (on-premises).

11. Specificare la condizione di filtraggop:

    a. Selezionare il nome del campo da utilizzare per il filtraggio.

    b. Selezionare un operatore (vedere la tabella seguente) e specificare il valore con cui confrontare il valore del campo dell'evento.

Elenco di operatori condizionali

Operatore	Descrizione
<	Se il valore del campo è inferiore al valore specificato nella condizione, l'evento verrà filtrato.
≤	Se il valore del campo è inferiore o uguale al valore specificato nella condizione, l'evento verrà filtrato.
=	Se il valore del campo è uguale al valore specificato nella condizione, l'evento verrà filtrato.
≥	Se il valore del campo è maggiore o uguale al valore specificato nella condizione, l'evento verrà filtrato.
>	Se il valore del campo è maggiore del valore specificato nella condizione, l'evento verrà escluso.
≠	Se il valore del campo non è uguale al valore specificato nella condizione, l'evento verrà filtrato.
simile a	Se il valore del campo corrisponde alla maschera specificata nella condizione, l'evento verrà filtrato. L'applicazione supporta i caratteri `*` e `?` quando si inserisce una maschera:
non simile a	Se il valore del campo non corrisponde alla maschera specificata nella condizione, l'evento verrà filtrato. L'applicazione supporta i caratteri `*` e `?` quando si inserisce una maschera:
uno di	Se il valore del campo corrisponde a uno dei valori nell'elenco specificato nella condizione, l'evento è considerato filtrato.
nessuno di	Se il valore del campo non corrisponde a nessuno dei valori nell'elenco specificato nella condizione, l'evento è considerato filtrato.
simile a uno di	Se il valore del campo corrisponde a una delle maschere specificate nella condizione, l'evento verrà filtrato. L'applicazione supporta i caratteri * e ? quando si inserisce una maschera:
non è simile a uno di	Se il valore del campo non corrisponde a nessuna delle maschere specificate nella condizione, l'evento verrà filtrato. L'applicazione supporta i caratteri * e ? quando si inserisce una maschera:
esiste	Se il campo specificato nella condizione è presente nell'evento, l'evento verrà escluso.
non esiste	Se il campo specificato nella condizione non è presente nell'evento, l'evento verrà filtrato.
contiene	Se il valore specificato nella condizione è presente nel valore del campo, l'evento verrà escluso.
è uguale a	Se il valore del campo è uguale al valore specificato nella condizione, l'evento verrà filtrato. La scansione non fa distinzione tra maiuscole e minuscole.
E bit a bit	Se il risultato dell'operazione Bitwise AND (&) tra il valore del campo e il valore specificato nella condizione è 1, l'evento verrà filtrato.

12. Se necessario, è possibile creare criteri di filtro complessi aggiungendo più condizioni di filtro e gruppi di condizioni. È inoltre possibile aggiungere condizioni e gruppi di condizioni nidificati a un gruppo di condizioni. È possibile utilizzare i seguenti operatori:

    - **E** indica che il filtro seleziona gli eventi che soddisfano tutte le condizioni specificate.
    - **O** indica che il filtro seleziona gli eventi che soddisfano una delle condizioni specificate.
    - **NOT** (per utilizzare questo operatore, selezionare l'opzione **Aggiungi NOT prima**) indica che il filtro seleziona gli eventi che non soddisfano nessuna delle condizioni specificate.

    Le condizioni e i gruppi di condizioni di primo livello sono combinati con l'operatore **E**.

13. Se nel computer è in esecuzione OSMP (Open Single Management Platform), è possibile eseguire la scansione della regola di filtraggio creata. Per eseguire la scansione, fare clic sul pulsante **Controlla regola**.

    Nella finestra visualizzata verrà mostrata una tabella di eventi filtrati in base alla regola creata. Per maggiori dettagli, consultare la Guida di EDR Expert (on-premises).

14. Se necessario, in **Tutti i tipi di eventi**, aggiungere le esclusioni della telemetria in base al tipo di evento.

    a. Fare clic sul nome del tipo di evento.

    b. Nella finestra visualizzata, fare clic sul pulsante **Configura manualmente**.

    c. Se necessario, configurare la trasmissione della telemetria per il tipo di evento selezionato utilizzando l'interruttore **Invia evento**. Per impostazione predefinita, la trasmissione della telemetria è abilitata per tutti i tipi di eventi.

    d. Nel blocco **Regole di esclusione**, fare clic sul pulsante **Aggiungi**.

    Verrà visualizzata la finestra **Aggiungi regola di esclusione**.

    e. Eseguire le azioni descritte nei passaggi 7-13 per ogni regola aggiunta.

15. Per alcuni tipi di eventi, è inoltre possibile aggiungere regole di inclusione per espandere la telemetria raccolta:

    a. Nel blocco **Regole di inclusione**, fare clic sul pulsante **Aggiungi**.

    Verrà visualizzata la finestra **Aggiungi regole di inclusione**.

    b. Immettere un nome per la regola.

    c. In **Condizione**, immettere i valori per i campi visualizzati. Il tipo di campi disponibili dipende dall'evento selezionato.

> Le regole di esclusione hanno la priorità rispetto alle regole di inclusione.

16. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Esportazione e importazione dei filtri eventi EDR Expert (on-premises).

È possibile esportare l'elenco delle esclusioni in un file JSON. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di ID di eventi. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dei filtri degli eventi o per eseguire la migrazione dell'elenco in un server diverso.

> L'utilizzo di un numero eccessivo di regole può aumentare il carico sul server di raccolta della telemetria e ridurre le prestazioni del computer. È consigliabile aggiungere solo le regole necessarie.

Come esportare e importare i filtri degli eventi in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali → Esclusioni e tipi di oggetti**.

5. Nel blocco **Impostazioni di telemetria → Telemetria EDR Expert (on-premises)**, fare clic sul pulsante **Impostazioni**.

6. Per esportare i filtri degli eventi:

   a. Fare clic su **Esporta**.

   Nella finestra visualizzata specificare il nome del file JSON in cui si desidera esportare i filtri degli eventi e selezionare la cartella in cui si desidera salvare il file.

   b. Salvare il file.

   Kaspersky Endpoint Security esporta i filtri degli eventi nel file JSON.

7. Per importare i filtri degli eventi:

   a. Fare clic su **Importa**.

   b. Nella finestra visualizzata, selezionare il file JSON da cui si desidera importare i filtri degli eventi.

   c. Aprire il file.

   Se esistono già regole di filtraggio degli eventi nel computer, Kaspersky Endpoint Security le sostituisce durante l'importazione.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come esportare e importare i filtri degli eventi in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse → Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali → Impostazioni di telemetria**.

5. Selezionare la scheda **Telemetria EDR Expert (on-premises)**.

6. Per esportare i filtri degli eventi:

   a. Fare clic su **Esporta**.

   b. Nella finestra visualizzata specificare il nome del file JSON in cui si desidera esportare i filtri degli eventi e selezionare la cartella in cui si desidera salvare il file.

   c. Salvare il file.

   Kaspersky Endpoint Security esporta i filtri degli eventi nel file JSON.

7. Per importare i filtri degli eventi:

   a. Fare clic su **Importa**.

   b. Nella finestra visualizzata, selezionare il file JSON da cui si desidera importare i filtri degli eventi.

c. Selezionare il modo in cui si desidera importare le regole di filtraggio degli eventi: aggiungendole alle regole esistenti o eliminando le regole esistenti e sostituendole con nuove.

d. Aprire il file.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

È inoltre possibile esportare o importare i filtri degli eventi nella riga di comando.

Considerazioni speciali sull'utilizzo dei profili criterio per configurare l'integrazione con EDR Expert (on-premises) ed EDR (KATA)

Per configurare l'integrazione con EDR (KATA) per determinati gruppi di amministrazione e con EDR Expert (on-premises) per altri nell'ambito di un singolo criterio, è necessario utilizzare i profili criterio. È necessario configurare le impostazioni di integrazione di EDR (KATA) nelle proprietà del criterio, mentre l'integrazione di EDR Expert (on-premises) per i gruppi di amministrazione selezionati deve essere configurata nelle proprietà del profilo criterio.

L'utilizzo dei profili criterio per configurare l'integrazione con EDR Expert (on-premises) presenta le seguenti limitazioni:

- Se si configura l'integrazione con EDR Expert (on-premises) nelle proprietà del criterio, queste impostazioni si applicheranno a tutti i gruppi di amministrazione; le impostazioni di integrazione dei profili criterio non verranno applicate.

- Quando si utilizzano i profili criterio per configurare l'integrazione con EDR Expert (on-premises), non è possibile utilizzare Administration Console (MMC) per gestire i criteri. Quando si aprono le proprietà del criterio in Administration Console, le impostazioni di integrazione di EDR Expert (on-premises) nei profili criterio verranno sovrascritte dalle impostazioni del criterio, provocando il malfunzionamento del componente. Sarà necessario reimpostare le impostazioni del componente Endpoint Detection and Response Expert (on-premises) secondo le istruzioni riportate di seguito.

- Quando si utilizzano i profili criterio per configurare l'integrazione con EDR Expert (on-premises), non è possibile utilizzare criteri figlio.

Se è già stato configurato un criterio in una versione precedente del plug-in Web, è necessario reimpostare le impostazioni del componente Endpoint Detection and Response Expert (on-premises) per applicare le impostazioni di integrazione di EDR Expert (on-premises) ai dispositivi gestiti dai profili criterio.

Per reimpostare le impostazioni del componente:

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response Expert (on-premises)**.

5. Modificare la modalità operativa da **Endpoint Detection and Response Expert (versione 7.1 o precedente)** a **Modalità Endpoint Detection and Response Expert (versione 8.0 o successiva)**.

6. Tornare a **Endpoint Detection and Response Expert (versione 7.1 o precedente)**.

7. Salvare le modifiche.

Endpoint Detection and Response Expert (cloud)

L'integrazione di Kaspersky Endpoint Security con Kaspersky Endpoint Detection and Response Expert (cloud) non è temporaneamente disponibile. Questa funzionalità dovrebbe essere supportata entro la fine del 2026. Tenere traccia delle nostre note sulla versione per essere a conoscenza degli upgrade delle applicazioni e delle nuove funzionalità.



Kaspersky Endpoint Security supporta l'integrazione con la soluzione Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* è una soluzione di sicurezza informatica aziendale basata su cloud che include le applicazioni Kaspersky che consentono a un'organizzazione di difendersi dalla maggior parte dei tipi di rischi informatici e coprire i più importanti scenari di propagazione delle minacce. I componenti di EDR Expert (cloud) vengono distribuiti in Open Single Management Platform (OSMP). Questa piattaforma esegue scenari multipiattaforma in un'unica interfaccia e consente di integrare le applicazioni Kaspersky con applicazioni di terze parti in un sistema di protezione completo.

Uno degli elementi centrali della soluzione è *SIEM*. SIEM monitora gli eventi provenienti da tutti i componenti e correla questi eventi tra loro utilizzando regole definite dal fornitore e dall'utente. EDR Expert (cloud) esamina i registri e la telemetria ricevuti dall'infrastruttura aziendale per rilevare automaticamente gli attacchi e consente di indagare sugli incidenti utilizzando un grafico di indagine unificato che combina tutti gli eventi raccolti in EDR Expert (cloud), inclusi gli eventi delle applicazioni Kaspersky e prodotti di terze parti per la sicurezza delle informazioni.

Per la risposta a incidenti avanzati, EDR Expert (cloud) utilizza scenari preimpostati e definiti dall'utente. È inoltre possibile utilizzare le azioni di reazione di applicazioni di terze parti e gli scenari di reazione che coinvolgono più applicazioni.

Strumenti di threat intelligence

Kaspersky Endpoint Detection and Response utilizza i seguenti strumenti Threat Intelligence:

- Integrazione con Kaspersky Threat Intelligence Portal, che contiene e mostra informazioni sulla reputazione di file e indirizzi Web.
- Database delle minacce di Kaspersky.
- L'infrastruttura di servizi cloud di Kaspersky Security Network (di seguito denominata anche "KSN"), che fornisce accesso ai file in tempo reale, siti Web e informazioni sulla reputazione del software dalla knowledge base di Kaspersky. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce risposte più rapide da parte delle applicazioni Kaspersky alle minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi positivi.

Principio di funzionamento della soluzione

L'applicazione Kaspersky Endpoint Security viene installata nei singoli computer dell'infrastruttura IT aziendale e monitora continuamente i processi, le connessioni di rete aperte e i file modificati.

Le informazioni sugli eventi nel computer (telemetria) vengono inviate al server di EDR Expert (cloud). In questo caso, Kaspersky Endpoint Security invia anche informazioni sulle minacce rilevate dall'applicazione, nonché informazioni sull'elaborazione dei risultati di tali minacce ai server di raccolta della telemetria.

L'integrazione di EDR Expert (cloud) è configurata nella console di Kaspersky Security Center. L'agente integrato viene quindi gestito tramite Open Single Management Platform (OSMP), inclusa l'esecuzione delle attività, la gestione degli oggetti in quarantena, la visualizzazione dei rapporti e altre azioni.

Integrazione dell'agente integrato con EDR Expert (cloud)

Per configurare l'integrazione con la soluzione Kaspersky Endpoint Detection and Response (cloud), è necessario installare il componente Endpoint Detection and Response Expert (cloud) e configurare Kaspersky Endpoint Security.

I componenti Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud), e Endpoint Detection and Response Expert (on-premises) i non sono compatibili tra loro.

Condizioni operative di EDR Expert (cloud)

Per il funzionamento di EDR Expert (cloud), devono essere soddisfatte le seguenti condizioni:

- L'infrastruttura Kaspersky Endpoint Detection and Response Expert (cloud) è disponibile nell'area geografica. Per informazioni sulla disponibilità dell'infrastruttura EDR Expert (cloud) nella propria area geografica, consultare contattare l'Assistenza tecnica.
- OSMP (Open Single Management Platform) è installato.
- Kaspersky Endpoint Security installato in modalità standard.
- L'applicazione Kaspersky Endpoint Security è attivata e la funzionalità è coperta dalla licenza.
- Sono stati accettati i termini dell'Accordo per il trattamento dei dati di Kaspersky Endpoint Detection and Response Expert (cloud).
- Il componente Endpoint Detection and Response Expert (cloud) è abilitato.
- I componenti dell'applicazione che garantiscono il funzionamento di EDR Expert (cloud) sono abilitati e operativi.
  - Protezione minacce file.
  - Protezione minacce web.
  - Protezione minacce di posta.
  - Prevenzione Exploit.
  - Rilevamento del Comportamento.
  - Prevenzione Intrusioni Host.

- Motore di Remediation.
- Controllo adattivo delle anomalie.

Passaggi per l'integrazione con EDR Expert (cloud)

La configurazione dell'integrazione di EDR Expert (cloud) prevede i passaggi seguenti:

1. **Installazione del componente Endpoint Detection and Response Expert (cloud)**

   È possibile selezionare il componente Endpoint Detection and Response Expert (cloud) durante l'installazione o l'upgrade, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

   > È necessario riavviare il computer per completare l'aggiornamento dell'applicazione con il nuovo componente.

2. **Attivazione di Kaspersky Endpoint Detection and Response Expert (cloud)**

   È necessario acquistare una licenza separata per Kaspersky Endpoint Detection and Response Expert (cloud).

   La funzionalità diventa disponibile dopo aver aggiunto una chiave separata per Kaspersky Endpoint Detection and Response Expert (cloud). Di conseguenza, nel computer vengono aggiunte due chiavi: una per Kaspersky Endpoint Security e l'altra per Kaspersky Endpoint Detection and Response Expert (cloud).

   La licenza per la funzionalità Endpoint Detection and Response Expert (cloud) autonoma è la stessa della licenza di Kaspersky Endpoint Security.

   Verificare che la funzionalità EDR Expert (cloud) sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

3. **Connessione al server di raccolta della telemetria e al server di risposta**

   Kaspersky Endpoint Detection and Response Expert (cloud) richiede una connessione attendibile tra Kaspersky Endpoint Security e due server:

   - Un *server di raccolta della telemetria* è un server che fa parte di una soluzione SIEM che raccoglie, normalizza, correla, analizza e archivia le informazioni sugli eventi che si verificano nel computer.
   - Un *server di risposta* è un server per la ricezione e la scansione dei dati, lo studio del comportamento degli oggetti e la pubblicazione dei risultati di tali studi.

   Come connettere un computer Kaspersky Endpoint Security a EDR Expert (cloud) tramite Web Console

   1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
   2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

      Verrà visualizzata la finestra delle proprietà del criterio.
   3. Selezionare la scheda **Impostazioni applicazione**.
   4. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response Expert (cloud)**.
   5. Abilitare il componente utilizzando l'interruttore **Endpoint Detection and Response Expert (cloud) DISABILITATO**.

6. Se il criterio corrente è un criterio secondario e il criterio principale vieta di modificare le impostazioni di integrazione di EDR Expert (cloud) ("lucchetto chiuso"), è possibile configurare l'ereditarietà delle impostazioni nella sezione **Eredità**:

   - **Eredita le impostazioni di connessione dal criterio** (valore predefinito). Le impostazioni di connessione verranno ereditate dal criterio principale. Non sarà possibile modificare le impostazioni.
   - **Usa impostazioni di connessione personalizzate**. È possibile configurare le impostazioni di connessione manualmente:

7. La scheda **Server di risposta** mostra il nome di dominio completo e la porta del server di risposta, che vengono recuperati automaticamente. Se il criterio di protezione nell'infrastruttura non consente la connessione diretta ai server EDR Expert (cloud), è possibile configurare una connessione tramite un tunnel TCP:

   a. Selezionare la casella di controllo **Usa un tunnel TCP per la risposta**.

   b. Specificare l'indirizzo del server (IPv4, IPv6) e la porta per connettersi al tunnel.

8. Se necessario, impostare la frequenza di invio delle richieste di sincronizzazione al server nel campo **Invia richiesta di sincronizzazione al server ogni (min)**. Durante la sincronizzazione, Kaspersky Endpoint Security riceve le attività di risposta alle minacce e invia i risultati delle attività.

9. Passare alla scheda **Server di raccolta della telemetria**.

10. Configurare le impostazioni di connessione al server di raccolta della telemetria:

    a. Fare clic sul collegamento **Modifica**.

    b. Nella finestra visualizzata selezionare il server di raccolta della telemetria dall'elenco. L'agente di raccolta KUMA funge da server di raccolta della telemetria in EDR Expert (cloud). Per ulteriori dettagli, fare riferimento alla Guida di Kaspersky Unified Monitoring and Analysis Platform.

    Se si verifica un errore durante la connessione al server di raccolta della telemetria, selezionare un altro server. Se non si riesce a connettersi al server di raccolta della telemetria, contattare l'Assistenza tecnica.

    c. Se necessario, è possibile configurare una connessione al server di raccolta della telemetria tramite un tunnel TCP, come per il server di risposta.

11. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

È possibile verificare lo stato del componente utilizzando *Rapporto sullo stato dei componenti dell'applicazione*. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Endpoint Detection and Response Expert (cloud)** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

Configurazione delle impostazioni di telemetria EDR Expert (cloud)

Telemetria è un elenco di eventi che si sono verificati nel computer protetto. Kaspersky Endpoint Security analizza i dati di telemetria e li invia ai server di raccolta della telemetria durante la sincronizzazione. Gli eventi di telemetria arrivano sul server quasi continuamente. Kaspersky Endpoint Security avvia la sincronizzazione con il server quando viene soddisfatta una delle seguenti condizioni:

- L'intervallo di sincronizzazione è scaduto.
- Il numero di eventi nel buffer supera il limite massimo.

Pertanto, per impostazione predefinita, l'applicazione esegue la sincronizzazione ogni 30 secondi oppure ogni volta che il buffer contiene 1024 eventi. È possibile configurare il comportamento di sincronizzazione nella policy di Kaspersky Endpoint Security e selezionare i valori ottimali in base al carico di rete (vedere le istruzioni di seguito).

Se non è presente alcuna connessione tra Kaspersky Endpoint Security e il server, l'applicazione accoda i nuovi eventi. Quando la connessione viene ripristinata, Kaspersky Endpoint Security invia gli eventi in coda al server nell'ordine corretto. Per evitare di sovraccaricare il server, Kaspersky Endpoint Security potrebbe ignorare alcuni eventi. Per abilitare questo, è possibile ottimizzare le impostazioni di trasmissione degli eventi, ad esempio, per impostare un valore massimo di eventi all'ora (vedere le istruzioni di seguito).

Per configurare le impostazioni di telemetria, procedere come segue:

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Endpoint Detection and Response Expert (cloud)**.
5. Nella finestra visualizzata, selezionare la scheda **Impostazioni trasmissione dati**.
6. Verificare che la casella di controllo **Invio della telemetria ABILITATO** sia selezionata.
7. Se necessario, abilitare la funzionalità **Invia telemetria solo con IOA**. *Indicatore di attacco (IOA)* è una regola che contiene una descrizione di un comportamento sospetto nel sistema che potrebbe indicare un attacco mirato. L'applicazione confronta il comportamento in corso nel sistema con queste regole e registra gli eventi indicativi di un attacco mirato. L'applicazione utilizza la tecnologia di *scansione in streaming*, che consente il monitoraggio in tempo reale di tali eventi. Per impostazione predefinita, la funzionalità è disabilitata.
8. Se necessario, configurare le impostazioni di sincronizzazione del server:

   - **Ritardo di trasmissione eventi massimo (sec)**. L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione. L'impostazione predefinita è 30 secondi.
   - **Numero massimo di pacchetti eventi**. L'applicazione si sincronizza con il server quando il buffer si riempie di eventi. L'impostazione predefinita è 1024 eventi.
9. Passare alla scheda **Limitazione delle richieste**.

10. Se necessario, disabilitare la limitazione delle richieste utilizzando l'interruttore **Limitazione delle richieste ABILITATA**.

    Questa funzionalità consente di ottimizzare il carico sul server. Se questa funzionalità è abilitata, l'applicazione limita la trasmissione degli eventi. Se il numero di eventi supera i limiti configurati, Kaspersky Endpoint Security interrompe l'invio degli eventi. Questa opzione è abilitata per impostazione predefinita.

11. Configurare le impostazioni di ottimizzazione per l'invio degli eventi al server:

    - **Numero massimo di eventi all'ora**. L'applicazione analizza il flusso di dati di telemetria e limita l'invio degli eventi se il flusso di eventi supera il limite di eventi all'ora configurato. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora. L'impostazione predefinita è 3000 eventi all'ora. Se l'applicazione è installata in un server, il flusso di dati di telemetria è maggiore. Per i server, è consigliabile aumentare il valore a 60.000 eventi all'ora.

    - **Percentuale di eccedenza limite eventi (%)**. L'applicazione ordina gli eventi in base al tipo (ad esempio, eventi di "Modifiche nel Registro di sistema") e limita la trasmissione degli eventi se il rapporto tra eventi dello stesso tipo e il numero totale di eventi supera il limite percentuale configurato. Kaspersky Endpoint Security riprende l'invio degli eventi quando il rapporto tra altri eventi e il numero totale di eventi diventa di nuovo sufficientemente elevato. L'impostazione predefinita è 15%.

12. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Esclusioni della telemetria EDR Expert (cloud)

Per migliorare le prestazioni e ottimizzare la trasmissione dei dati al server di raccolta della telemetria, è possibile aggiungere le esclusioni della telemetria. È ad esempio possibile scegliere di non inviare i dati sulle comunicazioni di rete per le singole applicazioni.

L'utilizzo di un numero eccessivo di regole può aumentare il carico sul server di raccolta della telemetria e ridurre le prestazioni del computer. È consigliabile aggiungere solo le regole necessarie.

Per creare un'esclusione di telemetria in Web Console e Cloud Console:

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Impostazioni di telemetria**.

5. Selezionare la scheda **Telemetria di EDR Expert (cloud)**.

6. Nel blocco **Esclusioni generali**, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Aggiungi regola di esclusione**.

7. Se necessario, modificare lo stato della regola. La regola è abilitata per impostazione predefinita.

8. Immettere un nome per la regola.

9. Selezionare l'azione da eseguire quando viene attivata la regola:

   - **Non raccogliere**. L'evento filtrato verrà escluso dalla telemetria inviata.
   - **Escludi IOA**. L'evento di attivazione della regola IOA verrà escluso dalla telemetria inviata.

10. Se l'opzione **Escludi IOA** è selezionata, specificare le regole IOA da aggiungere alle esclusioni:

    - **Escludi tutto**. Quando la condizione specificata viene soddisfatta, l'applicazione escluderà gli eventi generati in base a tutte le regole IOA dalla telemetria.
    - **Escludi in base a GUID**. Specificare il GUID della regola IOA. È possibile specificare più GUID utilizzando `,`. Per maggiori dettagli sulle regole IOA, fare riferimento alla Guida di EDR Expert (cloud).

11. Specificare la condizione di filtraggop:

    a. Selezionare il nome del campo da utilizzare per il filtraggio.

    b. Selezionare un operatore (vedere la tabella seguente) e specificare il valore con cui confrontare il valore del campo dell'evento.

Elenco di operatori condizionali

Operatore	Descrizione
<	Se il valore del campo è inferiore al valore specificato nella condizione, l'evento verrà filtrato.
≤	Se il valore del campo è inferiore o uguale al valore specificato nella condizione, l'evento verrà filtrato.
=	Se il valore del campo è uguale al valore specificato nella condizione, l'evento verrà filtrato.
≥	Se il valore del campo è maggiore o uguale al valore specificato nella condizione, l'evento verrà filtrato.
>	Se il valore del campo è maggiore del valore specificato nella condizione, l'evento verrà escluso.
≠	Se il valore del campo non è uguale al valore specificato nella condizione, l'evento verrà filtrato.
simile a	Se il valore del campo corrisponde alla maschera specificata nella condizione, l'evento verrà filtrato. L'applicazione supporta i caratteri `*` e `?` quando si inserisce una maschera:
non simile a	Se il valore del campo non corrisponde alla maschera specificata nella condizione, l'evento verrà filtrato. L'applicazione supporta i caratteri `*` e `?` quando si inserisce una maschera:
uno di	Se il valore del campo corrisponde a uno dei valori nell'elenco specificato nella condizione, l'evento è considerato filtrato.
nessuno di	Se il valore del campo non corrisponde a nessuno dei valori nell'elenco specificato nella condizione, l'evento è considerato filtrato.
simile a uno di	Se il valore del campo corrisponde a una delle maschere specificate nella condizione, l'evento verrà filtrato. L'applicazione supporta i caratteri * e ? quando si inserisce una maschera:
non è simile a uno di	Se il valore del campo non corrisponde a nessuna delle maschere specificate nella condizione, l'evento verrà filtrato. L'applicazione supporta i caratteri * e ? quando si inserisce una maschera:
esiste	Se il campo specificato nella condizione è presente nell'evento, l'evento verrà escluso.
non esiste	Se il campo specificato nella condizione non è presente nell'evento, l'evento verrà filtrato.
contiene	Se il valore specificato nella condizione è presente nel valore del campo, l'evento verrà escluso.
è uguale a	Se il valore del campo è uguale al valore specificato nella condizione, l'evento verrà filtrato. La scansione non fa distinzione tra maiuscole e minuscole.
E bit a bit	Se il risultato dell'operazione Bitwise AND (&) tra il valore del campo e il valore specificato nella condizione è 1, l'evento verrà filtrato.

12. Se necessario, è possibile creare criteri di filtro complessi aggiungendo più condizioni di filtro e gruppi di condizioni. È inoltre possibile aggiungere condizioni e gruppi di condizioni nidificati a un gruppo di condizioni. È possibile utilizzare i seguenti operatori:

    - **E** indica che il filtro seleziona gli eventi che soddisfano tutte le condizioni specificate.
    - **O** indica che il filtro seleziona gli eventi che soddisfano una delle condizioni specificate.
    - **NOT** (per utilizzare questo operatore, selezionare l'opzione **Aggiungi NOT prima**) indica che il filtro seleziona gli eventi che non soddisfano nessuna delle condizioni specificate.

    Le condizioni e i gruppi di condizioni di primo livello sono combinati con l'operatore **E**.

13. Per eseguire la scansione della regola di filtraggio creata, fare clic sul pulsante **Controlla regola**.

    Nella finestra visualizzata verrà mostrata una tabella di eventi filtrati in base alla regola creata. Per maggiori dettagli, consultare la Guida di EDR Expert (cloud).

14. Se necessario, in **Tutti i tipi di eventi**, aggiungere le esclusioni della telemetria in base al tipo di evento.

    a. Fare clic sul nome del tipo di evento.

    b. Nella finestra visualizzata, fare clic sul pulsante **Configura manualmente**.

    c. Se necessario, configurare la trasmissione della telemetria per il tipo di evento selezionato utilizzando l'interruttore **Invia evento**. Per impostazione predefinita, la trasmissione della telemetria è abilitata per tutti i tipi di eventi.

    d. Nel blocco **Regole di esclusione**, fare clic sul pulsante **Aggiungi**.

    Verrà visualizzata la finestra **Aggiungi regola di esclusione**.

    e. Eseguire le azioni descritte nei passaggi 7-13 per ogni regola aggiunta.

15. Per alcuni tipi di eventi, è inoltre possibile aggiungere regole di inclusione per espandere la telemetria raccolta:

    a. Nel blocco **Regole di inclusione**, fare clic sul pulsante **Aggiungi**.

    Verrà visualizzata la finestra **Aggiungi regole di inclusione**.

    b. Immettere un nome per la regola.

    c. In **Condizione**, immettere i valori per i campi visualizzati. Il tipo di campi disponibili dipende dall'evento selezionato.

    Le regole di esclusione hanno la priorità rispetto alle regole di inclusione.

16. Per applicare il criterio ai computer, assicurarsi che i lucchetti siano chiusi (🔒) e salvare le modifiche.

Come esportare o importare i filtri degli eventi di EDR Expert (cloud)

È possibile esportare l'elenco delle esclusioni in un file JSON. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di ID di eventi. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dei filtri degli eventi o per eseguire la migrazione dell'elenco in un server diverso.

L'utilizzo di un numero eccessivo di regole può aumentare il carico sul server di raccolta della telemetria e ridurre le prestazioni del computer. È consigliabile aggiungere solo le regole necessarie.

Per esportare o importare i filtri degli eventi in Web Console:

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di telemetria**.
5. Selezionare la scheda **Telemetria di EDR Expert (cloud)**.
6. Per esportare i filtri degli eventi:
   a. Fare clic su **Esporta**.
   b. Nella finestra visualizzata specificare il nome del file JSON in cui si desidera esportare i filtri degli eventi e selezionare la cartella in cui si desidera salvare il file.
   c. Salvare il file.

      Kaspersky Endpoint Security esporta i filtri degli eventi nel file JSON.
7. Per importare i filtri degli eventi:
   a. Fare clic su **Importa**.
   b. Nella finestra visualizzata, selezionare il file JSON da cui si desidera importare i filtri degli eventi.
   c. Selezionare il modo in cui si desidera importare le regole di filtraggio degli eventi: aggiungendole alle regole esistenti o eliminando le regole esistenti e sostituendole con nuove.
   d. Aprire il file.

8. Per applicare il criterio ai computer, assicurarsi che i lucchetti siano chiusi (🔒) e salvare le modifiche.

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di telemetria**.
5. Selezionare la scheda **Telemetria di EDR Expert (cloud)**.
6. Per esportare i filtri degli eventi:

   a. Fare clic su **Esporta**.

   b. Nella finestra visualizzata specificare il nome del file JSON in cui si desidera esportare i filtri degli eventi e selezionare la cartella in cui si desidera salvare il file.

   c. Salvare il file.

   Kaspersky Endpoint Security esporta i filtri degli eventi nel file JSON.
7. Per importare i filtri degli eventi:

   a. Fare clic su **Importa**.

   b. Nella finestra visualizzata, selezionare il file JSON da cui si desidera importare i filtri degli eventi.

   c. Selezionare il modo in cui si desidera importare le regole di filtraggio degli eventi: aggiungendole alle regole esistenti o eliminando le regole esistenti e sostituendole con nuove.

   d. Aprire il file.
8. Per applicare il criterio ai computer, assicurarsi che i lucchetti siano chiusi (🔒) e salvare le modifiche.

Gestione della quarantena

Quarantena è una memoria locale speciale sul computer. L'utente può mettere in quarantena i file che considera pericolosi per il computer. I file in quarantena vengono archiviati in uno stato criptato e non minacciano la sicurezza del dispositivo. Kaspersky Endpoint Security utilizza la Quarantena solo quando è integrato con le soluzioni Kaspersky Detection and Response. In altri casi, Kaspersky Endpoint Security inserisce il file pertinente in Backup. Per ulteriori dettagli sulla gestione di Quarantena come parte delle soluzioni, consultare la Guida di Kaspersky Sandbox Help, la Guida di Kaspersky Endpoint Detection and Response Optimum, la Guida di Kaspersky Endpoint Detection and Response Expert, la Guida di Kaspersky Anti Targeted Attack Platform e la Guida di Kaspersky Endpoint Detection and Response Expert (on-premises).

Kaspersky Endpoint Security utilizza l'account di sistema (SYSTEM) per mettere in quarantena i file.

È possibile configurare le impostazioni della quarantena solo nella console di Kaspersky Security Center. È possibile utilizzare Web Console per gestire gli oggetti in quarantena (ripristino, eliminazione, aggiunta ecc.) In locale, nel computer, è possibile ripristinare l'oggetto solo tramite la riga di comando.

Configurazione della dimensione massima della quarantena

Per impostazione predefinita, la dimensione della quarantena è limitata a 1024 MB. Quando Quarantena raggiunge le dimensioni massime, Kaspersky Endpoint Security interrompe l'invio dei file e genera l'evento *Spazio insufficiente nell'archivio Quarantena*. Per evitare che lo spazio su disco si esaurisca in quarantena, è possibile impostare una soglia oltre la quale Kaspersky Endpoint Security genera un evento *Spazio nell'archivio Quarantena quasi esaurito*. Non è possibile configurare un periodo di conservazione per i file in quarantena in modo da rimuoverli automaticamente.

Se la soluzione Kaspersky Anti Targeted Attack Platform (EDR) è distribuita nell'organizzazione, si consiglia di aumentare le dimensioni della Quarantena. Quando si esegue una scansione YARA, l'applicazione potrebbe riscontrare un dump di memoria di grandi dimensioni. Se la dimensione del dump della memoria supera la dimensione della Quarantena, la scansione YARA termina con un errore e il dump della memoria non viene messo in quarantena. Si consiglia di impostare la dimensione della Quarantena su una dimensione identica a quella totale della RAM nel computer (ad esempio, 8 GB) o di disabilitare il limite di dimensioni della Quarantena.

Come configurare la dimensione massima della quarantena in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali → Rapporti e archivi**.
4. Nel blocco **Quarantena**, configurare la dimensione della quarantena:
   - **Limita le dimensioni della Quarantena a N MB**. Se la casella di controllo è selezionata, le dimensioni massime della quarantena si limitano al valore definito. Per impostazione predefinita, la dimensione massima è di 1024 MB. Quando la Quarantena raggiunge la dimensione massima, Kaspersky Endpoint Security invia l'evento *Spazio insufficiente nell'archivio Quarantena* a Kaspersky Security Center e pubblica l'evento nel registro eventi di Windows. Nel frattempo, l'applicazione interrompe l'inserimento in quarantena dei nuovi oggetti. È necessario svuotare manualmente la Quarantena.

     Se la casella di controllo è deselezionata, le dimensioni della Quarantena sono limitate dallo spazio libero su disco disponibile.
   - **Invia notifica quando l'archivio Quarantena raggiunge N percento**. Valore soglia della Quarantena. Ad esempio, è possibile impostare la soglia di quarantena su 50%. Quando la Quarantena raggiunge la soglia, Kaspersky Endpoint Security invia l'evento corrispondente a Kaspersky Security Center e pubblica l'evento nel registro eventi di Windows. Nel frattempo, l'applicazione continua a mettere in quarantena i nuovi oggetti.

     Se questa casella di controllo è deselezionata, l'applicazione non genera eventi quando viene raggiunta la soglia di quarantena.
5. Salvare le modifiche.

Come configurare la dimensione massima della Quarantena in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Rapporti e archivi**.

5. Nel blocco **Quarantena**, configurare la dimensione della quarantena:

   - **Limita le dimensioni della Quarantena**. Se la casella di controllo è selezionata, le dimensioni della quarantena si limitano al valore specificato. Se la casella di controllo è deselezionata, le dimensioni della Quarantena sono limitate dallo spazio libero su disco disponibile. Questa operazione potrebbe essere necessaria per la scansione YARA poiché l'applicazione può salvare un file di dump della memoria di grandi dimensioni.

   - **Dimensione massima della Quarantena (MB)**. Se la casella di controllo è selezionata, le dimensioni massime della quarantena si limitano al valore definito. Per impostazione predefinita, la dimensione massima è di 1024 MB. Quando la Quarantena raggiunge la dimensione massima, Kaspersky Endpoint Security invia l'evento *Spazio insufficiente nell'archivio Quarantena* a Kaspersky Security Center e pubblica l'evento nel registro eventi di Windows. Nel frattempo, l'applicazione interrompe l'inserimento in quarantena dei nuovi oggetti. È necessario svuotare manualmente la Quarantena.

     Se la casella di controllo è deselezionata, le dimensioni della Quarantena sono limitate dallo spazio libero su disco disponibile.

   - **Invia notifica quando l'archivio Quarantena raggiunge (%)**. Valore soglia della Quarantena. Ad esempio, è possibile impostare la soglia di quarantena su 50%. Quando la Quarantena raggiunge la soglia, Kaspersky Endpoint Security invia l'evento corrispondente a Kaspersky Security Center e pubblica l'evento nel registro eventi di Windows. Nel frattempo, l'applicazione continua a mettere in quarantena i nuovi oggetti.

6. Salvare le modifiche.

Invio dei dati relativi ai file in quarantena a Kaspersky Security Center

Per eseguire azioni con oggetti in quarantena in Web Console, è necessario abilitare l'invio dei dati dei file in quarantena ad Administration Server. Ad esempio, è possibile scaricare un file dalla quarantena per l'analisi in Web Console. Affinché funzioni correttamente, l'invio dei dati dei file in quarantena deve essere abilitato per tutte le funzionalità di Kaspersky Sandbox e Kaspersky Endpoint Detection and Response.

Come abilitare il trasferimento dei dati dei file in quarantena in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Rapporti e archivi**.

4. Nel blocco **Trasferimento dei dati ad Administration Server**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, selezionare la casella di controllo **File in quarantena**.

6. Salvare le modifiche.

Come abilitare il trasferimento dei dati dei file in quarantena in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Integrazione KSC**.
5. Nella sezione **Trasferimento dei dati ad Administration Server** selezionare la casella di controllo **Informazioni sui file in Quarantena**.
6. Salvare le modifiche.

Di conseguenza, è possibile visualizzare un elenco di file, messi in quarantena nel computer, nella console di Kaspersky Security Center. È possibile utilizzare la console di Kaspersky Security Center per gestire gli oggetti in quarantena (ripristino, eliminazione, aggiunta ecc.) Per informazioni dettagliate sulle operazioni che è possibile eseguire con la Quarantena, consultare la Guida di Kaspersky Security Center.

Ripristino dei file dalla quarantena

Per impostazione predefinita, Kaspersky Endpoint Security ripristina i file nella cartella originale. Se la cartella di destinazione è stata eliminata o l'utente non dispone dei diritti di accesso a tale cartella, l'applicazione inserisce il file nella cartella `%DataRoot%\QB\Restored`. Quindi, è necessario spostare manualmente il file nella cartella di destinazione.

Per ripristinare i file dalla quarantena:

1. Nella finestra principale di Web Console, fare clic su **Operazioni** → **Archivi** → **Quarantena**.
2. Si apre l'elenco dei file in Quarantena; nell'elenco visualizzato, selezionare i file da ripristinare e fare clic su **Ripristina**.

   Kaspersky Endpoint Security ripristina il file. Se la cartella di destinazione contiene già un file con lo stesso nome, l'applicazione annulla il ripristino del file. L'applicazione salva una copia del file in Quarantena dopo averlo ripristinato. Per eliminare il file, è necessario svuotare manualmente la Quarantena.

Monitoraggio delle azioni EDR

Kaspersky Endpoint Security for Windows 12.9 introduce il Centro di monitoraggio delle azioni EDR. Il *Centro di monitoraggio delle azioni EDR* è una console in cui è possibile visualizzare la cronologia di Threat Response per tutte le soluzioni Kaspersky Detection and Response. Se nell'organizzazione sono distribuiti più dispositivi Detection and Response (ad esempio EDR Optimum e MDR), Kaspersky Endpoint Security mostra la cronologia di Threat Response per tutte le soluzioni. Questo consente di analizzare le prestazioni delle soluzioni Detection and Response in un computer separato e ottimizzare le impostazioni di tali soluzioni.

Il centro di monitoraggio fornisce le seguenti informazioni:

- Informazioni sulle attività di Threat Response (ad esempio l'attività *Termina processo*)
- Modifiche delle regole di isolamento della rete e prevenzione dell'esecuzione

Se la risposta alle minacce rileva un errore relativo all'accesso a una condivisione di rete, tale errore viene omesso dalla cronologia di risposta alle minacce visualizzata.

Per passare al centro di monitoraggio delle azioni EDR:

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Risorse (dispositivi)**.
2. Selezionare il computer per cui si desidera configurare le impostazioni locali dell'applicazione.

   Verranno visualizzate le proprietà del computer.
3. Selezionare la scheda **Applicazioni**.
4. Fare clic su **Kaspersky Endpoint Security for Windows 14.2**.

   Verranno visualizzate le impostazioni locali dell'applicazione.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Passare a **Detection and Response** → **Cronologia risposte**.

   Viene aperta la console del centro di monitoraggio delle azioni EDR. È possibile utilizzare la console per visualizzare gli stati delle attività di risposta alle minacce, la durata delle attività, le modifiche alle regole e i dettagli dell'iniziatore.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security for Windows supporta la soluzione Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* è una soluzione SIEM (Security Information and Event Management) per l'infrastruttura IT delle organizzazioni. KUMA consente di rilevare, analizzare e attenuare le minacce alla sicurezza prima che possano causare danni.

L'applicazione Kaspersky Endpoint Security viene installata nei singoli computer dell'infrastruttura IT aziendale e monitora continuamente i processi, le connessioni di rete aperte e i file modificati. Le informazioni sugli eventi nel computer (dati di telemetria) vengono inviate al server di Kaspersky Unified Monitoring and Analysis Platform (KUMA). Nella relativa console, KUMA mostra gli eventi come elenco senza commenti, in modo simile al registro eventi di Windows.

Kaspersky Endpoint Security non fornisce tutte le funzionalità di un agente per KUMA. L'applicazione invia eventi a KUMA solo senza commenti. Per accedere a tutte le funzionalità di KUMA, è necessario acquistare una licenza e distribuire la soluzione in conformità con la Guida dell'amministratore di KUMA.

Integrazione di Kaspersky Endpoint Security con KUMA

La configurazione dell'integrazione di KES con KUMA prevede i seguenti passaggi:

1. Nella console KUMA aggiungere un servizio di raccolta.
2. Nella console KUMA configurare un connettore affinché il servizio di raccolta riceva gli eventi da KES.
3. Nella console KUMA abilitare l'autenticazione a due vie (facoltativo).
4. Nel criterio di Kaspersky Endpoint Security for Windows configurare le impostazioni per la connessione di KES a KUMA.
5. Nella console KUMA assicurarsi che gli eventi di KES vengano inviati al tenant corretto e siano elaborati dalle regole di correlazione corrette.

Preparazione dell'integrazione di KES con KUMA

Per utilizzare KUMA, è necessario che le seguenti condizioni siano soddisfatte:

- Kaspersky Security Center versione 14.2 o successiva. Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità di integrazione di KUMA.
- L'applicazione è attivata e la funzionalità è coperta dalla licenza.
- Il componente per l'integrazione di KUMA è abilitato.

La preparazione dell'integrazione di KES con KUMA prevede i seguenti passaggi:

1. **Installazione del componente per l'integrazione di KUMA**

   È possibile selezionare il componente per l'integrazione di KUMA durante l'installazione o l'upgrade dell'applicazione, oltre a utilizzare l'attività *Modifica i componenti dell'applicazione*.

   È necessario riavviare il computer per completare l'aggiornamento dell'applicazione con il nuovo componente.

2. **Attivazione KUMA**

   Oltre a una licenza dell'applicazione Kaspersky Endpoint Security (ad esempio, Kaspersky Endpoint Security for Business Standard), è necessaria una licenza separata per l'integrazione di Kaspersky Endpoint Security con KUMA (Componente aggiuntivo di integrazione KUMA di Kaspersky Endpoint Security for Windows).

   Se si installa l'applicazione in modalità EDR Agent, è necessaria una licenza per l'integrazione di Kaspersky Endpoint Security con KUMA e una licenza Kaspersky Anti Targeted Attack Platform (KATA) o una licenza Kaspersky Managed Detection and Response (MDR). Non è possibile distribuire solo EDR Agent per KUMA.

   La funzionalità diventa disponibile dopo l'aggiunta della chiave KUMA separata. Di conseguenza, nel computer sarà presente un'altra chiave attiva per l'integrazione di Kaspersky Endpoint Security con KUMA.

   La licenza per la funzionalità KUMA autonoma è la stessa della licenza di Kaspersky Endpoint Security.

   Verificare che la funzionalità KUMA sia inclusa nella licenza e che venga eseguita nell'interfaccia locale dell'applicazione.

Connessione di KES a KUMA

Per connettere il computer con l'applicazione Kaspersky Endpoint Security alla soluzione KUMA:

1. Nella console KUMA, aggiungere un servizio di raccolta con connettori di tipo **tcp**, **udp** o **http** e specificare le impostazioni di rete di base della connessione. Per informazioni dettagliate sulla gestione dei connettori, fare riferimento alla Guida di Kaspersky Unified Monitoring and Analysis Platform.

2. Nel criterio di Kaspersky Endpoint Security, aggiungere gli indirizzi dei servizi di raccolta KUMA e specificare le impostazioni di rete della connessione.

Come connettere un computer Kaspersky Endpoint Security a KUMA tramite Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Integrazione KUMA**.
5. Selezionare la casella di controllo **Integrazione KUMA**.

6. Nella sezione **Impostazioni di integrazione** selezionare la casella di controllo **Abilita la trasmissione degli eventi Windows a un server KUMA**.

7. Aggiungere i server di KUMA:

   a. Fare clic su **Aggiungi**.

   Viene aperto il modulo in cui è possibile aggiungere i server KUMA.

   b. Selezionare il protocollo per la connessione al server di KUMA: **HTTP / HTTPS**, **TCP**, **UDP**.

   Il protocollo per la connessione al servizio di raccolta in Kaspersky Endpoint Security deve corrispondere al tipo di connettore in KUMA: **http**, **tcp** o **udp**.

   > Quando si utilizza il protocollo UDP, è possibile che i dati vadano persi a causa della perdita di traffico intrinseca al protocollo.

   c. Immettere l'indirizzo del server (IPv4, IPv6, FQDN) e la porta per connettersi al server (per impostazione predefinita, è specificata la porta 443).

   Quando si immette l'indirizzo del server, considerare quanto segue:

   - **TCP**:
     - **Senza TLS**. È possibile specificare l'indirizzo IP o l'FQDN del server.
     - **Con TLS**. È necessario specificare solo l'FQDN del server.
   - **HTTP / HTTPS**:
     - **Senza TLS**. È necessario specificare esplicitamente il protocollo HTTP nell'indirizzo del server (ad esempio, `http://server.com` o `http://10.10.10.100`).
     - **Con TLS**. Non è necessario specificare il protocollo (ad esempio, `https://server.com` o `server.com`).
   - **UDP**. Il protocollo UDP non supporta il criptaggio TLS. È possibile specificare l'indirizzo IP o l'FQDN del server.

   È possibile visualizzare l'indirizzo del server nelle proprietà del connettore nella console KUMA. Per ulteriori informazioni sui connettori KUMA, consultare la Guida di Kaspersky Unified Monitoring and Analysis Platform.

   d. Fare clic su **OK**.

   Kaspersky Endpoint Security si connette al primo server di KUMA nell'elenco. Se la connessione ha esito negativo, Kaspersky Endpoint Security si connette al secondo server di KUMA nell'elenco e così via.

8. Se necessario, configurare l'impostazione **Ritardo di trasmissione eventi massimo (sec)** nel blocco **Impostazioni trasmissione dati**. Allo scadere del tempo specificato, Kaspersky Endpoint Security tenta di connettersi allo stesso servizio di raccolta oppure si connette al servizio di raccolta successivo nell'elenco, se sono presenti più servizi di raccolta. L'impostazione predefinita è 30 secondi.

9. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come connettere un computer Kaspersky Endpoint Security a KUMA tramite Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Configurazione agenti integrati** → **Integrazione KUMA**.
5. Attivare l'interruttore **Integrazione KUMA ABILITATA**.
6. Aggiungere i server di KUMA:

   a. Fare clic su **Aggiungi**.

   Viene aperto il modulo in cui è possibile aggiungere i server KUMA.

   b. Selezionare il protocollo per la connessione al server di KUMA: **HTTP/HTTPS**, **TCP**, **UDP**.

   Il protocollo per la connessione al servizio di raccolta in Kaspersky Endpoint Security deve corrispondere al tipo di connettore in KUMA: **http**, **tcp** o **udp**.

   > Quando si utilizza il protocollo UDP, è possibile che i dati vadano persi a causa della perdita di traffico intrinseca al protocollo.

   c. Immettere l'indirizzo del server (IPv4, IPv6, FQDN) e la porta per connettersi al server (per impostazione predefinita, è specificata la porta 443).

   Quando si immette l'indirizzo del server, considerare quanto segue:

   - **TCP**:
     - **Senza TLS**. È possibile specificare l'indirizzo IP o l'FQDN del server.
     - **Con TLS**. È necessario specificare solo l'FQDN del server.
   - **HTTP/HTTPS**:
     - **Senza TLS**. È necessario specificare esplicitamente il protocollo HTTP nell'indirizzo del server (ad esempio, `http://server.com` o `http://10.10.10.100`).
     - **Con TLS**. Non è necessario specificare il protocollo (ad esempio, `https://server.com` o `server.com`).
   - **UDP**. Il protocollo UDP non supporta il criptaggio TLS. È possibile specificare l'indirizzo IP o l'FQDN del server.

   È possibile visualizzare l'indirizzo del server nelle proprietà del connettore nella console KUMA. Per ulteriori informazioni sui connettori KUMA, consultare la Guida di Kaspersky Unified Monitoring and Analysis Platform.

   d. Fare clic su **OK**.

Kaspersky Endpoint Security si connette al primo server di KUMA nell'elenco. Se la connessione ha esito negativo, Kaspersky Endpoint Security si connette al secondo server di KUMA nell'elenco e così via.

7. Se necessario, configurare l'impostazione **Ritardo massimo nell'invio degli eventi (sec)** nel blocco **Impostazioni della connessione al server**. Allo scadere del tempo specificato, Kaspersky Endpoint Security tenta di connettersi allo stesso servizio di raccolta oppure si connette al servizio di raccolta successivo nell'elenco, se sono presenti più servizi di raccolta. L'impostazione predefinita è 30 secondi.

8. Salvare le modifiche.

È possibile verificare che l'integrazione KUMA sia configurata correttamente nella console KUMA (per informazioni dettagliate, vedere Guida di Kaspersky Unified Monitoring and Analysis Platform). Verificare lo stato operativo del componente visualizzando il *Rapporto sullo stato dei componenti dell'applicazione* nella console di Kaspersky Security Center. È inoltre possibile visualizzare lo stato operativo di un componente nei rapporti nell'interfaccia locale di Kaspersky Endpoint Security. Il componente **Integrazione KUMA** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

Creazione di una connessione attendibile tra KES e KUMA

È possibile stabilire una connessione attendibile tra Kaspersky Endpoint Security e un servizio di raccolta KUMA dotato di un connettore di tipo tcp o http. Non è possibile stabilire una connessione attendibile con un connettore di tipo udp.

Per stabilire una connessione attendibile, è necessario configurare una modalità TLS nelle impostazioni del connettore. Sono disponibili le seguenti modalità TLS:

- **Disabled**: Non utilizzare il criptaggio TLS. Questa opzione è selezionata per impostazione predefinita.
- **Enabled**: Utilizzare il criptaggio TLS, ma senza verificare il certificato.
- **Custom PFX with client authentication**: Utilizzare il criptaggio TLS con un segreto PFX. In questa modalità, il client viene autenticato con un certificato.

Kaspersky Endpoint Security non supporta la modalità TLS **Custom PFX**. Quando si integra KES con KUMA tramite PFX, è richiesta l'autenticazione dell'utente con una password.

Per configurare una connessione attendibile, è necessario un certificato TLS: il *certificato CA per il microservizio*. È possibile ottenere un certificato TLS nella console KUMA. Per informazioni dettagliate sul download dei certificati TLS, fare riferimento alla Guida di Kaspersky Unified Monitoring and Analysis Platform. Quindi è necessario aggiungere il certificato TLS a Kaspersky Endpoint Security (vedere le istruzioni di seguito).

Per rendere la connessione più sicura, è possibile abilitare l'autenticazione aggiuntiva del computer in KUMA (autenticazione a due vie). Per abilitare tale autenticazione, è necessario creare un contenitore crittografico presso un'autorità di certificazione esterna. Un *contenitore crittografico* è un archivio PFX contenente un certificato e una chiave privata in formato PKCS#12. È quindi necessario abilitare l'autenticazione a due vie nelle impostazioni di KUMA (modalità TLS **Custom PFX with client authentication**), abilitare l'autenticazione a due vie in Kaspersky Endpoint Security e aggiungere un archivio PFX alla console KUMA e a Kaspersky Endpoint Security.

Come configurare una connessione attendibile tra KES e KUMA in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Integrazione KUMA**.
5. Selezionare la casella di controllo **Integrazione KUMA**.
6. Nella sezione **Impostazioni per la connessione ai server KUMA** selezionare la casella di controllo **Usa criptaggio TLS**.
7. Configurare la connessione attendibile:
   a. Fare clic su **Impostazioni per la connessione ai server KUMA**.
   b. Configurare la connessione al server:
      - **Timeout (sec)**. Tempo massimo di attesa di una risposta dal server KUMA (per impostazione predefinita, il valore è 5 secondi). Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server di KUMA.
      - **Certificato TLS del server**. Certificato TLS per stabilire una connessione attendibile con il server di KUMA. È possibile ottenere un certificato TLS nella console Kaspersky Unified Monitoring and Analysis Platform (vedere le istruzioni nella Guida di Kaspersky Unified Monitoring and Analysis Platform).

        Per stabilire una connessione attendibile, è necessario selezionare la modalità TLS **Enabled** nella console KUMA.
      - **Usa autenticazione a due vie**. Autenticazione a due vie durante la creazione di una connessione sicura tra KES e KUMA. Per utilizzare l'autenticazione a due vie, nella console KUMA, nelle impostazioni del connettore, è necessario selezionare la modalità TLS **Custom PFX with client authentication** (vedere le impostazioni del connettore nella Guida di Kaspersky Unified Monitoring and Analysis Platform). Quindi è necessario scaricare un certificato del server e impostare una password per proteggere il contenitore crittografico.

        > Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

   c. Fare clic su **OK**.
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare una connessione attendibile tra KES e KUMA in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Configurazione agenti integrati** → **Integrazione KUMA**.

5. Attivare l'interruttore **Integrazione KUMA ABILITATA**.

6. In **Impostazioni della connessione al server**, attivare l'interruttore **Usa criptaggio TLS**.

7. Configurare la connessione attendibile:

   a. Fare clic su **Impostazioni di connessione**.

   b. Configurare la connessione al server:

   - **Timeout (sec)**. Tempo massimo di attesa di una risposta dal server KUMA (per impostazione predefinita, il valore è 5 secondi). Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server di KUMA.

   - **Certificato TLS del server**. Certificato TLS per stabilire una connessione attendibile con il server di KUMA. È possibile ottenere un certificato TLS nella console Kaspersky Unified Monitoring and Analysis Platform (vedere le istruzioni nella Guida di Kaspersky Unified Monitoring and Analysis Platform).

     Per stabilire una connessione attendibile, è necessario selezionare la modalità TLS **Enabled** nella console KUMA.

   - **Usa autenticazione a due vie**. Autenticazione a due vie durante la creazione di una connessione sicura tra KES e KUMA. Per utilizzare l'autenticazione a due vie, nella console KUMA, nelle impostazioni del connettore, è necessario selezionare la modalità TLS **Custom PFX with client authentication** (vedere le impostazioni del connettore nella Guida di Kaspersky Unified Monitoring and Analysis Platform). Quindi è necessario scaricare un certificato del server e impostare una password per proteggere il contenitore crittografico.

     > Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.

   c. Fare clic su **OK**.

8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Abilitazione dell'invio della telemetria al server KUMA

Per impostazione predefinita, l'invio di eventi al server KUMA è disabilitato. Per garantire il corretto funzionamento di KUMA, è necessario abilitare l'invio della telemetria. È possibile selezionare un'origine evento tra i registri standard: *Application*, *Security* o *System*.

Come abilitare l'invio della telemetria a KUMA in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella struttura della console, selezionare **Criteri**.

3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.

5. Nel blocco **Impostazioni di telemetria** → **Telemetria KUMA**, fare clic sul pulsante **Impostazioni**.
6. Selezionare i registri eventi che si desidera utilizzare come sorgenti degli eventi: *Application*, *Security* o *System*.
   Oltre ai registri standard, è possibile specificare un registro di un'applicazione di terze parti.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come abilitare l'invio della telemetria a KUMA in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di telemetria**.
5. Selezionare la scheda **Telemetria KUMA**.
6. Selezionare i registri eventi che si desidera utilizzare come sorgenti degli eventi: *Application*, *Security* o *System*.
   Oltre ai registri standard, è possibile specificare un registro di un'applicazione di terze parti.
7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Filtraggio degli eventi da inviare a KUMA

Per impostazione predefinita, l'invio di eventi al server KUMA è disabilitato. Per garantire il corretto funzionamento di KUMA, è necessario abilitare l'invio della telemetria. È possibile selezionare un'origine evento tra i registri standard: *Application*, *Security* o *System*. Per migliorare le prestazioni e ottimizzare la trasmissione dei dati al server KUMA, è possibile aggiungere o escludere manualmente singoli eventi dalla telemetria. È ad esempio possibile escludere gli eventi Sysmon.

Come creare un elenco di eventi da inviare a KUMA in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.
5. Nel blocco **Impostazioni di telemetria** → **Telemetria KUMA**, fare clic sul pulsante **Impostazioni**.
6. Nella finestra visualizzata, configurare i filtri degli eventi da inviare a KUMA.

È possibile configurare il filtro degli eventi per i registri *Application*, *Security*, *System* standard o aggiungere manualmente un altro registro:

a. Aprire le proprietà del registro o fare clic sul pulsante **Aggiungi** e immettere il nome del log.

b. Selezionare una modalità di invio degli eventi:

- **Invia tutti gli eventi**. In questa modalità, l'applicazione invia tutti gli eventi dal registro di Windows ad eccezione degli eventi aggiunti alle regole di esclusione.
- **Invia solo gli eventi selezionati**. In questa modalità, l'applicazione invia solo gli eventi aggiunti nelle regole di inclusione.

c. Creare elenchi di regole di esclusione o di inclusione per la modalità di invio degli eventi pertinente.

Per aggiungere regole, è necessario specificare l'ID dell'evento nel registro eventi di Windows. È possibile elencare più ID evento in una regola. Per specificare più ID evento, utilizzare il carattere virgola (`,`).

d. Se necessario, abilitare la registrazione degli eventi utilizzando la casella di controllo accanto al nome del log.

7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come creare un elenco di eventi da inviare a KUMA in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di telemetria**.
5. Selezionare la scheda **Telemetria KUMA**.
6. Nella finestra visualizzata, configurare i filtri degli eventi da inviare a KUMA.

   È possibile configurare il filtro degli eventi per i registri *Application*, *Security*, *System* standard o aggiungere manualmente un altro registro:

   a. Aprire le proprietà del registro o fare clic sul pulsante **Aggiungi** e immettere il nome del log.

   b. Selezionare una modalità di invio degli eventi:

   - **Invia tutti gli eventi**. In questa modalità, l'applicazione invia tutti gli eventi dal registro di Windows ad eccezione degli eventi aggiunti alle regole di esclusione.
   - **Invia solo gli eventi selezionati**. In questa modalità, l'applicazione invia solo gli eventi aggiunti nelle regole di inclusione.

   c. Creare elenchi di regole di esclusione o di inclusione per la modalità di invio degli eventi pertinente.

   Per aggiungere regole, è necessario specificare l'ID dell'evento nel registro eventi di Windows. È possibile elencare più ID evento in una regola. Per specificare più ID evento, utilizzare il carattere virgola (`,`).

   d. Se necessario, abilitare la registrazione degli eventi utilizzando l'interruttore accanto al nome del log.

7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Esportazione e importazione di filtri degli eventi KUMA

È possibile esportare l'elenco delle esclusioni in un file JSON. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di ID di eventi. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup dei filtri degli eventi o per eseguire la migrazione dell'elenco in un server diverso.

L'utilizzo di un numero eccessivo di regole può aumentare il carico nel server KUMA e ridurre le prestazioni del computer. È consigliabile aggiungere solo le regole necessarie.

Come esportare e importare i filtri degli eventi in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare **Criteri**.
3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
4. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti**.
5. Nel blocco **Impostazioni di telemetria** → **Telemetria KUMA**, fare clic sul pulsante **Impostazioni**.
6. Per esportare i filtri degli eventi:
   a. Selezionare i registri eventi con i filtri che si desidera esportare.
   b. Fare clic sul pulsante → **Esporta**.
   c. Nella finestra visualizzata specificare il nome del file JSON in cui si desidera esportare i filtri degli eventi e selezionare la cartella in cui si desidera salvare il file.
   d. Salvare il file.

      Kaspersky Endpoint Security esporta i filtri degli eventi nel file JSON.
7. Per importare i filtri degli eventi:
   a. Fare clic sul pulsante → **Importa**.
   b. Nella finestra visualizzata, selezionare il file JSON da cui si desidera importare i filtri degli eventi.
   c. Aprire il file.

      Se esistono già regole di filtraggio degli eventi nel computer, Kaspersky Endpoint Security le sostituisce durante l'importazione.
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come esportare e importare i filtri degli eventi in Web Console

1. Nella finestra principale di Web Console, selezionare la scheda **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Impostazioni di telemetria**.
5. Selezionare la scheda **Telemetria KUMA**.
6. Per esportare i filtri degli eventi:
   a. Selezionare i registri eventi con i filtri che si desidera esportare.
   b. Fare clic sul pulsante → **Esporta**.
   c. Nella finestra visualizzata specificare il nome del file JSON in cui si desidera esportare i filtri degli eventi e selezionare la cartella in cui si desidera salvare il file.
   d. Salvare il file.

      Kaspersky Endpoint Security esporta i filtri degli eventi nel file JSON.
7. Per importare i filtri degli eventi:
   a. Fare clic sul pulsante → **Importa**.
   b. Nella finestra visualizzata, selezionare il file JSON da cui si desidera importare i filtri degli eventi.
   c. Aprire il file.

      Se esistono già regole di filtraggio degli eventi nel computer, Kaspersky Endpoint Security le sostituisce durante l'importazione.
8. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

È inoltre possibile esportare o importare i filtri degli eventi nella riga di comando.

Guida alla migrazione da KSWS a KES

A partire dalla versione 11.8.0, Kaspersky Endpoint Security for Windows supporta le funzionalità di base della soluzione Kaspersky Security for Windows Server (KSWS). *Kaspersky Security for Windows Server* protegge i server in cui vengono eseguiti i sistemi operativi Microsoft Windows e gli archivi collegati alla rete da virus e altre minacce alla sicurezza dei computer a cui i server e gli archivi collegati alla rete sono esposti durante lo scambio di file. Per informazioni dettagliate sul funzionamento della soluzione, consultare la Guida di Kaspersky Security for Windows Server. A partire da Kaspersky Endpoint Security 11.8.0 è possibile eseguire la migrazione da Kaspersky Security for Windows Server a Kaspersky Endpoint Security for Windows e utilizzare un'unica soluzione per proteggere workstation e server.

Requisiti software

Prima di iniziare la migrazione da KSWS a KES, assicurarsi che il server soddisfi i requisiti hardware e software di Kaspersky Endpoint Security for Windows. Gli elenchi delle versioni dei sistemi operativi supportate sono diversi per KES e KSWS. Ad esempio, KES non supporta i server in cui viene eseguito Windows Server 2003.

Requisiti software minimi per la migrazione da KSWS a KES:

- Kaspersky Endpoint Security for Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  Se è installata una versione precedente di Kaspersky Security for Windows Server, si consiglia di effettuare l'upgrade dell'applicazione alla versione più recente. La Conversione guidata di criteri e attività non supporta le versioni precedenti di Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Se è installata una versione precedente di Kaspersky Security Center, aggiornarla alla versione 14.2 o successiva. In questa versione di Kaspersky Security Center, la Conversione guidata di criteri e attività in batch consente di eseguire la migrazione dei criteri in un profilo anziché in un criterio. In questa versione di Kaspersky Security Center, la Conversione guidata di criteri e attività in batch consente inoltre di eseguire la migrazione di una gamma più ampia di impostazioni dei criteri.
- Kaspersky Endpoint Agent 3.10.

  Se è installata una versione precedente di Kaspersky Endpoint Agent, si consiglia di effettuare l'upgrade dell'applicazione alla versione più recente. Kaspersky Endpoint Security supporta la migrazione di una configurazione [KSWS+KEA] a [KES+agente integrato] a partire da Kaspersky Endpoint Agent 3.10.

Suggerimenti per la migrazione

Durante la migrazione da KSWS a KES, osservare i seguenti suggerimenti:

- Pianificare in anticipo la migrazione da KSWS a KES. Scegliere un orario in cui i server operano con il carico minimo, ad esempio durante il fine settimana.
- Dopo la migrazione, attivare gradualmente i componenti dell'applicazione. Ciò significa, ad esempio, iniziare abilitando solo il componente Protezione minacce file, abilitare gli altri componenti di protezione, quindi abilitare i componenti di controllo e così via. Ad ogni passaggio, è necessario assicurarsi che l'applicazione funzioni correttamente e monitorare le prestazioni del server. L'architettura di KES differisce da KSWS, quindi anche il sistema operativo potrebbe comportarsi diversamente.
- Eseguire la migrazione gradualmente. Migrare prima un singolo server, poi più server, quindi eseguire la migrazione su tutti i server dell'organizzazione.
- Migrare i diversi tipi di server separatamente. Ciò significa, ad esempio, migrare prima i server di database, quindi i server di posta e così via.
- La migrazione su server a carico elevato implica alcune considerazioni speciali.

Passaggi della migrazione

La migrazione da KSWS a KES viene eseguita in modo semiautomatico. Ciò è necessario a causa delle diverse architetture delle applicazioni. Per eseguire la migrazione delle impostazioni dei criteri, è necessario eseguire la Conversione guidata di criteri e attività in batch (la migrazione guidata). Dopo aver eseguito la migrazione delle impostazioni dei criteri, è necessario configurare manualmente le impostazioni che la migrazione guidata non può migrare automaticamente (ad esempio, le impostazioni di protezione tramite password). Dopo la migrazione, si consiglia inoltre di verificare se la migrazione guidata ha eseguito correttamente la migrazione di tutte le impostazioni.

Eseguire la migrazione da KSWS a KES nel seguente ordine:

1. **Migrazione delle attività e dei criteri di KSWS**

   Dopo aver eseguito la migrazione di criteri e attività, è necessario eseguire ulteriori passaggi di configurazione. Si consiglia inoltre di verificare che Kaspersky Endpoint Security fornisca il livello di sicurezza necessario dopo la migrazione da KSWS.

   > La Conversione guidata di criteri e attività in batch per Kaspersky Security for Windows Server è disponibile solo in Administration Console (MMC). Non è possibile eseguire la migrazione delle impostazioni dei criteri e delle attività in Web Console e Kaspersky Security Center Cloud Console.

2. **Installazione di Kaspersky Endpoint Security**

È possibile installare Kaspersky Endpoint Security nei seguenti modi:

- Installazione di KES dopo aver rimosso KSWS (consigliato).

  L'utilità kavremover non supporta la gestione di KSWS.

- Installazione di KES su KSWS.

3. Attivazione di KES con una chiave di KSWS

4. **Verifica che l'applicazione funzioni correttamente dopo la migrazione**

   Dopo la migrazione da KSWS a KES, assicurarsi che l'applicazione funzioni correttamente. Controllare lo stato del server nella console (deve essere *OK*). Assicurarsi che non vengano segnalati errori per l'applicazione; controllare inoltre l'ora dell'ultima connessione all'Administration Server, l'ora dell'ultimo aggiornamento del database e lo stato di protezione del server.

   Prestare particolare attenzione alla migrazione di elenchi di esclusione, applicazioni attendibili, indirizzi Web attendibili, regole di Controllo applicazioni.

Corrispondenza dei componenti di KSWS e KES

Durante la migrazione da KSWS a KES, il set di componenti viene migrato solo quando l'applicazione viene installata in locale.

Corrispondenza dei componenti Kaspersky Security for Windows Server e Kaspersky Endpoint Security for Windows Components

Componente Kaspersky Security for Windows Server	Componente Kaspersky Endpoint Security for Windows
Funzionalità di base	Kernel dell'applicazione
Log Inspection	Log Inspection
Controllo dispositivi	Controllo dispositivi
Gestione firewall	*(non supportato)* La funzioni dei firewall di KSWS vengono eseguite dal firewall a livello di sistema. In KES, un componente separato è responsabile della funzionalità Firewall. Dopo la migrazione, è possibile configurare il firewall di Kaspersky Endpoint Security.
Monitoraggio integrità file	Monitoraggio integrità di sistema
Prevenzione Exploit	Prevenzione Exploit
Icona dell'area di notifica	*(non supportato)* È possibile configurare l'interazione utente nelle impostazioni dell'interfaccia dell'applicazione.
Integrazione con Kaspersky Security Center	Connettore per Network Agent
Endpoint Agent	*(non supportato)* In Kaspersky Endpoint Security 11.9.0, il pacchetto di distribuzione di Kaspersky Endpoint Agent non fa più parte del kit di distribuzione di Kaspersky Endpoint Security. È necessario scaricare il pacchetto di distribuzione di Kaspersky Endpoint Agent separatamente.
Protezione minacce di rete	Protezione minacce di rete
Anti-Cryptor	Rilevamento del Comportamento
Anti-Cryptor per NetApp	*(non supportato)*

Componente Kaspersky Security for Windows Server	Componente Kaspersky Endpoint Security for Windows
Sicurezza del traffico	Protezione minacce Web Protezione minacce di posta Controllo Web
Scansione su richiesta	Kernel dell'applicazione
Protezione dell'archivio di rete ICAP	*(non supportato)* Kaspersky Endpoint Security non supporta i componenti di Network Storage Protection. Se questi componenti sono necessari, è possibile continuare a utilizzare Kaspersky Security for Windows Server.
Protezione dell'archivio di rete RPC	*(non supportato)* Kaspersky Endpoint Security non supporta i componenti di Network Storage Protection. Se questi componenti sono necessari, è possibile continuare a utilizzare Kaspersky Security for Windows Server.
Protezione file in tempo reale	Protezione minacce file
Monitoraggio degli script	*(non supportato)* Script Monitoring è gestito da altri componenti, ad esempio Protezione AMSI.
Utilizzo di KSN	Kaspersky Security Network
Controllo degli avvii delle applicazioni	Controllo applicazioni
Contatori delle prestazioni	*(non supportato)*

Corrispondenza delle impostazioni di KSWS e KES

Durante la migrazione di criteri e attività, KES viene configurato in base alle impostazioni di KSWS. Le impostazioni dei componenti dell'applicazione non presenti in KSWS sono impostate sui valori predefiniti.

Impostazioni applicazione

Impostazioni di scalabilità, dell'interfaccia e di scansione

Le impostazioni dell'applicazione non sono supportate in Kaspersky Endpoint Security for Windows.

Impostazioni applicazione

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Impostazioni di scalabilità	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security gestisce tutti i processi di lavoro.
Mostra l'icona nell'area di notifica	*(la migrazione non viene effettuata)* In un computer client sono disponibili la finestra principale di Kaspersky Endpoint Security e l'icona nell'area di notifica Windows per impostazione predefinita. Nel menu di scelta rapida dell'icona l'utente può eseguire operazioni con Kaspersky Endpoint Security. Kaspersky Endpoint Security visualizza inoltre le notifiche sopra l'icona dell'applicazione. È possibile configurare l'interazione utente nelle impostazioni dell'interfaccia dell'applicazione.
Ripristina gli attributi dei file dopo la scansione	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security ripristina automaticamente gli attributi dei file dopo la scansione di un file.
Limita l'utilizzo della CPU per i thread di scansione	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non limita l'utilizzo della CPU durante la scansione. È possibile configurare l'attività in modo che venga eseguita quando il computer funziona con carico minimo.

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Cartella per i file temporanei creati durante la scansione	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security inserisce i file temporanei nella cartella `C:\Windows\Temp`.
Impostazioni di sistema HSM	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non supportai sistemi HSM.

Sicurezza e affidabilità

Le impostazioni di sicurezza di KSWS sono state spostate nella sezione **Impostazioni generali** e nelle sottosezioni **Impostazioni applicazione** e **Interfaccia**.

Application security settings

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Proteggere i processi delle applicazioni dalle minacce esterne	**Abilita Auto-difesa** (sottosezione **Impostazioni applicazione**)
Applicare la protezione tramite password	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security dispone di una funzione di protezione tramite password (consultare la sottosezione **Interfaccia**).
Eseguire il ripristino delle attività	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security ripristina automaticamente solo le attività *Scansione malware*. Kaspersky Endpoint Security esegue altre attività in base a una pianificazione.
Non avviare le attività di scansione pianificate	**Rimanda attività pianificate durante l'alimentazione a batteria** (sottosezione **Impostazioni applicazione**)
Arrestare le attività di scansione correnti	*(la migrazione non viene effettuata)* Quando il computer viene alimentato da un gruppo di continuità, Kaspersky Endpoint Security non interrompe le attività di scansione già in esecuzione.

Impostazioni di connessione

Le impostazioni di interazione di Administration Server sono state spostate nella sezione **Impostazioni generali** e nelle sottosezioni **Impostazioni di rete** e **Impostazioni applicazione**.

Administration Server interaction settings

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Impostazioni del server proxy	**Impostazioni del server proxy** (sottosezione **Impostazioni di rete**)
Non utilizzare il server proxy per gli indirizzi locali	**Ignora il server proxy per gli indirizzi locali** (sottosezione **Impostazioni di rete**)
Impostazioni di autenticazione del server proxy	**Usa l'autenticazione per il server proxy** (sottosezione **Impostazioni di rete**) La password di autenticazione del server proxy non viene migrata. Dopo la migrazione di un criterio, la password deve essere immessa manualmente.
Utilizzare Kaspersky Security Center come server proxy durante l'attivazione dell'applicazione	**Usa Kaspersky Security Center come server proxy per l'attivazione** (sottosezione **Impostazioni applicazione**)

Eseguire le attività di sistema locali

Kaspersky Endpoint Security ignora le impostazioni per l'esecuzione delle attività del sistema locali di Kaspersky Security for Windows Server. È possibile configurare l'uso delle attività KES locali in **Attività locali**, **Gestione attività**. È inoltre possibile configurare una pianificazione per l'esecuzione di *Scansione malware* e *Aggiornamento di database e moduli dell'applicazione* nelle proprietà di queste attività.

Supplementare

Area attendibile

Le impostazioni delle aree attendibili di KSWS vengono migrate nella sezione **Impostazioni generali**, sottosezione **Esclusioni**.

Impostazioni delle aree attendibili

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Oggetto da sottoporre a scansione (Esclusioni)	**Esclusioni dalla scansione** (Esclusioni dalla scansione) Questi metodi utilizzati da KSWS e KES per la selezione degli oggetti differiscono. Durante la migrazione, KES supporta esclusioni definite come singoli file o percorsi di file/cartelle. Se in KSWS sono configurate esclusioni come aree predefinite o URL di script, tali esclusioni non vengono migrate. Dopo la migrazione, è necessario aggiungere tali esclusioni manualmente. Le esclusioni come aree predefinite devono essere configurate nelle impostazioni dell'attività *Scansione malware*. Le esclusioni come indirizzi Web script devono essere aggiunte agli indirizzi Web attendibili per la protezione dalle minacce Web.
Applica anche alle sottocartelle (Esclusioni)	**Includi sottocartelle** (Esclusioni dalla scansione)
Oggetti da rilevare (Esclusioni)	**Tipo di oggetto rilevato** (Esclusioni dalla scansione)
Ambito di applicazione dell'esclusione (Esclusioni)	**Componenti della protezione** (Esclusioni dalla scansione) Se in KSWS è selezionato almeno un componente, KES applica le esclusioni a tutti i componenti dell'applicazione.
Commento (Esclusioni)	**Commento** (Esclusioni dalla scansione)
Processo attendibile (Processo attendibile)	**Applicazioni attendibili** I metodi di selezione di processi/applicazioni attendibili differiscono in KSWS e KES. Durante la migrazione, KES supporta applicazioni attendibili configurate come percorso del file eseguibile o della maschera. Se in KSWS sono presenti processi attendibili configurati come hash file, tali processi attendibili non vengono migrati. Dopo la migrazione, è necessario aggiungere tali processi attendibili manualmente.
Non controllare le operazioni di backup dei file (Processo attendibile)	**Non monitorare le attività dell'applicazione** (Applicazioni attendibili)

Scansione unità rimovibili

Le impostazioni di Scansione unità rimovibili vengono migrate nella sezione **Attività locali**, sottosezione **Scansione unità rimovibili**.

Impostazioni di Scansione unità rimovibili

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Eseguire la scansione delle unità rimovibili quando vengono collegate tramite USB	**Azione alla connessione di un'unità rimovibile**
Eseguire la scansione delle unità rimovibili se il volume dei dati archiviati non supera (MB)	**Dimensione massima unità rimovibile**

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Eseguire la scansione con il livello di protezione: • **Massima protezione** • **Consigliati** • **Massime prestazioni**	**Azione alla connessione di un'unità rimovibile**: • **Protezione massima**. • **Consigliato**. I livelli di sicurezza di KSWS corrispondono alle modalità di scansione di KES come segue: • Massima protezione – Protezione massima • Consigliato – Consigliato • Massime prestazioni – Consigliato

Autorizzazioni utente per la gestione dell'applicazione

Kaspersky Endpoint Security non supporta l'assegnazione delle autorizzazioni di accesso utente per la gestione delle applicazioni e dei servizi delle applicazioni. È possibile configurare le impostazioni di accesso per utenti e gruppi di utenti per la gestione delle applicazioni in Kaspersky Security Center.

Autorizzazioni di accesso dell'utente per la gestione di Kaspersky Security Service

Kaspersky Endpoint Security non supporta l'assegnazione delle autorizzazioni di accesso utente per la gestione delle applicazioni e dei servizi delle applicazioni. È possibile configurare le impostazioni di accesso per utenti e gruppi di utenti per la gestione delle applicazioni in Kaspersky Security Center.

Archivi

Le impostazioni dell'archivio di KSWS vengono migrate nella sezione **Impostazioni generali**, sottosezione **Rapporti e archivi**, e nella sezione **Protezione minacce essenziale**, sottosezione **Protezione minacce di rete**.

Impostazioni degli archivi

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Cartella di backup	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security salva le copie di backup dei file nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Dimensione massima del backup (MB)	**Limita la dimensione del Backup a N MB** (sezione **Impostazioni generali** → **Rapporti e archivi**)
Valore soglia per lo spazio disponibile (MB)	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security registra l'evento *Spazio nell'archivio Quarantena quasi esaurito* quando viene raggiunta la soglia del 50%.
Cartella di destinazione per il ripristino degli oggetti	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security ripristina i file nella cartella originale.
Cartella di quarantena	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security salva le copie di backup dei file nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Dimensione massima della quarantena (MB)	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza Backup per archiviare gli oggetti probabilmente infetti. Durante la migrazione, Kaspersky Endpoint Security ignora le impostazioni di Quarantena.
Valore soglia per lo spazio disponibile (MB)	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza Backup per archiviare gli oggetti probabilmente infetti. Durante la migrazione, Kaspersky Endpoint Security ignora le impostazioni di Quarantena.
Cartella di destinazione per il ripristino degli oggetti	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security ripristina i file nella cartella originale.
Sblocca automaticamente dopo N	**Blocca dispositivi che hanno originato l'attacco per N min** (sezione **Protezione minacce essenziale** → **Protezione minacce di rete**)

Protezione server in tempo reale

Protezione file in tempo reale

Le impostazioni di protezione dei file in tempo reale di KSWS vengono migrate nella sezione **Protezione minacce essenziale**, sottosezione **Protezione minacce file**.

Impostazioni di protezione dei file in tempo reale

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Modalità di protezione degli oggetti: • **Modalità intelligente** • **All'esecuzione** • **All'accesso** • **All'accesso e alla modifica**	**Modalità di scansione**: • **Modalità Smart**. • **In fase di esecuzione**. • **In fase di accesso**. • **In fase di accesso e modifica**.
Analisi più approfondita dei processi avviati	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security supporta una sola modalità di analisi: la modalità Ottimale.
Analizzatore euristico: • **Leggera** • **Medio** • **Approfondita**	**Analisi euristica**: • **Superficiale**. • **Media**. • **Approfondita**.
Applica Zona attendibile	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security applica l'area attendibile a tutti i componenti. È possibile configurare le esclusioni nelle impostazioni delle aree attendibili.
Usa KSN per la protezione	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza KSN per tutti i componenti dell'applicazione.
Blocca l'accesso alle risorse condivise di rete per gli host che mostrano attività dannose	*(la migrazione non viene effettuata)* Per impostazione predefinita, Kaspersky Endpoint Security blocca l'accesso alle risorse condivise di rete per gli host che mostrano attività dannose.
Avvia la scansione delle aree critiche quando viene rilevata un'infezione attiva	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non avvia l'attività di scansione delle aree critiche quando viene rilevata un'infezione attiva.
Usa Kaspersky Sandbox per la protezione	*(la migrazione non viene effettuata)* Per impostazione predefinita, Kaspersky Endpoint Security invia gli oggetti da esaminare a Kaspersky Sandbox.
Ambito della protezione	**Ambito della protezione**
Impostazioni di pianificazione	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza la propria pianificazione per sospendere Protezione minacce file.

Utilizzo di KSN

Le impostazioni di KSWS per Kaspersky Security Network vengono migrate nella sezione **Protezione minacce avanzata**, sottosezione **Kaspersky Security Network**.

Impostazioni di Kaspersky Security Network

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Confermo di aver letto e compreso integralmente e di accettare le condizioni di partecipazione a Kaspersky Security Network	**Informativa di Kaspersky Security Network** Kaspersky Endpoint Security richiede il consenso all'Informativa di Kaspersky Security Network quando l'applicazione viene installata, viene creato un nuovo criterio o viene attivato l'utilizzo di Kaspersky Security Network.
Invia i dati sui file esaminati	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security invia automaticamente i dati relativi ai file esaminati se KSN è abilitato.

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Invia i dati sugli URL richiesti	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security invia automaticamente i dati sugli URL richiesti se KSN è abilitato.
Invia le statistiche di Kaspersky Security Network	**Abilita modalità KSN estesa**
Accetta i termini dell'Informativa di Kaspersky Managed Protection	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non include il servizio KMP.
Azione da eseguire sugli oggetti KSN non attendibili	*(la migrazione non viene effettuata)* È possibile configurare l'azione per il rilevamento delle minacce nelle impostazioni dei componenti della protezione e nelle impostazioni delle attività scansione.
Non calcolare il checksum prima dell'invio a KSN se le dimensioni del file superano N MB	*(la migrazione non viene effettuata)* È possibile configurare le limitazioni di scansione dei file di grandi dimensioni nelle impostazioni dei componenti della protezione e nelle impostazioni dell'attività scansione.
Usa Kaspersky Security Center come proxy KSN	**Usa Administration Server come server proxy KSN**
Impostazioni di pianificazione	*(la migrazione non viene effettuata)* Non è possibile configurare una pianificazione separata per il componente. Il componente è sempre attivo mentre Kaspersky Endpoint Security è operativo.

Sicurezza del traffico

Le impostazioni di sicurezza del traffico di KSWS vengono migrate nella sezione **Protezione minacce essenziale**, sottosezione **Protezione minacce Web** e **Protezione minacce di posta**, sezione **Controlli di sicurezza**, sottosezione **Controllo Web**, sezione **Impostazioni generali**, sottosezione **Impostazioni di rete**.

Impostazioni di sicurezza del traffico

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Applica le regole basate sugli URL	**Controllo Web** (sottosezione **Controllo Web**) Le regole basate su URL vengono migrate in regole separate in Kaspersky Endpoint Security.
Applica le regole basate sui certificati	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non supporta le regole basate su certificati.
Applica le regole per il controllo delle categorie di traffico Web	**Controllo Web** (sottosezione **Controllo Web**) Le regole di blocco per il controllo delle categorie di traffico Web vengono migrate in un'unica regola di blocco in Kaspersky Endpoint Security. Kaspersky Endpoint Security ignora le regole per il controllo delle categorie. La corrispondenza delle categorie di KSWS e KES è riportata di seguito.
Consenti l'accesso se la pagina Web non può essere classificata	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security consente l'accesso se la pagina Web non può essere classificata.
Consenti l'accesso a risorse Web legittime che possono essere utilizzate per danneggiare un dispositivo protetto	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security consente l'accesso a risorse Web legittime che possono essere utilizzate per danneggiare il dispositivo protetto.
Consenti l'accesso alla pubblicità legittima	*(la migrazione non viene effettuata)* È possibile gestire l'accesso agli annunci legittimi utilizzando la categoria di risorse Web *Banner* nelle impostazioni di controllo Web.
Modalità operativa: • **Intercettore driver** • **Redirector** • **Proxy esterno**	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security supporta solo la modalità Intercettore driver.
Impostazioni di connessione al servizio ICAP	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non supporta ICAP Network Storage Protection.
Controlla le connessioni protette tramite il protocollo HTTPS	Modalità **Esegui scansione delle connessioni criptate/Esamina sempre le connessioni criptate** (sottosezione **Impostazioni di rete**)

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Usa la versione del protocollo TLS	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security esamina il traffico di rete criptato trasmesso tramite i seguenti protocolli: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. È inoltre possibile bloccare le connessioni SSL 2.0 nelle impostazioni di scansione delle connessioni criptate.
Non considerare attendibili i server Web con un certificato non valido	**Indirizzo** (sottosezione **Impostazioni di rete**)
Porte da intercettare (Area di intercettazione)	**Porte monitorate** (sottosezione **Impostazioni di rete**) Durante la migrazione, KES deseleziona le caselle di controllo **Monitora tutte le porte per le applicazioni dell'elenco consigliato da Kaspersky** e **Monitora tutte le porte per le applicazioni specificate**.
Porte da escludere (Area di intercettazione)	*(la migrazione non viene effettuata)*
Indirizzi IP da escludere (Area di intercettazione)	**Configura indirizzi attendibili** (sottosezione **Impostazioni di rete**)
Processi da escludere (Area di intercettazione)	**Configura applicazioni attendibili** (sottosezione **Impostazioni di rete**) Durante la migrazione, KES configura le seguenti impostazioni per l'applicazione attendibile: • Selezionare la casella di controllo **Non esaminare il traffico di rete**. KES non analizza il traffico di rete di porte e indirizzi IP remoti. • Le altre caselle di controllo nelle impostazioni dell'applicazione attendibile vengono deselezionate.
Porta di sicurezza	*(la migrazione non viene effettuata)*
Usa il database degli URL dannosi per analizzare i collegamenti Web	**Verifica l'indirizzo Web a fronte del database degli indirizzi Web dannosi** (sottosezione **Protezione minacce Web**)
Usa il database anti-phishing per analizzare le pagine Web	**Verifica l'indirizzo Web a fronte del database degli indirizzi Web di phishing** (sottosezione **Protezione minacce Web**)
Usa KSN per la protezione	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza KSN per tutti i componenti dell'applicazione.
Usa Zona attendibile	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security applica l'area attendibile a tutti i componenti. È possibile configurare le esclusioni nelle impostazioni delle aree attendibili.
Usa l'analizzatore euristico	**Usa l'analisi euristica** (sottosezioni **Protezione minacce Web** e **Protezione minacce di posta**)
Livello di sicurezza	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security dispone dei propri livelli di protezione per i componenti Protezione minacce Web e Protezione minacce di posta. Per impostazione predefinita, Kaspersky Endpoint Security imposta il livello di protezione consigliato.
Abilita Protezione minacce di posta	**Protezione minacce di posta** (sottosezione **Protezione minacce di posta**) **Connetti estensione Microsoft Outlook** **Solo messaggi in entrata** (Ambito della protezione) **Scansione alla ricezione** (Protezione e-mail)
Impostazioni di pianificazione	*(la migrazione non viene effettuata)* Non è possibile configurare una pianificazione separata per il componente. Il componente è sempre attivo mentre Kaspersky Endpoint Security è operativo.

Prevenzione Exploit

Le impostazioni di Prevenzione Exploit di KSWS vengono migrate nella sezione **Protezione minacce avanzata**, sottosezione **Prevenzione Exploit**.

Impostazioni di Prevenzione Exploit

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Impedisci l'exploit dei processi vulnerabili: • **Termina in caso di exploit** • **Solo notifica**	**Al rilevamento di exploit**: • **Blocca**. • **Informa**.
Notifica i processi utilizzati in modo improprio tramite Servizio terminal	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non supporta i servizi terminal.
Impedisci l'exploit dei processi vulnerabili anche se Kaspersky Security Service è disabilitato	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security previene costantemente gli exploit dei processi vulnerabili.
Processi protetti	**Abilita protezione della memoria dei processi di sistema** Kaspersky Endpoint Security non supporta la selezione dei processi protetti. È possibile abilitare solo la protezione della memoria dei processi di sistema.
Tecniche di Prevenzione Exploit: • **Applica tutte le tecniche di Prevenzione Exploit disponibili** • **Applica le tecniche di Prevenzione Exploit selezionate**	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security applica tutte le tecniche di prevenzione degli exploit disponibili.

Protezione minacce di rete

Le impostazioni di Protezione minacce di rete di KSWS vengono migrate nella sezione **Protezione minacce essenziale**, sottosezione **Protezione minacce di rete**.

Impostazioni di Protezione minacce di Rete

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Modalità operativa: • **Passante** • **Informa solo sugli attacchi di rete** • **Blocca le connessioni quando viene rilevato un attacco**	**Protezione minacce di rete** Se è selezionata la modalità **Passante**, Protezione minacce di Rete è disabilitata. Se è selezionata la modalità **Informa solo sugli attacchi di rete** o **Blocca le connessioni quando viene rilevato un attacco**, Protezione minacce di Rete è abilitata. Kaspersky Endpoint Security funziona sempre in modalità **Blocca le connessioni quando viene rilevato un attacco**.
Non interrompere l'analisi del traffico quando l'attività non è in esecuzione	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security analizza il traffico in modo continuo se il componente è abilitato.
Non controllare gli indirizzi IP esclusi	**Esclusioni**
Impostazioni di pianificazione	*(la migrazione non viene effettuata)* Non è possibile configurare una pianificazione separata per il componente. Il componente è sempre attivo mentre Kaspersky Endpoint Security è operativo.

Monitoraggio degli script

Kaspersky Endpoint Security non supporta il componente Script Monitoring. Script Monitoring è gestito da altri componenti, ad esempio Protezione AMSI.

Categorie di siti Web

Kaspersky Endpoint Security non supporta tutte le categorie di Kaspersky Security for Windows Server. Le categorie che non esistono in Kaspersky Endpoint Security non vengono migrate. Pertanto, le regole di classificazione delle risorse Web con categorie non supportate non vengono migrate.

Categorie di siti Web

Categorie di Kaspersky Security for Windows Server	Categorie Kaspersky Endpoint Security for Windows
Giochi di guerra	Videogiochi
Aborto	*(la migrazione non viene effettuata)*
Lotterie (estese)	Gioco d'azzardo, lotterie, scommesse

Categorie di Kaspersky Security for Windows Server	Categorie Kaspersky Endpoint Security for Windows
Alcol	Alcolici, tabacco, droghe
Server proxy anonimi	Strumenti di anonimizzazione
Anoressia	*(la migrazione non viene effettuata)*
Affitti immobiliari	*(la migrazione non viene effettuata)*
Audio, video e software	Software, audio, video
Banche	Banche
Blog	Blog
Militari	Armi, esplosivi, contenuti militari
Per bambini	*(la migrazione non viene effettuata)*
Discriminazione	Violenza, intolleranza
Casa e famiglia	*(la migrazione non viene effettuata)*
Servizi di hosting e domini	Comunicazioni di rete
Animali domestici e altri animali	*(la migrazione non viene effettuata)*
Diritto e politica	Vietato dalle leggi regionali
Soggetto a restrizioni da parte di Roskomnadzor (Federazione Russa)	Vietato dalle leggi vigenti nella Federazione russa
Soggetto a restrizioni ai sensi della legge federale 436 (Federazione Russa)	Vietato dalle leggi vigenti nella Federazione russa
Soggetto a restrizioni ai sensi della legislazione della Federazione Russa	Vietato dalle leggi vigenti nella Federazione russa
Soggetto a restrizioni ai sensi della legislazione internazionale	Vietato dalle leggi regionali
Incontri per adulti	Contenuti per adulti
Servizi Internet	*(la migrazione non viene effettuata)*
Sexy shop	Contenuti per adulti
Tecnologie dell'informazione	*(la migrazione non viene effettuata)*
Casinò, giochi di carte	Gioco d'azzardo, lotterie, scommesse
Libri e scrittura	*(la migrazione non viene effettuata)*
Giochi per computer	Videogiochi
Salute e bellezza	*(la migrazione non viene effettuata)*
Cultura e società	*(la migrazione non viene effettuata)*
LGBT	Contenuti per adulti
Lotterie	Gioco d'azzardo, lotterie, scommesse
Medicina	*(la migrazione non viene effettuata)*
Moda	*(la migrazione non viene effettuata)*
Musica	*(la migrazione non viene effettuata)*
Droghe	Alcolici, tabacco, droghe
Violenza	Violenza, intolleranza
Malcontento	*(la migrazione non viene effettuata)*
Droghe illegali	Alcolici, tabacco, droghe
Odio e discriminazione	Violenza, intolleranza
Linguaggio osceno	Espressioni volgari, oscenità
Biancheria intima	Contenuti per adulti
Notizie	Notizie
Nudismo	Contenuti per adulti

Categorie di Kaspersky Security for Windows Server	Categorie Kaspersky Endpoint Security for Windows
Istruzione	*(la migrazione non viene effettuata)*
Acquisti online	Acquisti online
Tutti i mezzi di comunicazione	Comunicazioni di rete
Pagamento con carte di credito	Sistemi di pagamento
Acquisti online (sistema di pagamento proprietario)	Acquisti online
Enciclopedie online	*(la migrazione non viene effettuata)*
Servizi bancari online	Banche
Armi	Armi, esplosivi, contenuti militari
Pesca e caccia	*(la migrazione non viene effettuata)*
Sistemi di pagamento	Sistemi di pagamento
Ricerca di lavoro	Ricerca di lavoro
Motori di ricerca	*(la migrazione non viene effettuata)*
Decisione della polizia (JP)	Vietato dalla polizia del Giappone
Considerato attendibile da KPSN	*(la migrazione non viene effettuata)*
Considerato non attendibile da KPSN	*(la migrazione non viene effettuata)*
Pornografia	Contenuti per adulti
Hosting multimediale e streaming	Notizie
Posta Web	E-mail basata sul Web
Viaggi	*(la migrazione non viene effettuata)*
TV e radio	Notizie
Servizi di teaser e pubblicità	Banner
Religione	Religioni, associazioni religiose
Ristoranti, bar e cibo	*(la migrazione non viene effettuata)*
Siti di incontri	Siti di incontri
Educazione sessuale	Contenuti per adulti
Social network	Social network
Sport	*(la migrazione non viene effettuata)*
Scommesse	Gioco d'azzardo, lotterie, scommesse
Suicidio	Violenza, intolleranza
Tabacco	Alcolici, tabacco, droghe
Torrent	Torrent
Incluso nell'elenco federale degli estremisti (RF)	Vietato dalle leggi vigenti nella Federazione russa
Condivisione di file	Condivisione file
Farmacia	*(la migrazione non viene effettuata)*
Hobby e intrattenimento	*(la migrazione non viene effettuata)*
Chat e forum	Chat, forum, messaggistica istantanea
Pagine di scuole e università	*(la migrazione non viene effettuata)*
Astrologia ed esoterismo	*(la migrazione non viene effettuata)*
Estremismo e razzismo	Violenza, intolleranza
Commercio elettronico	Acquisti online

Categorie di Kaspersky Security for Windows Server	Categorie Kaspersky Endpoint Security for Windows
Erotismo	Contenuti per adulti
Umorismo	*(la migrazione non viene effettuata)*

Controllo delle attività locali

Controllo degli avvii delle applicazioni

Le impostazioni di Controllo applicazioni di KSWS vengono migrate nella sezione **Controlli di sicurezza**, sottosezione **Controllo applicazioni**.

Impostazioni di Controllo degli avvii delle applicazioni

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Modalità operativa: • **Solo statistiche** • **Attivo**	**Action** (Application Control): • **Testa regole**. • **Applica regole**.
Ripetere l'azione eseguita al primo avvio del file per tutti gli avvii successivi dello stesso file	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security esamina l'applicazione ogni volta che tenta di eseguirla.
Impedire l'avvio degli interpreti dei comandi senza un comando da eseguire	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security consente l'esecuzione di interpreti di comando se non sono vietati da Controllo applicazioni.
Regole	**Regole di Controllo applicazioni** *(supportate con limitazioni)* Kaspersky Endpoint Security 11.11.0 introduce il supporto per la migrazione delle regole di Applications Launch Control. La funzionalità di migrazione delle regole di Applications Launch Control presenta alcune limitazioni. Per impostazione predefinita, KSWS Applications Launch Control include due regole: • **Consenti script e pacchetti MSI con certificato considerato attendibile dal sistema operativo** • **Consenti file eseguibili con certificato considerato attendibile dal sistema operativo** Se almeno una regola di KSWS di origine è di tipo **Consenti**, durante la migrazione KES crea una nuova regola di autorizzazione: **Applicazioni con certificati radice attendibili**. In altre parole, Controllo applicazioni di KES utilizza un'unica regola per consentire l'esecuzione degli script, dei pacchetti MSI e dei file eseguibili attendibili. Se entrambe le regole di KSWS di origine sono di tipo **Nega**, KES non aggiunge regole per la gestione delle applicazioni con certificati radice attendibili.
Applicare le regole ai file eseguibili	*(la migrazione non viene effettuata)* L'ambito dell'applicazione della regola non può essere configurato nelle impostazioni di Controllo applicazioni di KES. Controllo applicazioni di KES applica regole a tutti i tipi di file: file eseguibili, script e pacchetti MSI. Se tutti i tipi di file sono inclusi nell'ambito dell'applicazione delle regole in KSWS, durante la migrazione KES trasferisce le regole KSWS. Se un tipo di file viene escluso dall'ambito dell'applicazione delle regole in KSWS, durante la migrazione KES trasferisce anche le regole KSWS, ma **Testa regole** viene selezionato come azione di Controllo applicazioni.
Monitorare il caricamento dei moduli DLL	**Monitora il caricamento dei moduli DLL (aumenta notevolmente il carico sul sistema)**
Applicare le regole agli script e ai pacchetti MSI	*(la migrazione non viene effettuata)* L'ambito dell'applicazione della regola non può essere configurato nelle impostazioni di Controllo applicazioni di KES. Controllo applicazioni di KES applica regole a tutti i tipi di file: file eseguibili, script e pacchetti MSI. Se tutti i tipi di file sono inclusi nell'ambito dell'applicazione delle regole in KSWS, durante la migrazione KES trasferisce le regole KSWS. Se un tipo di file viene escluso dall'ambito dell'applicazione delle regole in KSWS, durante la migrazione KES trasferisce le regole KSWS, ma **Testa regole** viene selezionato come azione di Controllo applicazioni.
Nega le applicazioni considerate non attendibili da KSN	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non tiene conto della reputazione delle applicazioni e consente o nega l'esecuzione delle applicazioni in conformità alle regole.
Consenti le applicazioni considerate attendibili da KSN	Durante la migrazione, KES aggiunge una nuova regola di autorizzazione. La categoria **Altro software\Applicazioni attendibili in base alla reputazione in KSN** è specificata come condizione di attivazione della regola.

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Utenti e/o gruppi di utenti autorizzati a eseguire applicazioni considerate attendibili da KSN	**Utenti e relativi diritti** in una regola di autorizzazione di Controllo applicazioni che include la categoria KL **Altro software\Applicazioni attendibili in base alla reputazione in KSN**.
Consenti automaticamente la distribuzione del software tramite le applicazioni e i pacchetti elencati	Il controllo della distribuzione del software Distribution Control in KSWS e KES funziona in modo diverso. Durante la migrazione, KES aggiunge nuove regole di autorizzazione per le applicazioni per le quali è consentita la distribuzione automatica del software. L'hash del file è specificato come condizione di attivazione della regola.
Consenti sempre la distribuzione del software tramite Windows Installer	Il controllo della distribuzione del software Distribution Control in KSWS e KES funziona in modo diverso. Durante la migrazione, KES aggiunge nuove regole di autorizzazione per le applicazioni per le quali è consentita la distribuzione automatica del software (**Applicazioni e pacchetti di distribuzione software consentiti**). L'hash del file è specificato come condizione di attivazione della regola. Nelle proprietà dell'account, la casella di controllo **Programmi di aggiornamento attendibili** è selezionata.
Consenti sempre la distribuzione del software tramite SCCM utilizzando il Servizio trasferimento intelligente in background	*(la migrazione non viene effettuata)*
Applicazioni e pacchetti di distribuzione software consentiti	Il controllo della distribuzione del software Distribution Control in KSWS e KES funziona in modo diverso. Durante la migrazione, KES aggiunge nuove regole di autorizzazione per le applicazioni per le quali è consentita la distribuzione automatica del software. L'hash del file è specificato come condizione di attivazione della regola. Nelle proprietà dell'account, la casella di controllo **Programmi di aggiornamento attendibili** è selezionata.
Impostazioni di pianificazione	*(la migrazione non viene effettuata)* Se una pianificazione è configurata per il componente nelle impostazioni di KSWS, il componente Controllo applicazioni viene abilitato al momento della migrazione. Se una pianificazione non è configurata per il componente nelle impostazioni di KSWS, Controllo applicazioni viene disabilitato al momento della migrazione. Non è possibile configurare una pianificazione separata per il componente. Il componente è sempre attivo mentre Kaspersky Endpoint Security è operativo.

Controllo dispositivi

Le impostazioni di Controllo dispositivi di KSWS vengono migrate nella sezione **Controlli di sicurezza**, sottosezione Controllo dispositivi.

Impostazioni di Controllo dispositivi

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Modalità operativa: • **Attivo** • **Solo statistiche**	*(la migrazione non viene effettuata)* Controllo Applicazioni viene eseguito in modalità *Attiva*. Le statistiche di connessione dei dispositivi sono fornite continuamente da Controllo.
Consenti l'utilizzo di tutti i dispositivi esterni quando l'attività Controllo dispositivi non è in esecuzione	*(la migrazione non viene effettuata)* Controllo dispositivi è sempre attivo quando Kaspersky Endpoint Security è in esecuzione.
Regole di Controllo dispositivi	**Dispositivi attendibili** Durante la migrazione, Kaspersky Endpoint Security ignora le regole di KSWS disabilitate.
Impostazioni di pianificazione	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza la propria pianificazione per accedere a determinati tipi di dispositivi.

Protezione degli archivi collegati alla rete

Protezione dell'archivio di rete RPC

Kaspersky Endpoint Security non supporta i componenti di Network Storage Protection. Se questi componenti sono necessari, è possibile continuare a utilizzare Kaspersky Security for Windows Server.

Protezione dell'archivio di rete ICAP

Kaspersky Endpoint Security non supporta i componenti di Network Storage Protection. Se questi componenti sono necessari, è possibile continuare a utilizzare Kaspersky Security for Windows Server.

Anti-Cryptor per NetApp

Kaspersky Endpoint Security non supporta Anti-Cryptor for NetApp. La funzionalità Anti-Cryptor è fornita da altri componenti dell'applicazione, ad esempio Rilevamento del Comportamento.

Controllo dell'attività di rete

Gestione firewall

Kaspersky Endpoint Security non supporta la gestione dei firewall di KSWS. La funzioni dei firewall di KSWS vengono eseguite dal firewall a livello di sistema. Dopo la migrazione, è possibile configurare il firewall di Kaspersky Endpoint Security.

Anti-Cryptor

Le impostazioni Anti-Cryptor di rete vengono migrate nella sezione **Protezione minacce avanzata**, sottosezione **Rilevamento del Comportamento**.

Impostazioni di Anti-Cryptor

Impostazioni di KSWS	Impostazioni di KES
Modalità operativa: • **Solo statistiche** • **Attivo**	**Al rilevamento del criptaggio esterno delle cartelle condivise**: • **Informa**. • **Blocca**.
Analizzatore euristico	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non utilizza l'analisi euristica per il Rilevamento del Comportamento.
Configurazione dell'ambito della protezione: • **Tutte le cartelle di rete condivise nel dispositivo protetto** • **Solo le cartelle condivise specificate**	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security impedisce la crittografia di tutte le cartelle di rete condivise del computer protetto.
Esclusioni	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security dispone di esclusioni proprie per il componente Rilevamento del Comportamento. Dopo la migrazione, è possibile aggiungere le esclusioni manualmente.
Impostazioni di pianificazione	*(la migrazione non viene effettuata)* Non è possibile configurare una pianificazione separata per il componente. Il componente è sempre attivo mentre Kaspersky Endpoint Security è operativo.

Ispezione sistema

Monitoraggio integrità file

Le impostazioni di Monitoraggio integrità file da KSWS vengono migrate alla sezione **Controlli di sicurezza**, sottosezione **Monitoraggio integrità di sistema**.

Impostazioni di Monitoraggio integrità file

Impostazioni di KSWS	Impostazioni di KES
Registra le informazioni sulle operazioni sui file eseguite durante il periodo di interruzione del monitoraggio	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non registra gli eventi per le operazioni file eseguite durante il periodo di interruzione del monitoraggio.
Blocca i tentativi di compromettere il registro USN	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non blocca i tentativi di compromissione del registro USN.
Ambito del monitoraggio	**Ambito del monitoraggio → File** *(supportate con limitazioni)* I record dell'ambito di monitoraggio disabilitati non vengono migrati in KES. Kaspersky Endpoint Security aggiunge solo i record abilitati all'ambito di monitoraggio.
Utenti attendibili	**Utenti e/o gruppi di utenti attendibili**
Indicatori di operazione sul file	**Marcatori operazioni sul file**
Calcola il checksum del file, se possibile	**Hashing**
Esclusioni	**Esclusioni → File**

Log Inspection

Le impostazioni di Log Inspection di KSWS vengono migrate nella sezione **Controlli di sicurezza**, sottosezione **Log Inspection**.

Impostazioni di Log Inspection

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Applica regole personalizzate per Log Inspection	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security applica tutte le regole personalizzate abilitate.
Regole personalizzate	**Regole personalizzate** La regola predefinita **Un servizio è stato installato nel sistema (per il sistema operativo Server 2003)** non viene migrata in KES.
Applica regole predefinite per Log Inspection	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security applica tutte le regole predefinite abilitate.
Regole predefinite	**Regole predefinite**
Rilevamento forza bruta password	**Rilevamento di attacco di forza bruta**
Rilevamento degli accessi di rete	**Rilevamento degli accessi di rete**
Esclusioni (indirizzi IP)	**Esclusioni** (Indirizzo IP)
Esclusioni (utenti)	**Esclusioni** (Utenti)
Impostazioni di pianificazione	*(la migrazione non viene effettuata)* Non è possibile configurare una pianificazione separata per il componente. Il componente è sempre attivo mentre Kaspersky Endpoint Security è operativo.

Registri e notifiche

Registri delle attività

Le impostazioni dei registri di KSWS sono state spostate nella sezione **Impostazioni generali** e nelle sottosezioni Interfaccia e Rapporti e archivi.

Impostazioni dei registri

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Registrazione degli eventi	**Notifiche** (sottosezione **Interfaccia**)
Cartella dei registri	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security salva i rapporti nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.
Rimuovi i registri delle attività più vecchi di N giorni	*(la migrazione non viene effettuata)* È possibile configurare il periodo di archiviazione dei rapporti di KES in **Impostazioni generali**, **Rapporti e archivi**.
Rimuovi dal registro di controllo gli eventi dopo N giorni	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security applica le limitazioni di archiviazione dei rapporti a tutti i rapporti, inclusi quelli di controllo del sistema.
Integrazione di SIEM	*(la migrazione non viene effettuata)* È possibile configurare l'integrazione SIEM in Kaspersky Security Center.

Notifiche degli eventi

Le impostazioni delle notifiche di KSWS vengono migrate nella sezione **Impostazioni generali**, sottosezione Interfaccia.

Impostazioni di notifica

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Notifiche	**Notifiche**
Avvisa gli utenti: • **Tramite il servizio Terminal** • **Tramite il comando del servizio Windows Messenger**	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non supporta la modifica del testo delle notifiche. Kaspersky Endpoint Security mostra notifiche standard.
Avvisa gli amministratori: • **Tramite il comando del servizio Windows Messenger** • **Tramite l'esecuzione di un file eseguibile** • **Tramite e-mail**	Solo le impostazioni delle notifiche via e-mail vengono migrate in Kaspersky Endpoint Security – **Impostazioni delle notifiche via e-mail** (blocco **Notifiche**). Non sono supportati altri metodi di notifica per gli amministratori.
Il database dell'applicazione non è aggiornato	**Invia la notifica "I database non sono aggiornati" se i database non sono stati aggiornati**
Il database dell'applicazione è estremamente obsoleto	**Invia la notifica "I database non sono aggiornati da tempo" se i database non sono stati aggiornati**
La scansione delle aree critiche non viene eseguita da molto tempo	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security genera un evento di scansione delle aree critiche non effettuato dopo tre giorni.

Interazione con Administration Server

Le impostazioni delle interazioni di Administration Server di KSWS vengono migrate nella sezione **Impostazioni generali**, sottosezione Rapporti e archivi.

Administration Server interaction settings

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
File in quarantena	**File in quarantena**
File sottoposti a backup	**File di backup**
Host bloccati	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security invia automaticamente i dati sugli host bloccati.

Attività

Attivazione dell'applicazione

Kaspersky Endpoint Security non supporta l'attività *Attivazione dell'applicazione* (KSWS). È possibile creare un'attività *Aggiungi chiave* (KES), aggiungere una chiave di licenza al pacchetto di installazione o abilitare la distribuzione automatica delle chiavi di licenza.

Copia degli aggiornamenti

Le impostazioni dell'attività *Copia degli aggiornamenti* (KSWS) vengono migrate nell'attività *Aggiornamento di database e moduli dell'applicazione* (KES).

Impostazioni di Copying Updates

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Sorgente degli aggiornamenti: • **Kaspersky Security Center Administration Server** • **Server di aggiornamento Kaspersky** • **Server HTTP o FTP personalizzati oppure cartelle di rete**	**Sorgente degli aggiornamenti**: • **Kaspersky Security Center**. • **Server degli aggiornamenti Kaspersky**. • **Specificato dall'utente**.
Utilizzare i server di aggiornamento Kaspersky se i server specificati non sono disponibili	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security consente di selezionare più sorgenti degli aggiornamenti, inclusi i server degli aggiornamenti Kaspersky. Se la prima sorgente degli aggiornamenti non è disponibile, Kaspersky Endpoint Security consente di recuperare gli aggiornamenti da un'altra sorgente nell'elenco.
Utilizzare le impostazioni del server proxy per connettersi ai server di aggiornamento Kaspersky	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza il server proxy per tutti i componenti. È possibile configurare la connessione al server proxy nelle opzioni di rete dell'applicazione.
Utilizzare le impostazioni del server proxy per connettersi ad altri server	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza il server proxy per tutti i componenti. È possibile configurare la connessione al server proxy nelle opzioni di rete dell'applicazione.
Impostazioni di copia degli aggiornamenti: • **Copiare gli aggiornamenti del database** • **Copiare gli aggiornamenti critici dei moduli software** • **Copiare gli aggiornamenti del database e gli aggiornamenti critici dei moduli dell'applicazione**	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security copia gli aggiornamenti del database e gli aggiornamenti critici dei moduli dell'applicazione come un unico pacchetto.
Cartella per l'archivio locale degli aggiornamenti copiati	**Copia aggiornamenti nella cartella**

Monitoraggio integrità file baseline

Le impostazioni dell'attività *Monitoraggio integrità file baseline* (KSWS) vengono migrate nell'attività *Controllo integrità di sistema* e nella sezione del criterio **Controlli di sicurezza**, sottosezione **Monitoraggio integrità di sistema**.

Impostazioni dell'attività Baseline File Integrity Monitor

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Algoritmo di calcolo dell'hash: • **MD5** • **SHA256**.	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza l'algoritmo SHA256 per il calcolo del checksum.
Ambito della scansione	**Ambito del monitoraggio** (sottosezione **Monitoraggio integrità di sistema**)

Aggiornamento database

Le impostazioni dell'attività *Aggiornamento database* (KSWS) vengono migrate nell'attività *Aggiornamento di database e moduli dell'applicazione* (KES).

Impostazioni dell'attività Database Update

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Sorgente degli aggiornamenti: • **Kaspersky Security Center Administration Server** • **Server di aggiornamento Kaspersky** • **Server HTTP o FTP personalizzati oppure cartelle di rete**	**Sorgente degli aggiornamenti**: • **Kaspersky Security Center**. • **Server degli aggiornamenti Kaspersky**. • **Specificato dall'utente**.
Utilizzare i server di aggiornamento Kaspersky se i server specificati non sono disponibili	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security consente di selezionare più sorgenti degli aggiornamenti, inclusi i server degli aggiornamenti Kaspersky. Se la prima sorgente degli aggiornamenti non è disponibile, Kaspersky Endpoint Security consente di recuperare gli aggiornamenti da un'altra sorgente nell'elenco.
Utilizzare le impostazioni del server proxy per connettersi ai server di aggiornamento Kaspersky	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza il server proxy per tutti i componenti. È possibile configurare la connessione al server proxy nelle opzioni di rete dell'applicazione.
Utilizzare le impostazioni del server proxy per connettersi ad altri server	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza il server proxy per tutti i componenti. È possibile configurare la connessione al server proxy nelle opzioni di rete dell'applicazione.
Ridurre il carico sull'I/O del disco	*(la migrazione non viene effettuata)*

Aggiornamenti dei moduli software

Le impostazioni dell'attività *Aggiornamento moduli software* (KSWS) vengono migrate nell'attività *Aggiornamento di database e moduli dell'applicazione* (KES).

Impostazioni dell'attività Software Modules Update

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Sorgente degli aggiornamenti: • **Kaspersky Security Center Administration Server** • **Server di aggiornamento Kaspersky** • **Server HTTP o FTP personalizzati oppure cartelle di rete**	**Sorgente degli aggiornamenti**: • **Kaspersky Security Center**. • **Server degli aggiornamenti Kaspersky**. • **Specificato dall'utente**.
Utilizzare i server di aggiornamento Kaspersky se i server specificati non sono disponibili	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security consente di selezionare più sorgenti degli aggiornamenti, inclusi i server degli aggiornamenti Kaspersky. Se la prima sorgente degli aggiornamenti non è disponibile, Kaspersky Endpoint Security consente di recuperare gli aggiornamenti da un'altra sorgente nell'elenco.

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Utilizzare le impostazioni del server proxy per connettersi ai server di aggiornamento Kaspersky	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza il server proxy per tutti i componenti. È possibile configurare la connessione al server proxy nelle opzioni di rete dell'applicazione.
Utilizzare le impostazioni del server proxy per connettersi ad altri server	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security utilizza il server proxy per tutti i componenti. È possibile configurare la connessione al server proxy nelle opzioni di rete dell'applicazione.
Copiare e installare gli aggiornamenti critici dei moduli software	**Installa aggiornamenti critici e approvati**
Verificare solo la disponibilità di aggiornamenti software critici	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security controlla continuamente la disponibilità di aggiornamenti critici per i moduli delle applicazioni.
Consentire il riavvio del sistema operativo	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security richiede all'utente l'autorizzazione per riavviare il computer.
Ricevere informazioni sugli aggiornamenti pianificati disponibili dei moduli software	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security mostra le notifiche sugli aggiornamenti dei moduli software.

Rollback dell'aggiornamento dei database dell'applicazione

Le impostazioni dell'attività *Rollback dell'aggiornamento dei database dell'applicazione* (KSWS) vengono migrate nell'attività *Rollback degli aggiornamenti* (KES). La nuova attività *Rollback degli aggiornamenti* (KES) ha una pianificazione di avvio delle attività: *Manualmente*.

Scansione su richiesta

Le impostazioni dell'attività *Scansione su richiesta* (KSWS) vengono migrate nell'attività *Scansione malware* (KES).

Impostazioni dell'attività Scansione virus

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Ambito della scansione	**Ambito della scansione**
Livello di protezione: • **Massima protezione** • **Consigliati** • **Massime prestazioni**	**Livello di sicurezza**: • **Alto**. • **Consigliato**. • **Basso**. Le impostazioni dei livelli di sicurezza differiscono in KSWS e KES.
Oggetti da esaminare: • **Tutti gli oggetti** • **Oggetti esaminati in base al formato** • **Oggetti esaminati in base all'elenco delle estensioni specificate nel database anti-virus** • **Oggetti esaminati in base all'elenco di estensioni specificato**	**Tipi di file**: • **Tutti i file**. • **File esaminati per formato**. • **File esaminati per estensione**. Kaspersky Endpoint Security non consente la creazione di elenchi di estensioni personalizzati. Kaspersky Endpoint Security sostituisce il valore **Oggetti esaminati in base all'elenco di estensioni specificato** con il valore **File esaminati per estensione**.
Sottocartelle	**Includi sottocartelle**
Sottofile	*(la migrazione non viene effettuata)*
Eseguire la scansione dei settori di avvio del disco e dell'MBR	*(la migrazione non viene effettuata)*
Eseguire la scansione dei flussi NTFS alternativi	*(la migrazione non viene effettuata)*
Eseguire la scansione solo dei file nuovi e modificati	**Esamina solo i file nuovi e modificati**
Scansione degli oggetti composti: • **Tutti gli archivi** • **Tutti gli archivi SFX** • **Tutti i database di posta elettronica** • **Tutti gli oggetti compressi** • **Tutti i messaggi di posta elettronica in testo normale** • **Tutti gli oggetti OLE incorporati**	**Scansione dei file compositi**: • **Esamina gli archivi**. • **Esamina gli archivi protetti da password**. • **Esamina i pacchetti di distribuzione**. • **Esamina i file in formato e-mail**. • **Esamina i file nei formati Microsoft Office**.

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Azione da eseguire sugli oggetti infetti e sugli altri oggetti: • **Disinfetta** • **Disinfetta. Rimuovi se la disinfezione non riesce** • **Rimuovi** • **Eseguire l'azione consigliata** • **Solo notifica**	**Azione se viene rilevata una minaccia**: • **Disinfetta (se non è possibile, elimina)**. • **Disinfetta (se la disinfezione non riesce, informa)**. • **Informa**.
Azione da eseguire sugli oggetti probabilmente infetti: • **Quarantena** • **Rimuovi** • **Eseguire l'azione consigliata** • **Solo notifica**	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security applica l'azione se viene rilevata una minaccia.
Eseguire le azioni in base al tipo di oggetto rilevato	*(la migrazione non viene effettuata)*
Rimuovere completamente il file composto che non può essere modificato dall'applicazione in caso di rilevamento di un oggetto incorporato	*(la migrazione non viene effettuata)*
Escludi file	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security applica l'area attendibile a tutti i componenti. È possibile configurare le esclusioni nelle impostazioni delle aree attendibili.
Non rilevare	*(la migrazione non viene effettuata)*
Interrompere la scansione se richiede più di N sec	**Ignora i file esaminati per più di N sec**
Non eseguire la scansione degli oggetti composti di dimensioni superiori a N MB	**Non decomprimere i file compositi di grandi dimensioni**
Utilizzare la tecnologia iSwift	**Tecnologia iSwift**
Utilizzare la tecnologia iChecker	**Tecnologia iChecker**
Azione sui file offline: • **Non eseguire scansione** • **Eseguire la scansione solo della parte residente del file** • **Eseguire la scansione dell'intero file** • **Solo se è stato effettuato l'accesso al file entro il periodo specificato (giorni)** • **Non copiare il file su un disco rigido locale, se possibile**	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security esamina i file offline nella loro interezza.

Controllo dell'integrità dell'applicazione

Le impostazioni dell'attività *Controllo integrità applicazioni* (KSWS) vengono migrate nell'attività *Controllo integrità applicazione* (KES).

Generatore di regole per Controllo avvio applicazioni

Kaspersky Endpoint Security non supporta l'attività *Generatore di regole per Controllo avvio applicazioni*. È possibile generare le regole nelle impostazioni di Controllo applicazioni.

Generatore di regole per Controllo dispositivi

Kaspersky Endpoint Security non supporta l'attività *Generatore di regole per Controllo dispositivi*. È possibile generare le regole nelle impostazioni di Controllo dispositivi.

Migrazione dei componenti di KSWS

Prima dell'installazione locale, Kaspersky Endpoint Security verifica la presenza di applicazioni Kaspersky nel computer. Se Kaspersky Security for Windows Server è installato nel computer, KES rileva la serie di componenti di KSWS installati e seleziona gli stessi componenti per l'installazione.

La corrispondenza dei componenti di KSWS e KES è riportata di seguito:

- Protezione AMSI, Prevenzione Intrusioni Host, Motore di Remediation vengono installate con le impostazioni predefinite.
- I componenti Prevenzione Attacchi BadUSB, Controllo adattivo delle anomalie, Criptaggio dei dati e Detection and Response vengono ignorati.

Se installata in remoto, l'applicazione KES ignora il set dei componenti installati di KSWS. Il programma di installazione installa i componenti selezionati nelle proprietà del pacchetto di installazione. Dopo aver installato Kaspersky Endpoint Security e aver migrato i criteri e le attività, le impostazioni KES vengono configurate in base alle impostazioni di KSWS.

Migrazione delle attività e dei criteri di KSWS

È possibile eseguire la migrazione delle impostazioni di criteri e attività di KSWS nei seguenti modi:

- Utilizzando la procedura Conversione guidata criteri e attività (di seguito definita anche "migrazione guidata").

  > La migrazione guidata di KSWS è disponibile solo in Administration Console (MMC). Non è possibile migrare le impostazioni dei criteri e delle attività in Web Console e Cloud Console.

  La Conversione guidata in batch funziona in modo diverso per le diverse versioni di Kaspersky Security Center. Si consiglia di effettuare l'upgrade della soluzione alla versione 14.2 o successiva. In questa versione di Kaspersky Security Center, la Conversione guidata di criteri e attività in batch consente di eseguire la migrazione dei criteri in un profilo anziché in un criterio. In questa versione di Kaspersky Security Center, la Conversione guidata di criteri e attività in batch consente inoltre di eseguire la migrazione di una gamma più ampia di impostazioni dei criteri.

- Utilizzando Creazione guidata nuovo criterio per Kaspersky Endpoint Security for Windows.

  Creazione guidata nuovo criterio consente di creare un criterio di KES basato su un criterio di KSWS.

Le procedure di migrazione dei criteri di KSWS sono diverse quando si utilizza Migrazione guidata e Creazione guidata nuovo criterio.

Conversione guidata di criteri e attività in batch

La migrazione guidata trasferisce le impostazioni dei criteri di KSWS nel profilo dei criteri anziché le impostazioni dei criteri di KES. Il *profilo dei criteri* è un set di impostazioni dei criteri che viene attivato in un computer se il computer soddisfa le regole di attivazione configurate. Il tag del dispositivo `UpgradedFromKSWS` viene selezionato come criterio di attivazione del profilo dei criteri. Kaspersky Security Center aggiunge automaticamente il tag `UpgradedFromKSWS` a tutti i computer in cui si installa KES oltre a KSWS utilizzando l'attività di installazione remota. Se è stato scelto un altro metodo di installazione, è possibile assegnare il tag ai dispositivi manualmente.

Per aggiungere un tag a un dispositivo:

1. Creare un nuovo tag per i server - `UpgradedFromKSWS`.

   Per informazioni dettagliate sulla creazione di tag per i dispositivi, consultare la Guida di Kaspersky Security Center.

2. Creare un nuovo gruppo di amministrazione nella console di Kaspersky Security Center e aggiungere i server a cui si desidera assegnare il tag a questo gruppo.

   È possibile raggruppare i server utilizzando lo strumento di selezione. Per informazioni dettagliate sulle selezioni, consultare la Guida di Kaspersky Security Center.

3. Selezionare tutti i server del gruppo di amministrazione nella console di Kaspersky Security Center, aprire le proprietà dei server selezionati e assegnare il tag.

Se si esegue la migrazione di più criteri KSWS, ogni criterio viene convertito in un profilo all'interno di un criterio generale. Se il criterio KSWS contiene già profili, anche questi profili vengono migrati come profili. Di conseguenza, si otterrà un unico criterio che include i profili corrispondenti a tutti i criteri di KSWS.

Come utilizzare Conversione guidata criteri e attività per migrare le impostazioni dei criteri di KSWS

1. In Administration Console, selezionare Administration Server e fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.

2. Selezionare **Tutte le attività** → **Conversione guidata in batch criteri e attività**.

Viene avviata la procedura Conversione guidata criteri e attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione dell'applicazione con cui è necessario convertire i criteri e le attività

In questa fase, è necessario selezionare Kaspersky Endpoint Security for Windows. Procedere con il passaggio successivo.

Passaggio 2. Conversione dei criteri

La migrazione guidata crea i profili dei criteri di KSWS all'interno di un criterio di KES. Selezionare i criteri di Kaspersky Security for Windows Server che si desidera convertire in profili dei criteri. Procedere con il passaggio successivo.

A questo punto, la migrazione guidata inizia a convertire i criteri. I nomi dei nuovi profili dei criteri corrisponderanno ai criteri originali di KSWS.

Passaggio 3. Rapporto sulla migrazione dei criteri

La migrazione guidata crea un rapporto sulla migrazione dei criteri. Il rapporto sulla migrazione dei criteri contiene la data e l'ora di conversione dei criteri, il nome del criterio originale di KSWS, il nome del criterio di KES di destinazione e il nome del nuovo profilo dei criteri.

Passaggio 4. Conversione delle attività

La migrazione guidata crea nuove attività per Kaspersky Endpoint Security for Windows. Nell'elenco delle attività, selezionare le attività di KSWS che si desidera creare per Kaspersky Endpoint Security. Le nuove attività verranno denominate *<nome attività KSWS> (convertito)*. Procedere con il passaggio successivo.

Passaggio 5. Completamento della procedura guidata

Terminare la procedura guidata. Di conseguenza, la procedura guidata esegue le seguenti operazioni:

- I nuovi profili dei criteri vengono aggiunti al criterio di Kaspersky Endpoint Security.

  Il criterio include i profili con le impostazioni di Kaspersky Security for Windows Server. Il nuovo criterio presenta lo stato *Attivo*. La procedura guidata lascia invariati i criteri di KSWS.

- Crea nuove attività di Kaspersky Endpoint Security.

  Le nuove attività sono copie delle attività di KSWS. La procedura guidata lascia invariate le attività di KSWS.

Il nuovo profilo dei criteri con le impostazioni di KSWS verrà denominato *UpgradedFromKSWS <Nome del criterio di Kaspersky Security for Windows Server>*. Nelle proprietà del profilo, la migrazione guidata seleziona automaticamente il tag del dispositivo `UpgradedFromKSWS` come criterio di attivazione. Pertanto, le impostazioni del profilo dei criteri vengono applicate automaticamente ai server.

Procedura guidata per la creazione di un criterio basato su un criterio di KSWS

Quando viene creato un criterio di KES basato su un criterio di KSWS, la procedura guidata trasferisce le impostazioni al nuovo criterio di conseguenza. In altre parole, un criterio di KES corrisponderà a un criterio di KSWS. La procedura guidata non converte il criterio in un profilo.

Come utilizzare Creazione guidata nuovo criterio per migrare le impostazioni dei criteri di KSWS

1. Aprire Kaspersky Security Center Administration Console.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console, selezionare la cartella con il nome del gruppo di amministrazione a cui appartengono i computer client desiderati.
3. Nell'area di lavoro, selezionare la scheda **Criteri**.
4. Fare clic su **Nuovo criterio**.

   Verrà avviata la Creazione guidata nuovo criterio.
5. Attenersi alle istruzioni della Creazione guidata nuovo criterio.

Passaggio 1. Selezione dell'applicazione per creare il criterio di gruppo

Selezionare l'applicazione **Kaspersky Endpoint Security for Windows (14.2)**.

Passaggio 2. Denominazione del criterio di gruppo

Immettere un nome per il criterio di gruppo, ad esempio *Criterio per l'ufficio*.

Selezionare la casella di controllo **&Utilizza le impostazioni del criterio per una versione precedente dell'applicazione**. Fare clic su **Sfoglia** e selezionare il criterio di KSWS.

Passaggio 3. Partecipazione a Kaspersky Security Network

Leggere e accettare le condizioni dell'Informativa su Kaspersky Security Network (KSN).

Passaggio 4. Selezione della modalità di utilizzo dell'applicazione nei computer

Selezionare **Modalità standard per proteggere gli host**. Kaspersky Endpoint Security fornisce un criterio comune per tutte le modalità di applicazione e i tipi di sistemi operativi.

È consigliabile utilizzare criteri diversi a seconda delle modalità e dei tipi di sistemi operativi.

Passaggio 5. Importazione delle impostazioni

Questo passaggio è disponibile se si seleziona la configurazione manuale dei criteri al passaggio 4.

È possibile creare un criterio basato sulle impostazioni di Kaspersky Endpoint Security da un file di configurazione CFG. La procedura guidata Nuovo criterio non supporta i file di configurazione criptati. Quando si esporta il file di configurazione, omettere il passaggio relativo al criptaggio del file.

Quando si importa un file di configurazione CFG dell'applicazione, non tutte le impostazioni del criterio sono disponibili per la procedura guidata. Ad esempio, i profili criterio non sono presenti nelle impostazioni dell'applicazione. Se si desidera trasferire tutte le impostazioni e i profili nel criterio, è possibile importare un altro criterio da un file KLP.

Durante l'importazione di un file di configurazione, Kaspersky Endpoint Security non trasferisce le password dei contenitori crittografici. Se si utilizza l'autenticazione bidirezionale durante la connessione ai server, è necessario specificare da zero le password dei contenitori crittografici.

Passaggio 6-10. Configurazione delle impostazioni dei criteri

Questo passaggio è disponibile se si seleziona la configurazione manuale dei criteri al passaggio 4.

Seguire i passaggi per gestire le impostazioni dei criteri.

Passaggio 11. Configurazione dell'area attendibile

Configura l'area attendibile. È possibile aggiungere esclusioni dalla scansione e applicazioni attendibili predefinite. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server. Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono inoltre contribuire a configurare rapidamente Kaspersky Endpoint Security in modalità Light Agent negli ambienti virtuali Citrix e VMware.

Passaggio 12. Selezione dello stato del criterio

- **Attivo**. In seguito alla successiva sincronizzazione, il criterio verrà utilizzato come criterio attivo nel computer.

  Le impostazioni di un criterio attivo vengono salvate nei computer client durante la sincronizzazione. Non è possibile applicare più criteri contemporaneamente in un computer, quindi in ogni gruppo può essere attivo un solo criterio.

- **Inattivo**. Criterio di backup. Se necessario, un criterio inattivo può passare allo stato attivo.

  È possibile creare un numero illimitato di criteri inattivi. Un criterio inattivo non influisce sulle impostazioni dell'applicazione nei computer della rete. I criteri inattivi vengono utilizzati come strumenti preventivi per situazioni di emergenza, ad esempio un attacco virus. Se si verifica un attacco tramite unità flash, è possibile attivare un criterio che blocca l'accesso alle unità flash. In questo caso, il criterio attivo diventa automaticamente inattivo.

- **Fuori sede**. Il criterio viene attivato quando un computer esce dal perimetro di rete dell'organizzazione.

Terminare la procedura guidata.

Configurazione aggiuntiva di criteri e attività dopo la migrazione

KSWS e KES hanno diversi set di componenti e impostazioni dei criteri, quindi dopo la migrazione è necessario verificare che le impostazioni dei criteri soddisfino i requisiti di sicurezza aziendali.

Controllare le seguenti impostazioni dei criteri di base:

- Protezione tramite password. Le impostazioni di protezione tramite password di KSWS non vengono migrate. Kaspersky Endpoint Security dispone di una funzionalità di protezione tramite password integrata. Se necessario, attivare la protezione tramite password e impostare una password.

- Area attendibile. Questi metodi utilizzati da KSWS e KES per la selezione degli oggetti differiscono. Durante la migrazione, KES supporta esclusioni definite come singoli file o percorsi di file/cartelle. Se in KSWS sono configurate esclusioni come aree predefinite o URL di script, tali esclusioni non vengono migrate. Dopo la migrazione, è necessario aggiungere tali esclusioni manualmente.

  Per assicurarsi che Kaspersky Endpoint Security funzioni correttamente sui server, si consiglia di aggiungere i file importanti per il funzionamento del server all'area attendibile. Per i server SQL, è necessario aggiungere file di database MDF e LDF. Per i server Microsoft Exchange, è necessario aggiungere i file CHK, EDB, JRS, LOG e JSL. È possibile utilizzare anche maschere, ad esempio, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  A partire da Kaspersky Endpoint Security 12.6 for Windows, le esclusioni dalle scansioni e le applicazioni attendibili vengono aggiunte all'area attendibile. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server.

- Firewall. La funzioni dei firewall di KSWS vengono eseguite dal firewall a livello di sistema. In KES, un componente separato è responsabile della funzionalità Firewall. Dopo la migrazione, è possibile configurare il firewall di Kaspersky Endpoint Security.

- Kaspersky Security Network. Kaspersky Endpoint Security non supporta la configurazione di KSN per i singoli componenti. Kaspersky Endpoint Security utilizza KSN per tutti i componenti dell'applicazione. Per utilizzare KSN, è necessario accettare i nuovi termini e condizioni dell'Informativa di Kaspersky Security Network.

- Controllo Web. Le regole di blocco per il controllo delle categorie di traffico Web vengono migrate in un'unica regola di blocco in Kaspersky Endpoint Security. Kaspersky Endpoint Security ignora le regole per il controllo delle categorie. Kaspersky Endpoint Security non supporta tutte le categorie di Kaspersky Security for Windows Server. Le categorie che non esistono in Kaspersky Endpoint Security non vengono migrate. Pertanto, le regole di classificazione delle risorse Web con categorie non supportate non vengono migrate. Se necessario, aggiungere le regole di Controllo Web.

- Server proxy. La password di connessione del server proxy non viene migrata. Immettere la password da utilizzare per la connessione manuale al server proxy.

- Schede dei singoli componenti. Kaspersky Endpoint Security non supporta le pianificazioni di configurazione per i singoli componenti. I componenti sono sempre attivi mentre Kaspersky Endpoint Security è operativo.

- Set di componenti. Il set di funzionalità Kaspersky Endpoint Security disponibili dipende dal tipo di sistema operativo: workstation o server. Ad esempio, tra gli strumenti di criptaggio, nei server è disponibile solo Crittografia unità BitLocker.

- Attributo . Lo stato dell'attributo non viene migrato. L'attributo avrà il valore predefinito. Per impostazione predefinita, quasi tutte le impostazioni nel nuovo criterio hanno un divieto applicato alla modifica delle impostazioni nei criteri figlio e nell'interfaccia dell'applicazione locale. L'attributo ha il valore per le impostazioni dei criteri nella sezione **Managed Detection and Response (Industrial CyberSecurity)** e nel gruppo di impostazioni **Assistenza agli utenti** (sezione **Interfaccia**). Se necessario, configurare l'eredità delle impostazioni dal criterio padre.

- Come affrontare le minacce attive. Disinfezione avanzata funziona in modo diverso per le workstation e i server. È possibile configurare la disinfezione avanzata nelle impostazioni dell'attività *Scansione malware* e nelle impostazioni dell'applicazione.

- Upgrade dell'applicazione. Per installare i principali aggiornamenti e patch senza riavviare, è necessario modificare la modalità di upgrade dell'applicazione. Per impostazione predefinita, la funzionalità Installa aggiornamenti delle applicazioni senza riavvio è disabilitata.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security è dotato di un agente integrato per l'utilizzo delle soluzioni Detection and Response. Se necessario, trasferire le impostazioni dei criteri di Kaspersky Endpoint Agent nel criterio di Kaspersky Endpoint Security.

- Attività *Aggiornamento di database e moduli dell'applicazione*. Assicurarsi che le impostazioni dell'attività *Aggiornamento di database e moduli dell'applicazione* siano state migrate correttamente. Anziché le tre attività di KSWS, KES utilizza un'unica attività KES. È possibile ottimizzare le attività *Aggiornamento di database e moduli dell'applicazione* e rimuovere le attività superflue.

- Altre attività. I componenti Controllo applicazioni, Controllo dispositivi e Monitoraggio integrità file funzionano in modo diverso in KSWS e KES. KES non utilizza le attività *Monitoraggio integrità file di base*, *Generatore di Controllo avvio applicazioni* e *Generatore di regole per Controllo dispositivi*. Pertanto, queste attività non vengono migrate. Dopo la migrazione, è possibile configurare i componenti Monitoraggio integrità file, Controllo applicazioni, Controllo dispositivi.

Migrazione della zona attendibile di KSWS

Un'*area attendibile* è un elenco configurato dall'amministratore di sistema di oggetti e applicazioni che non vengono monitorati da Kaspersky Endpoint Security durante l'esecuzione. È possibile eseguire la migrazione degli oggetti della zona attendibile da KSWS a KES utilizzando la *conversione guidata in batch di criteri e attività* o la *procedura guidata per la creazione di un nuovo criterio di KES basato sul criterio di KSWS*. KSWS e KES hanno diversi set di componenti e funzionalità, quindi dopo la migrazione è necessario verificare che le esclusioni soddisfino i requisiti di sicurezza aziendali. Inoltre, i metodi per aggiungere esclusioni alla zona attendibile sono diversi per KES e KSWS. La migrazione guidata non dispone di strumenti per eseguire la migrazione di tutte le esclusioni di KSWS. Questo significa che, dopo la migrazione, sarà necessario aggiungere manualmente alcune esclusioni di KSWS.

Per assicurarsi che Kaspersky Endpoint Security funzioni correttamente sui server, si consiglia di aggiungere i file importanti per il funzionamento del server all'area attendibile. Per i server SQL, è necessario aggiungere file di database MDF e LDF. Per i server Microsoft Exchange, è necessario aggiungere i file CHK, EDB, JRS, LOG e JSL. È possibile utilizzare anche maschere, ad esempio, `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

A partire da Kaspersky Endpoint Security 12.6 for Windows, le esclusioni dalle scansioni e le applicazioni attendibili vengono aggiunte all'area attendibile. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server.

Metodi di creazione di zone attendibili KES e KSWS.

KSWS		KES
Oggetto da esaminare		
• Ambito predefinito	*(la migrazione non viene effettuata)*	
• Disco, cartella o percorso di rete	→	**File o cartella**
• File	→	**File o cartella**
• File script o indirizzo Web	*(la migrazione non viene effettuata)*	
Oggetto rilevato	→	**Tipo di oggetto rilevato**
Processi attendibili	→	**Applicazioni attendibili**

Migrazione degli oggetti

Le esclusioni di KSWS con il metodo **Oggetto da esaminare** selezionato nelle relative proprietà vengono migrate alle esclusioni di KES con il metodo **File o cartella** selezionato nelle relative proprietà, con alcune limitazioni. La migrazione di un'esclusione dipende dal metodo di selezione degli oggetti:

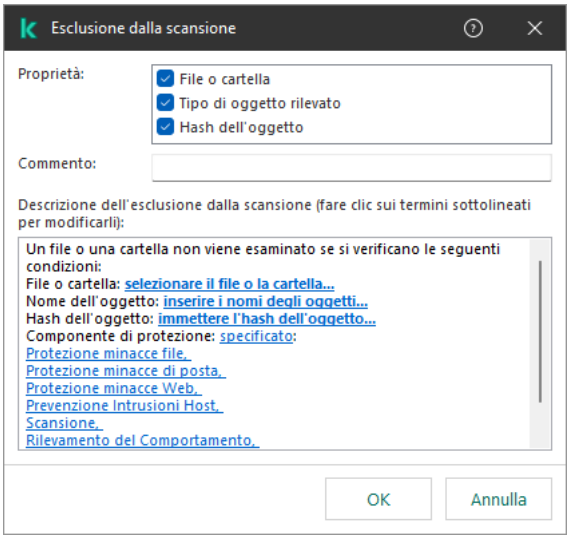
- Ambito predefinito – *non viene migrato*.

  Dopo la migrazione, è necessario aggiungere tali esclusioni manualmente. Le esclusioni come aree predefinite devono essere configurate nelle impostazioni dell'attività *Scansione malware*.

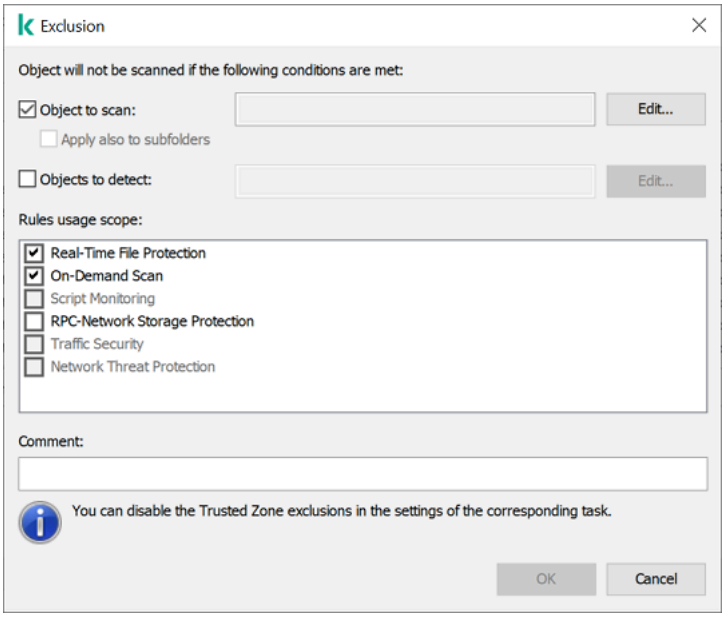
- Disco, cartella o percorso di rete – viene eseguita la migrazione alle esclusioni di KES con il metodo "File o cartella" selezionato nelle proprietà.
- File – viene eseguita la migrazione alle esclusioni di KES con il metodo "File o cartella" selezionato nelle proprietà.
- File script o indirizzo Web – *non viene migrato*.

  Dopo la migrazione, è necessario aggiungere tali esclusioni manualmente. Le esclusioni come indirizzi Web script devono essere aggiunte agli indirizzi Web attendibili per la protezione dalle minacce Web.

Se la casella di controllo **Applica anche alle sottocartelle** è selezionata per l'oggetto esaminato, questa impostazione viene migrata alle esclusioni di KES (la casella di controllo **Includi sottocartelle**).



Impostazioni delle esclusioni di KES



Impostazioni delle esclusioni di KSWS

Migrazione degli oggetti rilevati

Le esclusioni di KSWS con il metodo **Oggetto rilevato** selezionato nelle relative proprietà vengono migrate alle esclusioni di KES con il metodo **Tipo di oggetto rilevato** selezionato nelle relative proprietà. Il nome dell'oggetto rilevato corrisponde alla classificazione dell'Enciclopedia Kaspersky (ad esempio `Email-Worm`, `Rootkit` o `RemoteAdmin`). Kaspersky Endpoint Security supporta le maschere con il punto interrogativo `?` (corrisponde a qualsiasi carattere singolo) e l'asterisco `*` (corrisponde a qualsiasi sequenza di caratteri).

Migrazione dell'ambito di utilizzo delle esclusioni

L'ambito di utilizzo di un'esclusione è un insieme di componenti a cui si applica l'esclusione. KES e KSWS hanno set di componenti diversi, pertanto la migrazione guidata non può eseguire la migrazione dell'ambito di utilizzo delle esclusioni. Pertanto, se nell'ambito di utilizzo di KSWS è selezionato almeno un componente, KES applica l'esclusione a tutti i componenti dell'applicazione.

È possibile configurare l'ambito di utilizzo di KSWS nelle impostazioni della zona attendibile e anche nelle impostazioni dei componenti di protezione di KSWS. A tale scopo, è possibile selezionare o deselezionare la casella di controllo **Applica Zona attendibile** nella sezione corrispondente del criterio. Le impostazioni dei componenti di protezione KES non includono tale casella di controllo. Questo significa che lo stato della zona attendibile nelle impostazioni dei singoli componenti viene perso durante la migrazione. Dopo aver completato la migrazione, selezionare i componenti a cui si applica l'esclusione nelle impostazioni della zona attendibile nel criterio di KES.

Migrazione dei commenti

I commenti dalla zona attendibile di KSWS vengono migrati ai commenti delle esclusioni di KES senza modifiche.

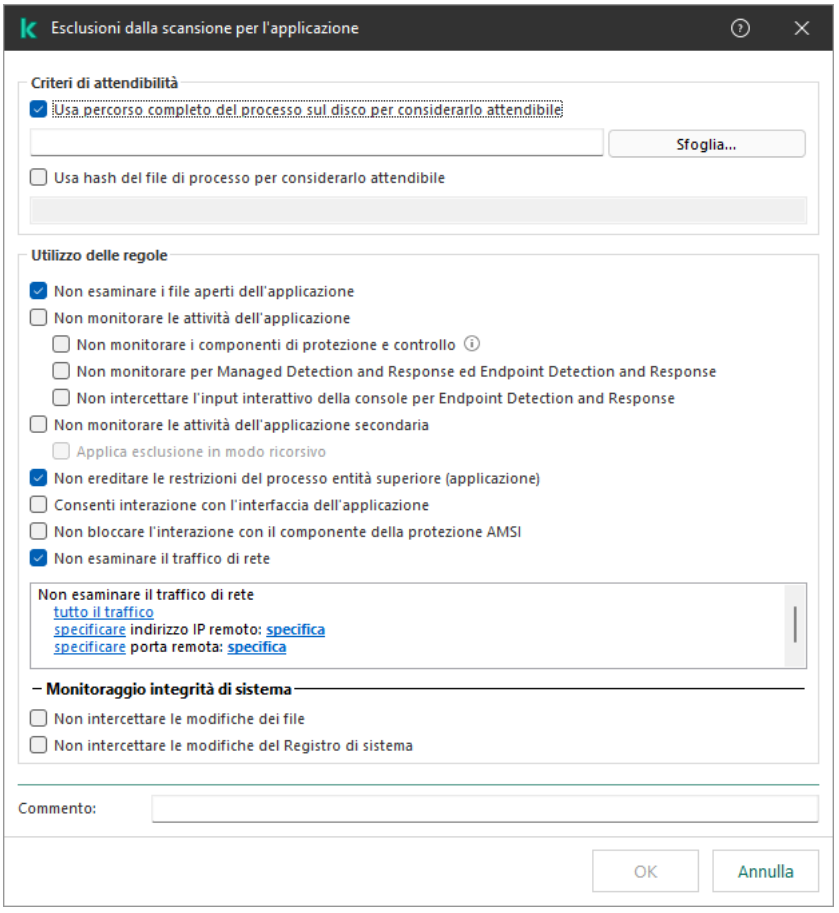
Migrazione dei processi attendibili

I processi attendibili di KSWS vengono migrati nei processi attendibili di KES con alcune limitazioni. La migrazione dei processi attendibili dipende dal metodo di selezione degli oggetti:

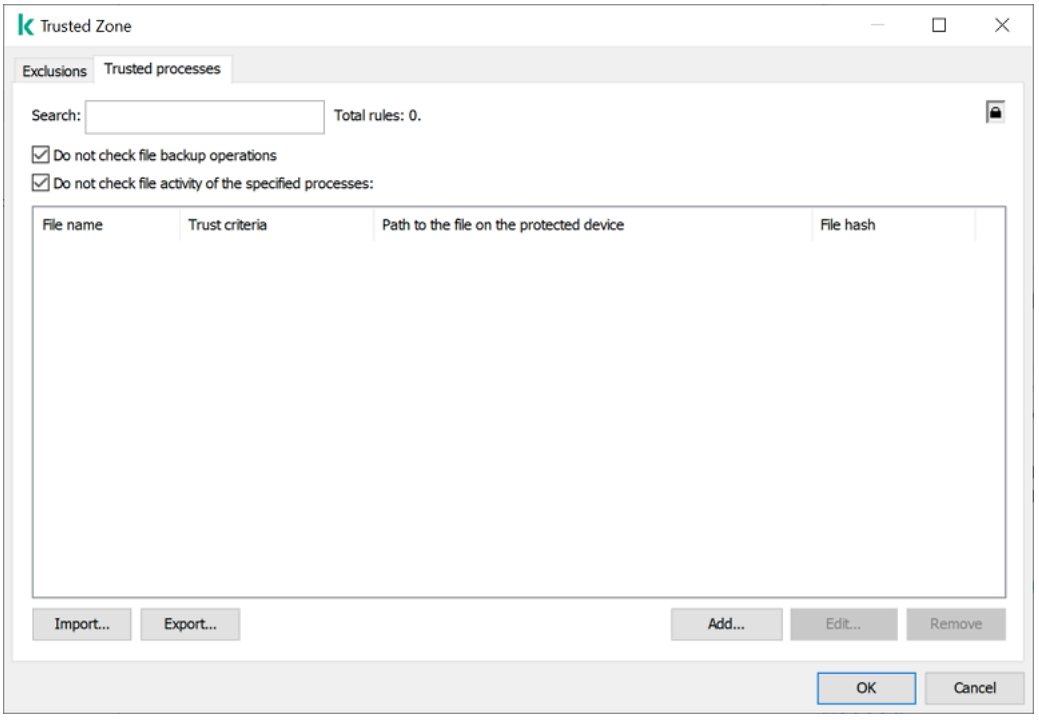
- Percorso del file nel dispositivo protetto – viene eseguita la migrazione alle applicazioni attendibili di KES.
- Hash del file – *non viene migrato*.

Se in KSWS sono presenti processi attendibili configurati come hash file, tali processi attendibili non vengono migrati. Dopo la migrazione, è necessario aggiungere tali processi attendibili manualmente.

Se la casella di controllo **Non controllare le operazioni di backup dei file** è selezionata nelle impostazioni dei processi attendibili, questa impostazione viene migrata alle applicazioni attendibili di KES (la casella di controllo **Non monitorare le attività dell'applicazione**).



Impostazioni delle applicazioni attendibili di KES



Impostazioni dei processi attendibili di KSWS

Migrazione delle regole di Controllo degli avvii delle applicazioni di KSWS

Controllo degli avvii delle applicazioni di KSWS è bloccato per impostazione predefinita. Controllo degli avvii delle applicazioni blocca automaticamente tutte le applicazioni che non sono specificate nelle regole come applicazioni consentite. Pertanto, la migrazione guidata per Controllo applicazioni di KES imposta automaticamente la modalità di controllo **Lista consentiti**, che corrisponde al principio del blocco per impostazione predefinita.

È possibile eseguire la migrazione delle regole da KSWS a KES utilizzando la *conversione guidata in batch di criteri e attività* o la *procedura guidata per la creazione di un nuovo criterio di KES basato sul criterio di KSWS*.

Migrazione della modalità di Controllo degli avvii delle applicazioni

La modalità Controllo degli avvii delle applicazioni di KSWS esegue la migrazione a Controllo applicazioni di KES come segue:

- **Solo statistiche** → **Testa regole**;
- **Attivo** → **Applica regole**.

Migrazione delle regole predefinite di Controllo degli avvii delle applicazioni di KSWS

Per impostazione predefinita, KSWS Applications Launch Control include due regole:

- **Consenti script e pacchetti MSI con certificato considerato attendibile dal sistema operativo**
- **Consenti file eseguibili con certificato considerato attendibile dal sistema operativo**

Le regole predefinite consentono l'esecuzione di *script*, *pacchetti MSI* e *file eseguibili* firmati da un certificato radice attendibile. Se almeno una regola KSWS predefinita è di tipo **Consenti**, la procedura guidata di migrazione crea una nuova regola di autorizzazione: **Applicazioni con certificati radice attendibili**. In altre parole, Controllo applicazioni di KES utilizza un'unica regola per consentire l'esecuzione degli script, dei pacchetti MSI e dei file eseguibili attendibili.

Se entrambe le regole predefinite di KSWS hanno l'estensione di tipo **Nega**, KES ignora le regole predefinite.

Migrazione delle regole personalizzate di Controllo degli avvii delle applicazioni di KSWS

Le regole di Controllo degli avvii delle applicazioni di KSWS regolano l'esecuzione dei file in base ai seguenti criteri:

- firma con un certificato digitale;
- hash SHA256;
- percorso del file.

Le regole vengono create in modo diverso in KSWS e KES, pertanto la migrazione guidata crea *categorie di applicazioni*, che includono condizioni ed esclusioni dalle regole di KSWS e aggiunge queste categorie di applicazioni alle regole di KES. La procedura guidata utilizza le condizioni **Certificato**, **Percorso cartella** e **Hash file** nelle categorie di applicazioni. Le nuove categorie di applicazioni sono disponibili in Kaspersky Security Center Administration Console nella sezione **Gestione applicazioni → Categorie di applicazioni**.

La migrazione guidata raggruppa le regole di KSWS in base al tipo e all'utente. La procedura guidata crea quindi le categorie di applicazioni che includono condizioni ed esclusioni dalle regole di KSWS e aggiunge le categorie di applicazioni alle nuove regole di KES. La procedura guidata specifica i nomi delle regole di KSWS nel campo **Descrizione** delle regole di KES.

Migrazione delle impostazioni avanzate di Controllo degli avvii delle applicazioni di KSWS

Il principio di funzionamento di Controllo degli avvii delle applicazioni di KSWS e Controllo applicazioni di KES è diverso, pertanto la migrazione guidata può eseguire la migrazione di un sottoinsieme di impostazioni.

Impostazioni di Controllo degli avvii delle applicazioni

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Ripetere l'azione eseguita al primo avvio del file per tutti gli avvii successivi dello stesso file	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security esamina l'applicazione ogni volta che tenta di eseguirla.
Impedire l'avvio degli interpreti dei comandi senza un comando da eseguire	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security consente l'esecuzione di interpreti di comando se non sono vietati da Controllo applicazioni.
Applicare le regole ai file eseguibili	*(la migrazione non viene effettuata)* L'ambito dell'applicazione della regola non può essere configurato nelle impostazioni di Controllo applicazioni di KES. Controllo applicazioni di KES applica regole a tutti i tipi di file: file eseguibili, script e pacchetti MSI. Se tutti i tipi di file sono inclusi nell'ambito dell'applicazione delle regole in KSWS, durante la migrazione KES trasferisce le regole KSWS. Se un tipo di file viene escluso dall'ambito dell'applicazione delle regole in KSWS, durante la migrazione KES trasferisce anche le regole KSWS, ma **Testa regole** viene selezionato come azione di Controllo applicazioni.
Monitorare il caricamento dei moduli DLL	**Monitora il caricamento dei moduli DLL (aumenta notevolmente il carico sul sistema)**
Applicare le regole agli script e ai pacchetti MSI	*(la migrazione non viene effettuata)* L'ambito dell'applicazione della regola non può essere configurato nelle impostazioni di Controllo applicazioni di KES. Controllo applicazioni di KES applica regole a tutti i tipi di file: file eseguibili, script e pacchetti MSI. Se tutti i tipi di file sono inclusi nell'ambito dell'applicazione delle regole in KSWS, durante la migrazione KES trasferisce le regole KSWS. Se un tipo di file viene escluso dall'ambito dell'applicazione delle regole in KSWS, durante la migrazione KES trasferisce le regole KSWS, ma **Testa regole** viene selezionato come azione di Controllo applicazioni.

Impostazioni di Kaspersky Security for Windows Server	Impostazioni di Kaspersky Endpoint Security for Windows
Nega le applicazioni considerate non attendibili da KSN	*(la migrazione non viene effettuata)* Kaspersky Endpoint Security non tiene conto della reputazione delle applicazioni e consente o nega l'esecuzione delle applicazioni in conformità alle regole.
Consenti le applicazioni considerate attendibili da KSN	Durante la migrazione, KES aggiunge una nuova regola di autorizzazione. La categoria **Altro software\Applicazioni attendibili in base alla reputazione in KSN** è specificata come condizione di attivazione della regola.
Utenti e/o gruppi di utenti autorizzati a eseguire applicazioni considerate attendibili da KSN	**Utenti e relativi diritti** in una regola di autorizzazione di Controllo applicazioni che include la categoria KL **Altro software\Applicazioni attendibili in base alla reputazione in KSN**.
Consenti automaticamente la distribuzione del software tramite le applicazioni e i pacchetti elencati	Il controllo della distribuzione del software Distribution Control in KSWS e KES funziona in modo diverso. Durante la migrazione, KES aggiunge nuove regole di autorizzazione per le applicazioni per le quali è consentita la distribuzione automatica del software. L'hash del file è specificato come condizione di attivazione della regola.
Consenti sempre la distribuzione del software tramite Windows Installer	Il controllo della distribuzione del software Distribution Control in KSWS e KES funziona in modo diverso. Durante la migrazione, KES aggiunge nuove regole di autorizzazione per le applicazioni per le quali è consentita la distribuzione automatica del software (**Applicazioni e pacchetti di distribuzione software consentiti**). L'hash del file è specificato come condizione di attivazione della regola. Nelle proprietà dell'account, la casella di controllo **Programmi di aggiornamento attendibili** è selezionata.
Consenti sempre la distribuzione del software tramite SCCM utilizzando il Servizio trasferimento intelligente in background	*(la migrazione non viene effettuata)*
Applicazioni e pacchetti di distribuzione software consentiti	Il controllo della distribuzione del software Distribution Control in KSWS e KES funziona in modo diverso. Durante la migrazione, KES aggiunge nuove regole di autorizzazione per le applicazioni per le quali è consentita la distribuzione automatica del software. L'hash del file è specificato come condizione di attivazione della regola. Nelle proprietà dell'account, la casella di controllo **Programmi di aggiornamento attendibili** è selezionata.
Impostazioni di pianificazione	*(la migrazione non viene effettuata)* Se una pianificazione è configurata per il componente nelle impostazioni di KSWS, il componente Controllo applicazioni viene abilitato al momento della migrazione. Se una pianificazione non è configurata per il componente nelle impostazioni di KSWS, Controllo applicazioni viene disabilitato al momento della migrazione. Non è possibile configurare una pianificazione separata per il componente. Il componente è sempre attivo mentre Kaspersky Endpoint Security è operativo.

Installazione di KES anziché KSWS

È possibile installare Kaspersky Endpoint Security nei seguenti modi:

- Installazione di KES dopo aver rimosso KSWS (consigliato).
- Installazione di KES su KSWS.

Rimozione di Kaspersky Security for Windows Server

È possibile rimuovere l'applicazione in remoto utilizzando l'attività *Disinstalla l'applicazione in remoto* o in locale sul server. Potrebbe essere necessario riavviare il server dopo aver rimosso KSWS. Se si desidera installare Kaspersky Endpoint Security senza riavviare, assicurarsi che Kaspersky Security for Windows Server sia stato rimosso completamente. Se l'applicazione non viene rimossa completamente, l'installazione di Kaspersky Endpoint Security potrebbe causare un funzionamento errato del server. Si consiglia inoltre di verificare che l'applicazione sia completamente rimossa se è stata utilizzata l'utilità kavremover. L'utilità kavremover non supporta la gestione di KSWS.

> Se l'opzione Protezione tramite password è abilitata per limitare l'accesso a KSWS, immettere la password di disinstallazione nelle impostazioni del pacchetto di installazione di KES.

Dopo aver rimosso KSWS, installare Kaspersky Endpoint Security for Windows utilizzando qualsiasi metodo disponibile.

Installazione di Kaspersky Endpoint Security

Quando si installa KES in remoto, i componenti selezionati nelle proprietà del pacchetto di installazione vengono installati nel server. Si consiglia di selezionare i componenti predefiniti nelle proprietà del pacchetto di installazione. Quando si installa KES su KSWS, il riavvio non è necessario.

Prima dell'installazione locale, Kaspersky Endpoint Security verifica la presenza di applicazioni Kaspersky nel computer. Se Kaspersky Security for Windows Server è installato nel computer, KES rileva la serie di componenti di KSWS installati e seleziona gli stessi componenti per l'installazione. Quando si installa KES su KSWS, il riavvio non è necessario.

> Se l'installazione di KES su KSWS non è riuscita, è possibile eseguire il rollback dell'installazione. Dopo aver ripristinato l'installazione, si consiglia di riavviare il server e riprovare.

Quando è installato Kaspersky Endpoint Security for Windows, non viene eseguita la migrazione delle impostazioni e delle attività di KSWS. Per eseguire la migrazione delle impostazioni e delle attività, eseguire la Conversione guidata di criteri e attività in batch.

È possibile consultare l'elenco di componenti installati nella sezione **Sicurezza** dell'interfaccia dell'applicazione, con il comando `status` o nella console di Kaspersky Security Center nelle proprietà del computer. È possibile modificare il set di componenti dopo l'installazione utilizzando *Modifica i componenti dell'applicazione*.

Migrazione della configurazione [KSWS+KEA] alla configurazione [KES+agente integrato]

Per supportare l'utilizzo di Kaspersky Endpoint Security for Windows come parte di EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA e MDR, all'applicazione è stato aggiunto un agente integrato. Non è più necessaria un'applicazione Kaspersky Endpoint Agent separata per utilizzare tali soluzioni.

Durante la migrazione da KSWS a KES, le soluzioni EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA e MDR continuano a funzionare con gli agenti integrati di Kaspersky Endpoint Security. Inoltre, Kaspersky Endpoint Agent verrà rimosso dal computer.

La migrazione della configurazione [KSWS+KEA] a [KES+agente integrato] prevede i seguenti passaggi:

1. **Migrazione da KSWS a KES**

   La migrazione da KSWS a KES comporta l'installazione di Kaspersky Endpoint Security anziché di Kaspersky Security for Windows Server.

   In genere, gli amministratori abilitano la protezione tramite password per limitare l'accesso a KSWS e KEA. A partire da Kaspersky Security Center Linux 15.1, è possibile immettere la password di disinstallazione dell'applicazione nelle impostazioni dell'attività *Installa l'applicazione in remoto*. L'attività consente di immettere una sola password di disinstallazione. In altre parole, se la stessa password è impostata per KSWS e KEA, le applicazioni KSWS e KEA vengono rimosse correttamente. Se le password sono diverse, la rimozione di una delle applicazioni non riesce con un errore di accesso. Per completare la migrazione, è necessario disabilitare Protezione tramite password per cui non è stato possibile immettere la password nelle impostazioni dell'attività *Installa l'applicazione in remoto*.

   Per eseguire la migrazione, è necessario selezionare i componenti necessari per supportare le soluzioni Detection and Response come parte di Kaspersky Endpoint Security. Dopo aver installato l'applicazione, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent.

2. **Migrazione di criterio e attività**

   La migrazione dei criteri e delle attività di [KSWS+KEA] a [KES+agente integrato] prevede i seguenti passaggi:

   1. Migrazione di criteri e attività da KSWS a KES tramite la Conversione guidata criteri e attività (disponibile solo in Administration Console (MMC)).

      Di conseguenza, viene aggiunto un profilo criterio denominato *UpgradedFromKSWS <Nome del criterio di Kaspersky Security for Windows Server>* al criterio KES. Vengono create anche nuove attività KES denominate *<Nome attività KSWS> (convertito)*.

   2. Migrazione di criteri e attività da KEA a KES tramite la migrazione guidata da Kaspersky Endpoint Agent (disponibile solo su Web Console e Cloud Console).

      Di conseguenza, viene creato un nuovo criterio denominato *<Nome del criterio Kaspersky Endpoint Security> & <Nome del criterio Kaspersky Endpoint Agent>*. Vengono create anche nuove attività e attività KES.

3. **Funzionalità di concessione di licenze**

Se si utilizza una licenza comune di Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security per attivare Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Agent, la funzionalità EDR Optimum verrà attivata automaticamente dopo l'upgrade dell'applicazione alla versione 11.7.0. Non è necessario eseguire altre operazioni.

Se si utilizza una licenza del componente aggiuntivo standalone di Kaspersky Endpoint Detection and Response Optimum per attivare la funzionalità EDR Optimum, è necessario accertarsi che la chiave del componente aggiuntivo EDR Optimum sia aggiunta al repository di Kaspersky Security Center e che la funzionalità di distribuzione della chiave di licenza automatica sia abilitata. Dopo aver eseguito l'upgrade dell'applicazione alla versione 11.7.0, la funzionalità EDR Optimum viene attivata automaticamente.

Se si utilizza una licenza di Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security per attivare Kaspersky Endpoint Agent e una licenza diversa per attivare Kaspersky Endpoint Security for Windows, è necessario sostituire la chiave di Kaspersky Endpoint Security con la chiave comune di Kaspersky Endpoint Detection and Response Optimum o Kaspersky Optimum Security. È possibile sostituire la chiave tramite l'attività *Aggiungi chiave*.

Non è necessario attivare la funzionalità Kaspersky Sandbox. La funzionalità Kaspersky Sandbox sarà disponibile subito dopo l'upgrade e l'attivazione di Kaspersky Endpoint Security for Windows.

Solo la licenza Kaspersky Anti Targeted Attack Platform può essere utilizzata per attivare Kaspersky Endpoint Security come parte della soluzione Kaspersky Anti Targeted Attack Platform. Dopo aver eseguito l'upgrade dell'applicazione alla versione 12.1, la funzionalità EDR (KATA) viene attivata automaticamente. Non è necessario eseguire altre operazioni.

4. **Verifica dell'integrità di Kaspersky Endpoint Detection and Response Optimum e Kaspersky Sandbox**

   Se dopo l'upgrade il computer presenta lo stato *Critico* nella console di Kaspersky Security Center:

   - Accertarsi che nel computer sia installato Network Agent versione 13.2 o successiva.
   - Controllare lo stato operativo dell'agente integrato visualizzando *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non installato*, installare il componente tramite l'attività *Modifica i componenti dell'applicazione*.
   - Accertarsi di accettare l'Informativa di Kaspersky Security Network nel nuovo criterio di Kaspersky Endpoint Security for Windows.

   Assicurarsi che la funzionalità EDR Optimum sia attivata utilizzando il *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non incluso nella licenza*, accertarsi che la funzionalità di distribuzione della chiave di licenza automatica di EDR Optimum sia attivata.

Assicurarsi che Kaspersky Security for Windows Server sia stato rimosso correttamente

Assicurarsi che Kaspersky Security for Windows Server sia completamente rimosso:

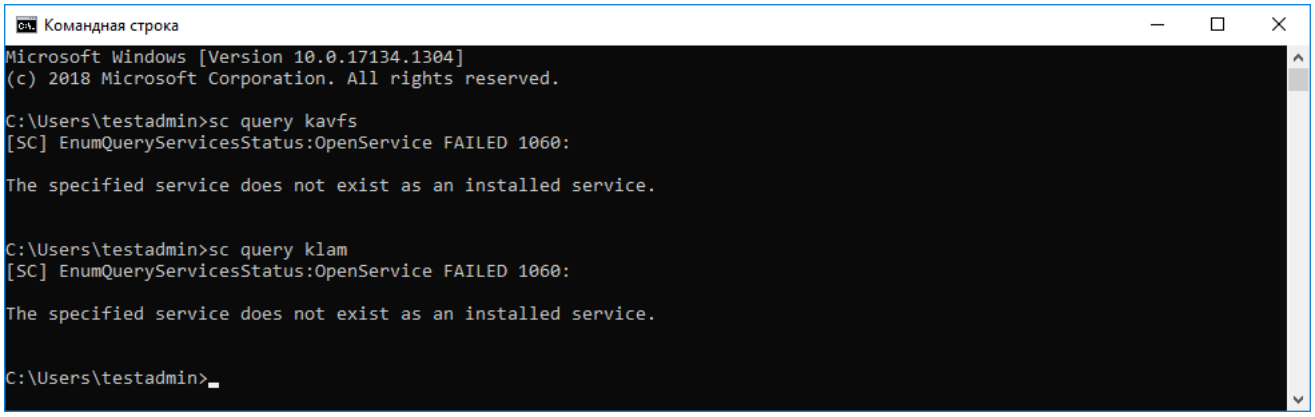
- La cartella `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` non esiste.
- I seguenti servizi non sono presenti:
  - Kaspersky Security Service (KAVFS)
  - Servizio Kaspersky Security Management (KAVFSGT)

- Servizio Kaspersky Security Exploit Prevention (KAVFSSLP)
- Servizio Kaspersky Security Script Checker (KAVFSSCS)

È possibile controllare i servizi in esecuzione in Gestione attività o emettendo il comando `sc query` (vedere la figura riportata di seguito).

- I seguenti driver non sono presenti:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

  È possibile controllare i driver installati nella cartella `C:\Windows\System32\drivers` o emettendo il comando `sc query`. Se manca un servizio o un driver, si riceverà la seguente risposta:



Assicurarsi che i servizi e i driver di Kaspersky Security for Windows Server siano stati rimossi correttamente

Se i file dell'applicazione o del driver restano nel server, eliminare manualmente i file pertinenti. Se i servizi di Kaspersky Security for Windows Server sono ancora in esecuzione nel server, interrompere (`sc stop`) ed eliminare (`sc delete`) i servizi manualmente. Per arrestare il driver klam.sys, utilizzare il comando `fltmc unload klam`.

Attivazione di KES con una chiave di KSWS

Dopo aver installato l'applicazione, è possibile attivare Kaspersky Endpoint Security for Windows (KES) utilizzando una chiave di licenza di Kaspersky Security for Windows Server (KSWS). Il processo di attivazione dopo la migrazione dipende dal metodo di attivazione di KSWS (vedere la tabella seguente).

Kaspersky Endpoint Security non supporta la *licenza di Kaspersky Security for Storage*. Per utilizzare questa licenza, è necessario utilizzare Kaspersky Security for Windows Server.

Per attivare KES con la chiave di KSWS, è possibile usare solo il codice di attivazione. Se si utilizza un file chiave per attivare l'applicazione, è necessario contattare l'Assistenza tecnica per richiedere un file chiave di Kaspersky Endpoint Security.

Attivazione di Kaspersky Endpoint Security for Windows con una chiave di Kaspersky Security for Windows Server

Metodo di attivazione di Kaspersky Security for Windows Server	Migrazione della chiave di Kaspersky Endpoint Security for Windows.
Distribuzione automatica della chiave di licenza di KSWS ai computer.	Se la distribuzione automatica delle chiavi è abilitata nelle proprietà della chiave di licenza di KSWS, KES viene attivato automaticamente con la chiave di KSWS.
La chiave di KSWS viene aggiunta da un'attività.	Se KSWS viene attivato tramite l'attività, la chiave di licenza di KSWS viene eliminata durante la migrazione da KSWS. È necessario attivare nuovamente l'applicazione. Ad esempio, è possibile aggiungere una chiave di licenza al pacchetto di installazione di Kaspersky Endpoint Security for Windows.
La chiave di KSWS viene aggiunta in locale nell'interfaccia dell'applicazione.	Se KSWS viene attivato in locale mediante l'attivazione guidata dell'applicazione, la chiave di licenza di KSWS viene eliminata durante la migrazione da KSWS. È necessario attivare nuovamente l'applicazione. Ad esempio, è possibile aggiungere una chiave di licenza al pacchetto di installazione di Kaspersky Endpoint Security for Windows.
La chiave di KSWS viene aggiunta al pacchetto di installazione.	Se KSWS viene attivato con la chiave del pacchetto di installazione, la chiave di licenza di KSWS viene eliminata durante la migrazione da KSWS. È necessario attivare nuovamente l'applicazione. Ad esempio, è possibile aggiungere una chiave di licenza al pacchetto di installazione di Kaspersky Endpoint Security for Windows.
Immagine della macchina virtuale a pagamento (Amazon Machine Image - AMI) in Amazon Web Services (AWS).	Se Kaspersky Security Center è stato acquistato come immagine di una macchina virtuale a pagamento (Amazon Machine Image - AMI) in Amazon Web Services (AWS), l'attivazione di KES non è richiesta. In questo caso, Kaspersky Security Center utilizza l'abbonamento ad AWS già aggiunto all'applicazione.
Immagine di Kaspersky Security Center già pronta e gratuita con la propria licenza (modello Bring Your Own License - BYOL).	Se si utilizza un'immagine gratuita predefinita di Kaspersky Security Center con la propria licenza in un ambiente cloud (modello Bring Your Own License - BYOL), è necessario attivare l'applicazione utilizzando qualsiasi metodo disponibile. Sarà necessaria una licenza di Kaspersky Hybrid Cloud Security.

Considerazioni speciali per la migrazione di server a carico elevato

Nei server a carico elevato, è importante monitorare le prestazioni ed evitare errori. Dopo la migrazione a Kaspersky Endpoint Security for Windows, si consiglia di disabilitare temporaneamente i componenti dell'applicazione che utilizzano notevoli risorse del server rispetto ad altri componenti. Dopo aver verificato che il server funzioni normalmente, è possibile riattivare i componenti dell'applicazione.

Si consiglia di eseguire la migrazione dei server a carico elevato come segue:

1. Creare un criterio di Kaspersky Endpoint Security con le impostazioni predefinite.

   Le impostazioni predefinite sono considerate ottimali. Queste impostazioni sono consigliate dagli esperti di Kaspersky. Le impostazioni predefinite forniscono il livello di protezione consigliato e un utilizzo ottimale delle risorse.

2. Nelle impostazioni dei criteri, disattivare i seguenti componenti: Protezione minacce di rete, Rilevamento del Comportamento, Prevenzione Exploit, Motore di Remediation, Controllo applicazioni.

   Se nell'organizzazione è stata distribuita la soluzione Kaspersky Managed Detection and Response (MDR), caricare il file di configurazione BLOB nel criterio di Kaspersky Endpoint Security.

3. Rimuovere Kaspersky Security for Windows Server dal server.

4. Installare Kaspersky Endpoint Security for Windows con il set predefinito di componenti.

   Se nell'organizzazione sono state distribuite le soluzioni Detection and Response, selezionare i componenti pertinenti nelle proprietà del pacchetto di installazione.

5. Controllare le impostazioni dell'applicazione:

   - L'applicazione viene attivata con la chiave di licenza KSWS.
   - Il nuovo criterio è applicato. I componenti precedentemente selezionati sono disabilitati.

6. Verificare che il server funzioni. Verificare che Kaspersky Endpoint Security for Windows non utilizzi più dell'1% delle risorse del server.

7. Se necessario, creare esclusioni di scansione, aggiungere applicazioni attendibili, creare un elenco di indirizzi Web attendibili.

8. Attivare i componenti Rilevamento del Comportamento, Prevenzione Exploit, Motore di Remediation. Verificare che Kaspersky Endpoint Security for Windows non utilizzi più dell'1% delle risorse del server.

9. Attivare il componente Protezione minacce di rete. Verificare che Kaspersky Endpoint Security for Windows non utilizzi più dell'2% delle risorse del server.

10. Attivare il componente Controllo applicazioni in modalità di test delle regole.

11. Verificare che Controllo applicazioni funzioni. Se necessario, aggiungere nuove regole di Controllo applicazioni e disattivare la modalità di test delle regole dopo aver verificato il corretto funzionamento di Controllo applicazioni.

Dopo la migrazione da KSWS a KES, assicurarsi che l'applicazione funzioni correttamente. Controllare lo stato del server nella console (deve essere *OK*). Assicurarsi che non vengano segnalati errori per l'applicazione; controllare inoltre l'ora dell'ultima connessione all'Administration Server, l'ora dell'ultimo aggiornamento del database e lo stato di protezione del server.

Gestione dell'applicazione in un server in modalità Server Core

Un server in modalità Server Core non dispone di un'interfaccia utente. Pertanto, è possibile gestire l'applicazione solo da remoto utilizzando la console di Kaspersky Security Center o in locale sulla riga di comando.

Gestione dell'applicazione tramite la console di Kaspersky Security Center

L'installazione dell'applicazione tramite la console di Kaspersky Security Center non differisce da un'installazione eseguita normalmente. Quando si crea un pacchetto di installazione, è possibile aggiungere una chiave di licenza per attivare l'applicazione. È possibile utilizzare una chiave di Kaspersky Endpoint Security for Windows o una chiave di Kaspersky Security for Windows Server.

Su un server in modalità Server Core, i seguenti componenti dell'applicazione non sono disponibili: Protezione minacce Web, Protezione minacce di posta, Controllo Web, Prevenzione Attacchi BadUSB, Criptaggio a livello di file (FLE), Kaspersky Disk Encryption (FDE).

Il riavvio non è richiesto durante l'installazione di Kaspersky Endpoint Security. Il riavvio è richiesto solo se è necessario rimuovere applicazioni incompatibili prima dell'installazione. Potrebbe essere necessario il riavvio anche durante l'aggiornamento della versione dell'applicazione. L'applicazione non può mostrare una finestra per richiedere all'utente di riavviare il server. È possibile ottenere informazioni sulla necessità di riavviare il server dai rapporti nella console di Kaspersky Security Center.

La gestione dell'applicazione su un server in modalità Server Core non è diversa dalla gestione di un computer. È possibile utilizzare criteri e attività per configurare l'applicazione.

La gestione dell'applicazione su un server in modalità Server Core comporta le seguenti considerazioni speciali:

- Il server in modalità Server Core non dispone di un'interfaccia utente, pertanto Kaspersky Endpoint Security non mostra un avviso che informa l'utente che è necessaria la disinfezione avanzata. Per disinfettare una minaccia, è necessario abilitare la tecnologia Disinfezione avanzata nelle impostazioni dell'applicazione e abilitare immediatamente Disinfezione avanzata nelle impostazioni dell'attività *Scansione malware*. Quindi, è necessario avviare l'attività *Scansione malware*.

- Crittografia unità BitLocker è disponibile solo con un Trusted Platform Module (TPM). Non è possibile utilizzare un PIN/password per il criptaggio, poiché l'applicazione non è in grado di mostrare la finestra di richiesta della password per l'autenticazione di preavvio. Se nel sistema operativo è abilitata la modalità di compatibilità FIPS (Federal Information Processing Standard), collegare un'unità rimovibile per il salvataggio della chiave di crittografia prima di avviare il criptaggio dell'unità.

Gestione dell'applicazione dalla riga di comando

Quando non è possibile utilizzare un'interfaccia utente, è possibile gestire Kaspersky Endpoint Security dalla riga di comando.

Per installare l'applicazione in un server in modalità Server Core, eseguire il comando seguente:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Per attivare l'applicazione, eseguire il comando seguente:

```
avp.com license /add <activation code or key file>
```

Per controllare gli stati del profilo dell'applicazione, eseguire il comando seguente:

```
avp.com status
```

Per visualizzare l'elenco dei comandi di gestione dell'applicazione, eseguire il comando seguente:

```
avp.com help
```

Migrazione da [KSWS+KEA] a [KES+agente integrato]

Durante la migrazione da Kaspersky Security for Windows Server (KSWS) a Kaspersky Endpoint Security (KES), è possibile utilizzare i seguenti suggerimenti per configurare la protezione del server e ottimizzare le prestazioni. Qui esamineremo un esempio di migrazione per una singola organizzazione.

Infrastruttura dell'organizzazione

L'azienda dispone delle seguenti apparecchiature installate:

- Kaspersky Security Center 14.2

  L'amministratore gestisce le soluzioni Kaspersky utilizzando Administration Console (MMC). Anche Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) è distribuito

  In Kaspersky Security Center vengono creati tre gruppi di amministrazione, con i server dell'organizzazione: due gruppi di amministrazione per i server SQL e un gruppo di amministrazione per i server Microsoft Exchange. Ogni gruppo di amministrazione è gestito dal proprio criterio. Le attività *Aggiornamento database* e *Scansione su richiesta* vengono create per tutti i server dell'organizzazione.

  La chiave di attivazione di KSWS viene aggiunta a Kaspersky Security Center. Viene abilitata la distribuzione automatica delle chiavi.

- Server SQL con Kaspersky Security for Windows Server 11.0.1 e Kaspersky Endpoint Agent 3.11 installati. I server SQL vengono combinati in due cluster.

  KSWS è gestito dai criteri *SQL_Policy(1)* e *SQL_Policy(2)*. Vengono create anche le attività *Aggiornamento database* e *Scansione su richiesta*.

- Un server Microsoft Exhange con Kaspersky Security for Windows Server 11.0.1 e Kaspersky Endpoint Agent 3.11 installati.

  KSWS è gestito dal criterio *Exchange_Policy*. Vengono create anche le attività *Aggiornamento database* e *Scansione su richiesta*.

Pianificazione della migrazione

La migrazione prevede i seguenti passaggi:

1. Migrazione di criteri e attività di KSWS utilizzando la Conversione guidata di criteri e attività in batch.
2. Migrazione del criterio di Kaspersky Endpoint Agent tramite la Conversione guidata di criteri e attività in batch.
3. Utilizzo dei tag per attivare i profili dei criteri nelle proprietà del nuovo criterio.
4. Installazione di KES anziché KSWS.
5. Attivazione di EDR Optimum.
6. Verifica che KES funzioni.

Lo scenario di migrazione viene inizialmente eseguito in uno dei cluster di server SQL. Quindi lo scenario di migrazione viene eseguito nell'altro cluster di server SQL. Quindi lo scenario di migrazione viene eseguito in Microsoft Exchange.

Migrazione di criteri e attività di KSWS utilizzando la Conversione guidata di criteri e attività in batch

Per eseguire la migrazione delle attività di KSWS, è possibile utilizzare la Conversione guidata di criteri e attività in batch (la migrazione guidata). Di conseguenza, anziché i criteri *SQL_Policy(1)*, *SQL_Policy(2)* e *Exchange_Policy*, si otterrà un singolo criterio con tre profili rispettivamente per i server SQL e Microsoft Exchange. Il nuovo profilo dei criteri con le impostazioni di KSWS verrà denominato *UpgradedFromKSWS <Nome del criterio di Kaspersky Security for Windows Server>*. Nelle proprietà del profilo, la migrazione guidata seleziona automaticamente il tag del dispositivo `UpgradedFromKSWS` come criterio di attivazione. Pertanto, le impostazioni del profilo dei criteri vengono applicate automaticamente ai server.

Migrazione del criterio di Kaspersky Endpoint Agent tramite la Conversione guidata di criteri e attività in batch

Per eseguire la migrazione dei criteri di Kaspersky Endpoint Agent, è possibile utilizzare la Conversione guidata di criteri e attività in batch. La migrazione guidata di criteri e attività per Kaspersky Endpoint Agent è disponibile solo in Web Console.

Utilizzo dei tag per attivare i profili dei criteri nelle proprietà del nuovo criterio

Selezionare il tag del dispositivo assegnato in precedenza come condizione di attivazione del profilo. Aprire le proprietà dei criteri e selezionare *Regole generali per l'attivazione del profilo criterio* come condizione di attivazione del profilo.

Installazione di KES anziché KSWS

Prima di installare KES, è necessario disabilitare la protezione tramite password nelle proprietà dei criteri di KSWS.

L'installazione di KES prevede i seguenti passaggi:

1. Preparare il pacchetto di installazione. Nelle proprietà del pacchetto di installazione, selezionare il kit di distribuzione di Kaspersky Endpoint Security for Windows 12.0 e selezionare il set di componenti predefinito.
2. Creare un'attività *Installa l'applicazione in remoto* per uno dei gruppi di amministrazione dei server SQL.
3. Nelle proprietà dell'attività, selezionare il pacchetto di installazione e il file della chiave di licenza.
4. Attendere fino al completamento dell'attività.
5. Ripetere l'installazione di KES per i restanti gruppi di amministrazione.

Kaspersky Security Center aggiunge automaticamente il tag `UpgradedFromKSWS` ai nomi dei computer sulla console dopo che l'installazione di KES è stata completata.

Per verificare l'installazione di KES, è possibile utilizzare il *Rapporto sulla distribuzione della protezione*. È inoltre possibile controllare lo stato del dispositivo. Per confermare l'attivazione dell'applicazione, è possibile utilizzare il *rapporto sull'utilizzo delle chiavi di licenza*.

Attivazione di EDR Optimum

È possibile attivare la funzionalità EDR Optimum utilizzando una licenza autonoma del componente aggiuntivo di Kaspersky Endpoint Detection and Response Optimum. È necessario verificare che la chiave di EDR Optimum sia stata aggiunta al repository di Kaspersky Security Center e che la funzionalità di distribuzione automatica della chiave di licenza sia abilitata.

Per verificare l'attivazione di EDR Optimum, è possibile utilizzare il *Rapporto sullo stato dei componenti dell'applicazione*.

Verifica che KES funzioni

Per verificare che KES funzioni, è possibile controllare e vedere che non vengano segnalati errori. Lo stato del dispositivo deve essere *OK*. Attività di aggiornamento e scansione malware completate correttamente.

Modalità Light Agent per proteggere le macchine virtuali

A partire dalla versione 12.8, è possibile utilizzare Kaspersky Endpoint Security for Windows come parte di Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* è una soluzione integrata che fornisce una protezione completa delle macchine virtuali da vari tipi di minacce alla sicurezza delle informazioni, attacchi di rete e attacchi di phishing. Per utilizzare questa soluzione, è necessario installare l'applicazione in modalità Light Agent.

L'installazione di Kaspersky Endpoint Security in modalità Light Agent in macchine virtuali basate su Arm non è supportata.

È possibile utilizzare Kaspersky Endpoint Security in modalità Light Agent come parte di Kaspersky Security for Virtualization Light Agent a partire dalla versione 6.2.

Quando si avvia Light Agent, questo stabilisce e mantiene una connessione alla SVM della macchina virtuale (Secure Virtual Machine). Nella SVM viene distribuito un server di protezione. Il *server di protezione* è il componente della soluzione Kaspersky Security for Virtualization Light Agent che esegue la scansione dei file alla ricerca di virus e altro malware, aggiorna i database anti-virus e gestisce le chiavi di licenza. Light Agent invia alla SVM i file o i relativi frammenti che richiedono la scansione. I risultati della scansione sono disponibili per tutte le macchine virtuali in cui è installato Light Agent (la tecnologia SharedCache). Questa tecnologia aumenta l'efficienza della soluzione e fornisce una risposta più rapida alle minacce.

L'infrastruttura dell'organizzazione può contenere molte macchine virtuali in cui è installato Light Agent e molte SVM. Il Server di integrazione gestisce l'interazione tra le macchine virtuali e le SVM. Il *Server di integrazione* è un componente della soluzione Kaspersky Security for Virtualization Light Agent che genera un elenco delle SVM disponibili e trasferisce questi dati ai Light Agent, partecipa al rilevamento delle SVM da parte dei Light Agent, protegge la connessione tra i Light Agent e le SVM ed esegue altre funzioni.

Considerazioni speciali sulla modalità Light Agent

È possibile gestire Kaspersky Endpoint Security in modalità Standard e in modalità Light Agent utilizzando i criteri e le attività di Kaspersky Endpoint Security. In modalità Light Agent, alcuni componenti e funzionalità dell'applicazione non sono disponibili.

Aggiornamento di database e moduli software dell'applicazione

Kaspersky Endpoint Security in modalità Light Agent utilizza database di malware speciali di cui l'applicazione ha bisogno quando funziona come parte della soluzione Kaspersky Security for Virtualization Light Agent. Kaspersky Endpoint Security ottiene gli aggiornamenti dei database e dei moduli dell'applicazione dal server di protezione.

I database e i moduli nelle macchine virtuali protette vengono aggiornati tramite un'attività *Aggiornamento di database e moduli dell'applicazione* speciale, in cui una cartella nelle SVM viene specificata come sorgente degli aggiornamenti. Light Agent esegue automaticamente l'attività *Aggiornamento di database e moduli dell'applicazione*. Non è possibile selezionare una sorgente degli aggiornamenti diversa, configurare la pianificazione dell'attività o rimuovere l'attività.

Il server di protezione gestisce anche il rollback degli aggiornamento più recente del database di malware. Dopo il rollback di un aggiornamento di database e moduli dell'applicazione nella SVM, un'attività *Aggiornamento di database e moduli dell'applicazione* locale speciale viene avviata nella macchina virtuale protetta. Questa attività consente a Light Agent di tornare a utilizzare il set precedente di database di malware.

Kaspersky Endpoint Security in modalità Light Agent non supporta l'attività *Rollback degli aggiornamenti*.

Attivazione di Light Agent

Per attivare l'applicazione, è necessario aggiungere una chiave di licenza alla SVM a cui è connesso Light Agent. Non è necessario attivare l'applicazione separatamente.

Altre considerazioni speciali sulla modalità Light Agent

- Durante la creazione di un criterio per l'applicazione, è consigliabile selezionare la modalità Light Agent. In questa modalità, la Creazione guidata nuovo criterio richiede di configurare la connessione SVM. Queste impostazioni sono necessarie per il funzionamento dell'applicazione in modalità Light Agent.
- Non è possibile installare i componenti di Criptaggio dati e Controllo adattivo delle anomalie in modalità Light Agent. Il set di componenti dipende anche dal tipo di sistema operativo guest: workstation o server.
- Light Agent non supporta l'integrazione con le soluzioni Kaspersky Endpoint Detection and Response Expert e Kaspersky Endpoint Detection and Response Expert (cloud).
- È possibile gestire Light Agent in Administration Console (MMC) e Kaspersky Security Center Web Console. Non è possibile gestire Light Agent in Kaspersky Security Center Cloud Console.
- La modifica del set di componenti dell'applicazione nelle macchine virtuali VDI non è supportata.
- Kaspersky Endpoint Security comunica con i server KSN tramite un server proxy KSN. La comunicazione diretta con KSN non è supportata.
- La modalità cloud di Kaspersky Security Network non è supportata.
- L'utilizzo del server proxy dell'applicazione durante la connessione al server di integrazione (VIIS), al server di protezione (SVM) e ai server di KSN non è supportato.

Configurazione preliminare della macchina virtuale

È possibile installare Kaspersky Endpoint Security in una macchina virtuale che utilizza la tecnologia della piattaforma virtuale. Kaspersky Endpoint Security supporta le piattaforme virtuali VMware, Microsoft Hyper-V e Citrix. Prima dell'installazione, è necessario eseguire la configurazione preliminare delle macchine virtuali.

Compatibilità con la tecnologia Citrix App Layering

Se si intende utilizzare Full User Layer per il salvataggio dello stato delle macchine virtuali temporanee, è necessario eseguire le seguenti operazioni prima di installare il modello delle macchine virtuali:

1. Creare il file C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt e aggiungervi le seguenti esclusioni:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. Nel Registro di sistema del sistema operativo, nella HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr, creare un nuovo valore DWORD denominato MiniFilterBypass e impostarlo su 1.

3. Nel Registro di sistema del sistema operativo, nella chiave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd, creare un nuovo valore MULTI_SZ denominato ExcludeKey e impostarlo su \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Riavviare la macchina virtuale.

Per l'installazione in macchine virtuali in un'infrastruttura che utilizza Citrix App Layering, è necessario eseguire le seguenti operazioni:

1. Installare Kaspersky Security Center Administration Agent e Kaspersky Endpoint Security for Windows nel modello di macchina virtuale nel livello applicazione.

2. Creare un'immagine di macchina virtuale composta da più livelli.

3. Distribuire l'immagine creata negli hypervisor che supportano la soluzione Citrix App Layering.

4. Configurare la creazione di macchine virtuali temporanee dall'immagine creata.

Per i dettagli sull'installazione del software anti-virus insieme a Citrix App Layering, fare riferimento alla documentazione su Citrix App Layering.

Compatibilità con la tecnologia Citrix Provisioning (Citrix Provisioning Services)

Per assicurarsi che l'applicazione sia compatibile con la tecnologia Citrix Provisioning (Citrix Provisioning Services):

- Se il software Citrix Provisioning Target Device è installato sulla macchina virtuale, è necessario rimuoverlo prima di installare l'applicazione Kaspersky Endpoint Security (per ulteriori dettagli, visitare il sito Web dell'assistenza tecnica di Citrix). Dopo l'installazione dell'applicazione, è necessario reinstallare Citrix Provisioning Target Device. È inoltre necessario reinstallare Citrix Provisioning Target Device durante il ripristino dell'applicazione, anche in caso di aggiornamento del sistema operativo.

L'aggiornamento del sistema operativo prevede i seguenti passaggi:

1. Eliminare Citrix Provisioning Target Device.
2. Aggiornare il sistema operativo.
3. Dopo aver avviato la macchina virtuale, assicurarsi che l'applicazione Kaspersky Endpoint Security sia in esecuzione e funzioni correttamente.
4. Reinstallare Citrix Provisioning Target Device.

- Durante l'installazione dell'applicazione utilizzando l'Installazione guidata o in remoto utilizzando Kaspersky Security Center, è necessario selezionare la casella di controllo **Garantisci la compatibilità con Citrix PVS**.

Compatibilità con la tecnologia Omnissa App Volumes

Prima di installare nel modello delle macchine virtuali, è necessario creare il file %SVAgent%\Config\Custom\snapvol.cfg file e aggiungervi le seguenti esclusioni:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`

- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Per informazioni dettagliate, consultare la documentazione di Omnissa.

Installazione di Light Agent

L'installazione di Kaspersky Endpoint Security in modalità Light Agent in macchine virtuali basate su Arm non è supportata.

L'installazione dell'applicazione in modalità Light Agent è la stessa della modalità Standard. Prima di installare Light Agent in una macchina virtuale, è necessario assicurarsi che Kaspersky Security Center Network Agent sia installato. *Network Agent* semplifica l'interazione tra Administration Server e una macchina virtuale.

EDR Agent può essere installato in una macchina virtuale in uno dei seguenti modi:

- Da remoto tramite Kaspersky Security Center.
- In locale, utilizzando l'Installazione guidata.
- In locale tramite la riga di comando.

Per installare Light Agent, è necessario selezionare la configurazione appropriata nelle impostazioni del pacchetto di installazione o in Installazione guidata.

Quando si installa Light Agent in un server, i componenti della protezione avanzata (Rilevamento del Comportamento, Prevenzione Exploit, Motore di Remediation) vengono esclusi dalla configurazione predefinita dell'applicazione. Le impostazioni predefinite dell'applicazione forniscono il livello di protezione consigliato e un utilizzo ottimale delle risorse del server. Quando si installa Light Agent in una workstation, i componenti della protezione avanzata sono inclusi nella configurazione predefinita dell'applicazione.

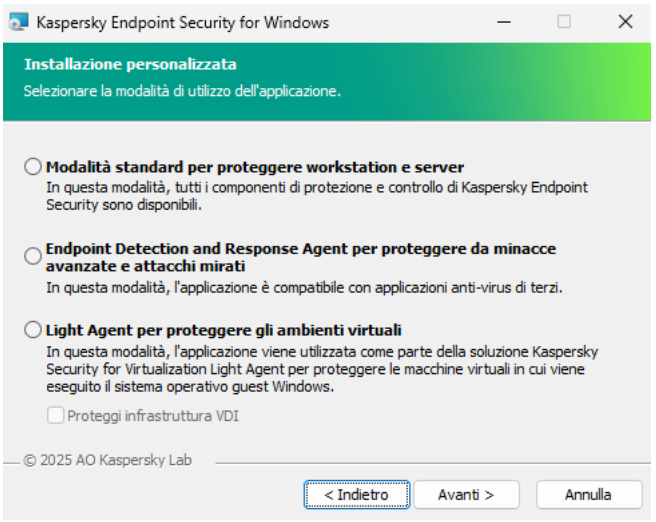
Durante l'installazione di Light Agent, è consigliabile selezionare le esclusioni predefinite e le applicazioni attendibili per l'ambiente virtuale pertinente. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente l'applicazione ed evitare problemi di compatibilità con l'ambiente virtuale. È inoltre possibile configurare esclusioni dalle scansioni predefinite e applicazioni attendibili dopo l'installazione, nel criterio.

Come installare Light Agent utilizzando l'Installazione guidata

1. Copiare la cartella del kit di distribuzione nella macchina virtuale.
2. Eseguire setup_kes.exe.

   Verrà avviata l'Installazione guidata.

Configurazione di Kaspersky Endpoint Security



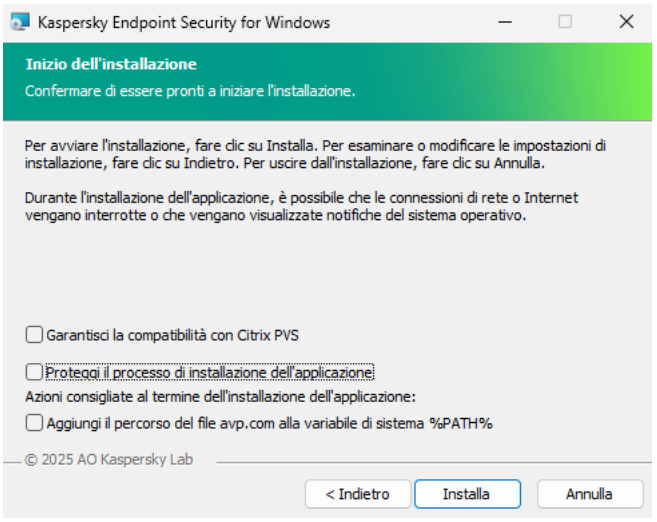
Scelta della configurazione dell'applicazione

Selezionare la configurazione **Light Agent per proteggere gli ambienti virtuali**. Questa configurazione è destinata all'applicazione utilizzata come parte della soluzione Kaspersky Security for Virtualization Light Agent. Light Agent deve essere installato in ogni macchina virtuale da proteggere tramite la soluzione. In questa configurazione, non è possibile utilizzare i componenti di Criptaggio dati o Controllo adattivo delle anomalie. Se si installa Light Agent in un modello di macchina virtuale che verrà utilizzato per creare *macchine virtuali non persistenti*, selezionare la casella di controllo **Proteggi infrastruttura VDI** (VDI è l'acronimo di Virtual Desktop Infrastructure). La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. In questa modalità, Light Agent rifiuta gli aggiornamenti delle applicazioni che richiedono il riavvio della macchina virtuale. Quando si riceve gli aggiornamenti delle applicazioni che richiedono il riavvio, Light Agent genera un evento sulla necessità di aggiornare il modello delle macchine virtuali protette.

Componenti di Kaspersky Endpoint Security

Selezionare i componenti che si desidera installare (vedere la figura riportata di seguito). È possibile modificare i componenti dell'applicazione disponibili dopo l'installazione dell'applicazione. A tale scopo, è necessario eseguire nuovamente l'Installazione guidata e scegliere di modificare i componenti disponibili.

Impostazioni avanzate



Impostazioni avanzate di installazione dell'applicazione

Proteggi il processo di installazione dell'applicazione. La protezione dell'installazione include la protezione dalla sostituzione del pacchetto di distribuzione con applicazioni dannose, bloccando l'accesso alla cartella di installazione di Kaspersky Endpoint Security e bloccando l'accesso alla sezione del Registro di sistema che contiene le chiavi dell'applicazione. Se tuttavia è impossibile installare l'applicazione (ad esempio, durante l'esecuzione dell'installazione remota tramite Windows Remote Desktop), è possibile disabilitare la protezione del processo di installazione.

Garantisci la compatibilità con Citrix PVS. È possibile abilitare il supporto di Citrix Provisioning Services per installare Kaspersky Endpoint Security in una macchina virtuale.

Aggiungi il percorso del file avp.com alla variabile di sistema %PATH%. È possibile aggiungere il percorso di installazione alla variabile %PATH% per agevolare l'utilizzo dell'interfaccia della riga di comando.

Come installare EDR Agent tramite la riga di comando

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il pacchetto di distribuzione di Kaspersky Endpoint Security.
3. Eseguire il seguente comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
```

oppure

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
```

L'opzione `VDI` abilita la modalità di protezione VDI (Virtual Desktop Infrastructure). La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. In questa modalità, Light Agent rifiuta gli aggiornamenti delle applicazioni che richiedono il riavvio della macchina virtuale. Quando si riceve gli aggiornamenti delle applicazioni che richiedono il riavvio, Light Agent genera un evento sulla necessità di aggiornare il modello delle macchine virtuali protette. Per impostazione predefinita, la modalità di protezione VDI è disabilitata.

In seguito a questa operazione, Light Agent viene installato nella macchina virtuale con il set di componenti predefinito. È possibile modificare il set di componenti e specificare l'impostazione avanzata utilizzando il file setup.ini. È anche possibile specificare le impostazioni di installazione nella riga di comando.

Come installare Light Agent utilizzando Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura della console, selezionare la cartella **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.

   Si aprirà un elenco di pacchetti di installazione che sono stati scaricati in Kaspersky Security Center.
3. Aprire le proprietà del pacchetto di installazione di Kaspersky Endpoint Security for Windows.

   Se necessario, creare un nuovo pacchetto di installazione.
4. Passare alla sezione **Impostazioni**.
5. Selezionare la configurazione **Light Agent per proteggere gli ambienti virtuali**. Questa configurazione è destinata all'applicazione utilizzata come parte della soluzione Kaspersky Security for Virtualization Light Agent. Light Agent deve essere installato in ogni macchina virtuale da proteggere tramite la soluzione. In questa configurazione, non è possibile utilizzare i componenti di Criptaggio dati o Controllo adattivo delle anomalie. Se si installa Light Agent in un modello di macchina virtuale che verrà utilizzato per creare *macchine virtuali non persistenti*, selezionare la casella di controllo **Proteggi infrastruttura VDI** (VDI è l'acronimo di Virtual Desktop Infrastructure). La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. In questa modalità, Light Agent rifiuta gli aggiornamenti delle applicazioni che richiedono il riavvio della macchina virtuale. Quando si riceve gli aggiornamenti delle applicazioni che richiedono il riavvio, Light Agent genera un evento sulla necessità di aggiornare il modello delle macchine virtuali protette.
6. Selezionare i componenti che si desidera installare.

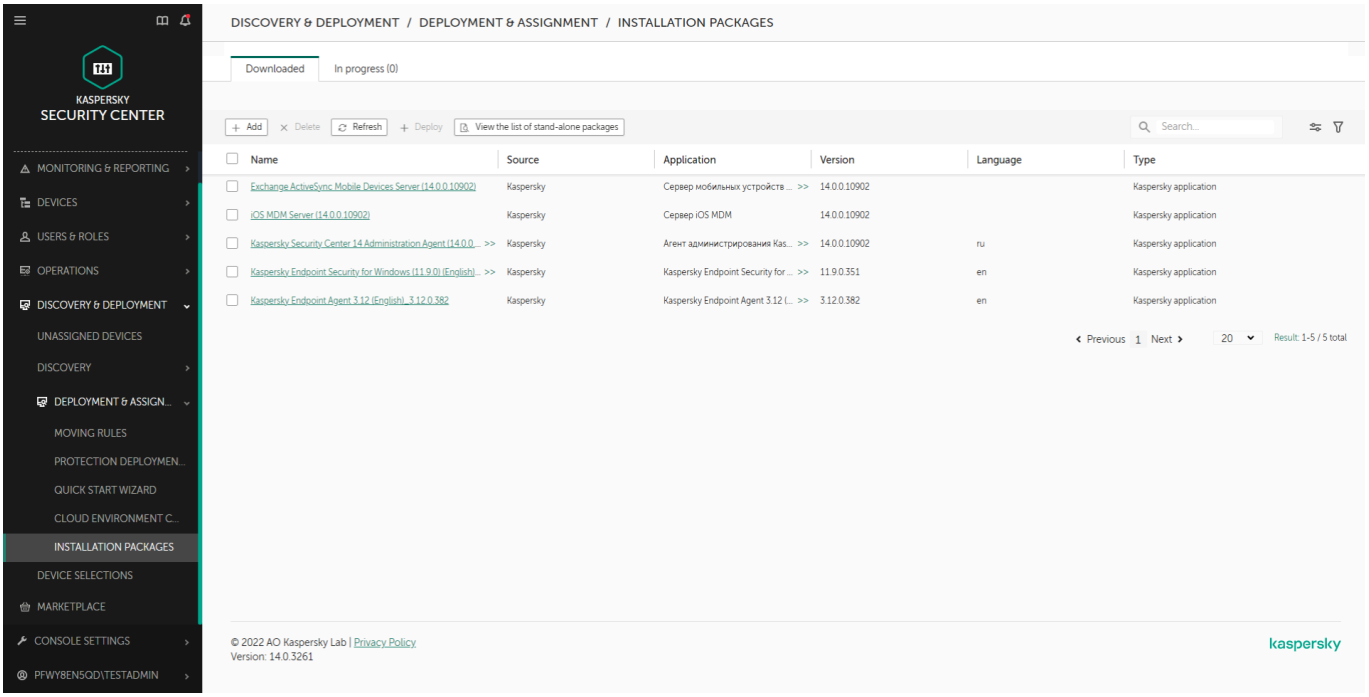
   È possibile modificare i componenti dell'applicazione disponibili dopo l'installazione dell'applicazione.
7. Configura l'area attendibile. Selezionare le esclusioni dalle scansioni predefinite e le applicazioni attendibili per l'ambiente virtuale in cui si installa l'applicazione.

   Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente l'applicazione ed evitare problemi di compatibilità con l'ambiente virtuale.
8. Salvare le modifiche.
9. Creare di un'attività di installazione remota. Nelle proprietà dell'attività, quindi selezionare il pacchetto di installazione creato.

Come installare Light Agent utilizzando Web Console

1. Nella finestra principale di Web Console, fare clic su **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

Si aprirà un elenco di pacchetti di installazione che sono stati scaricati in Kaspersky Security Center.



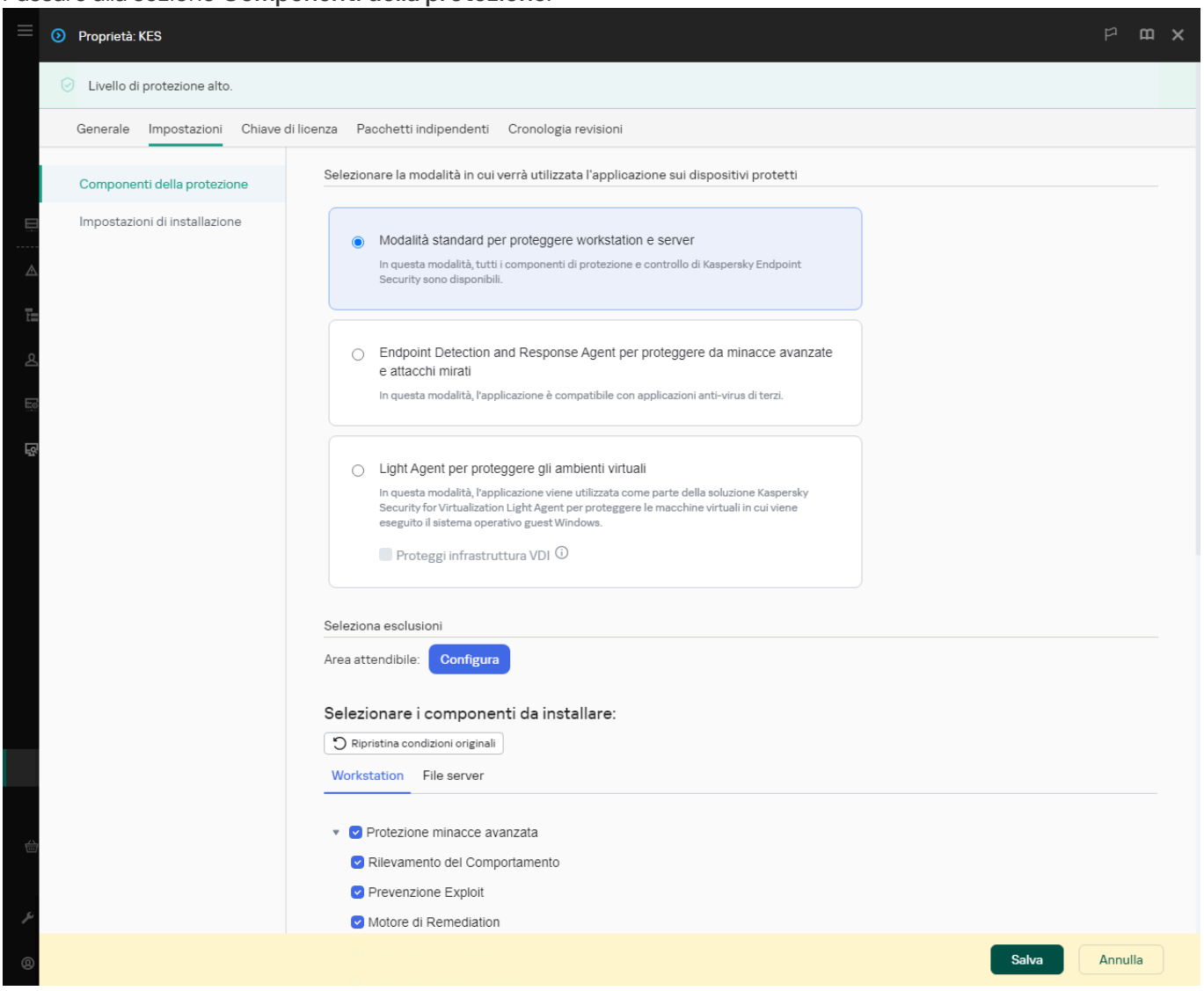
Elenco dei pacchetti di installazione

2. Aprire le proprietà del pacchetto di installazione di Kaspersky Endpoint Security for Windows.

   Se necessario, creare un nuovo pacchetto di installazione.

3. Selezionare la scheda **Impostazioni**.

4. Passare alla sezione **Componenti della protezione**.



Componenti inclusi nel pacchetto di installazione

5. Selezionare la configurazione **Light Agent per proteggere gli ambienti virtuali**. Questa configurazione è destinata all'applicazione utilizzata come parte della soluzione Kaspersky Security for Virtualization Light Agent. Light Agent deve essere installato in ogni macchina virtuale da proteggere tramite la soluzione. In questa configurazione, non è possibile utilizzare i componenti di Criptaggio dati o Controllo adattivo delle anomalie. Se si installa Light Agent in un modello di macchina virtuale che verrà utilizzato per creare *macchine virtuali non persistenti*, selezionare la casella di controllo **Proteggi infrastruttura VDI** (VDI è l'acronimo di Virtual Desktop Infrastructure). La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. In questa modalità, Light Agent rifiuta gli aggiornamenti delle applicazioni che richiedono il riavvio della macchina virtuale. Quando si riceve gli aggiornamenti delle applicazioni che richiedono il riavvio, Light Agent genera un evento sulla necessità di aggiornare il modello delle macchine virtuali protette.

6. Selezionare i componenti che si desidera installare.

   È possibile modificare i componenti dell'applicazione disponibili dopo l'installazione dell'applicazione.

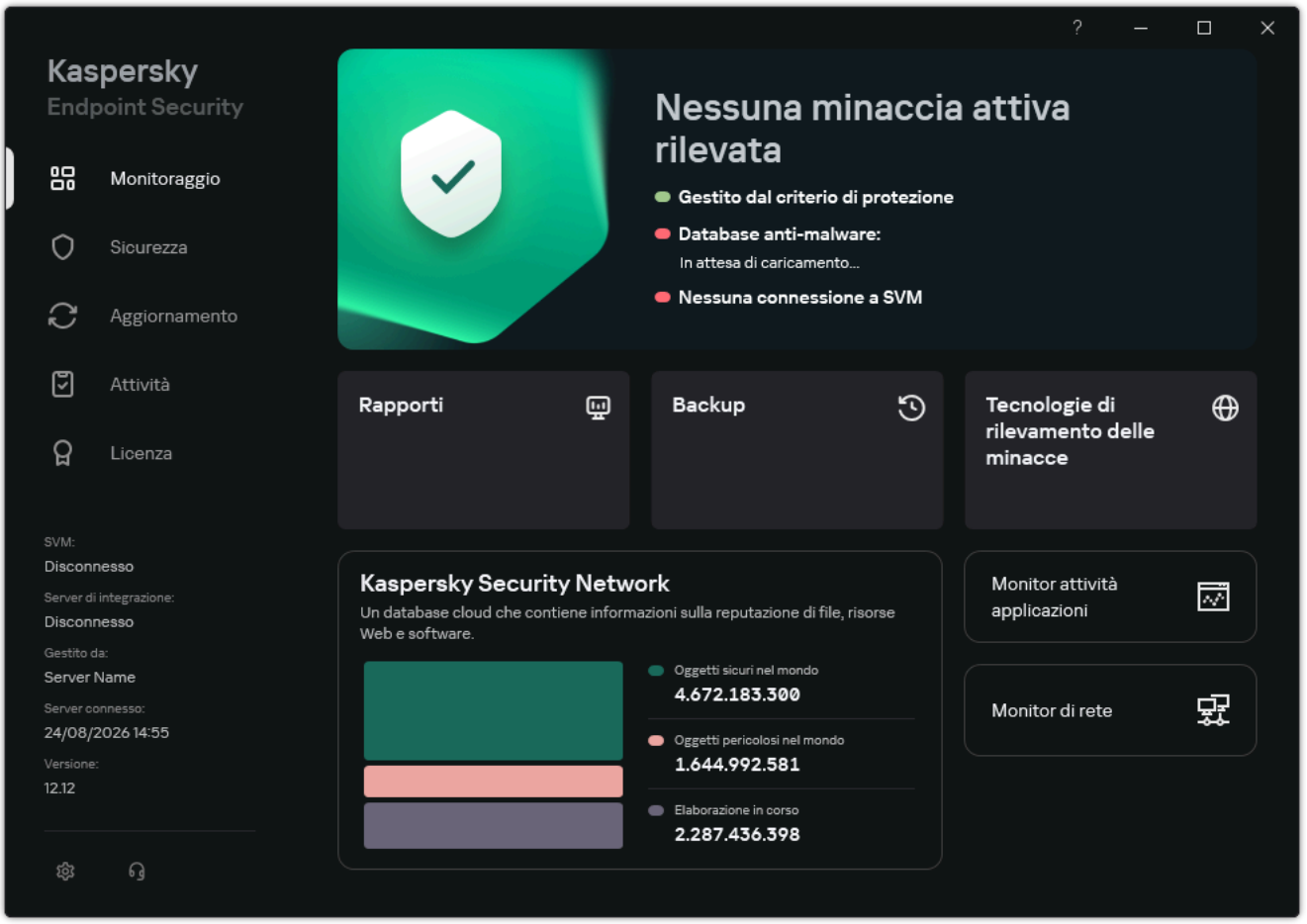
7. Configura l'area attendibile. Selezionare le esclusioni dalle scansioni predefinite e le applicazioni attendibili per l'ambiente virtuale in cui si installa l'applicazione.

   Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente l'applicazione ed evitare problemi di compatibilità con l'ambiente virtuale.

8. Salvare le modifiche.

9. Creare di un'attività di installazione remota. Nelle proprietà dell'attività, quindi selezionare il pacchetto di installazione creato.

In seguito a questa operazione, Light Agent viene installato nella macchina virtuale. È possibile utilizzare l'interfaccia dell'applicazione e nell'area di notifica viene visualizzata un'icona dell'applicazione . A questo punto è necessario configurare la connessione del Light Agent alla SVM.



Finestra principale di Light Agent

Connessione di Light Agent alla SVM

La soluzione Kaspersky Security for Virtualization Light Agent richiede la comunicazione continua tra Light Agent e SVM. Questo è necessario per eseguire la scansione dei file inviati da Light Agent alla ricerca di virus e altro malware. Senza una connessione alle SVM, Light Agent non può inviare i file per la scansione. Se non è possibile stabilire la connessione per più di cinque minuti, la scansione viene terminata con un errore.

La connessione di un Light Agent a una SVM comporta i seguenti passaggi:

1. Light Agent ottiene l'elenco delle SVM disponibili.

2. Light Agent determina un server di protezione (SVM) disponibile ottimale per la connessione in base all'algoritmo di selezione delle SVM.

3. Light Agent controlla le impostazioni di connessione alle SVM aggiuntive: tag, stato di protezione della connessione, funzionalità dell'applicazione coperte dalla licenza.

4. Connessione di Light Agent alla SVM.

È possibile ottenere informazioni sullo stato della connessione di Light Agent alla SVM in Kaspersky Endpoint Security o utilizzando il comando dell'applicazione. L'applicazione genera un evento ogni volta che viene persa o stabilita la connessione alle SVM di Light Agent e invia gli eventi a Kaspersky Security Center. Se si utilizza un server di integrazione per il rilevamento delle SVM, è possibile ottenere informazioni sullo stato della SVM e sul numero di Light Agent connessi nella console del server di integrazione. Per informazioni dettagliate sul monitoraggio dello stato delle SVM, consultare la Guida di Kaspersky Security for Virtualization Light Agent.

Rilevamento di SVM

È possibile selezionare uno dei metodi di rilevamento delle SVM per Light Agent:

- Utilizzo del server di integrazione (VIIS).

  Server di integrazione è il componente della soluzione che consente l'interazione di Kaspersky Security for Virtualization Light Agent con l'infrastruttura virtuale e genera un elenco di SVM disponibili per la connessione. Light Agent stabilisce una connessione con il server di integrazione e ottiene l'elenco degli indirizzi di SVM.

  Il Server di integrazione è particolarmente utile nelle infrastrutture virtuali di grandi dimensioni perché bilancia automaticamente il carico tra le SVM, ottiene informazioni sulle SVM disponibili, analizza queste informazioni e fornisce ai Light Agent un elenco di Protection Server (SVM) ottimali per la connessione.

  Affinché Light Agent possa ottenere un elenco di SVM, è sufficiente immettere l'indirizzo del server di integrazione.

- Utilizzo di un cluster ad alta disponibilità di Server di integrazione.

  La distribuzione di un cluster ad alta disponibilità di Server di integrazione è disponibile in Kaspersky Security for Virtualization Light Agent a partire dalla versione 6.4. Un cluster ad alta disponibilità di Server di integrazione garantisce la protezione ininterrotta dell'ambiente virtuale grazie al failover delle SVM e dei Light Agent su un Server di integrazione di backup in caso di malfunzionamento del Server di integrazione primario. Uno speciale componente del cluster, il *bilanciatore del carico*, è responsabile del failover dei server. Per informazioni dettagliate su un cluster ad alta disponibilità di Server di integrazione, consultare la Guida di Kaspersky Security for Virtualization Light Agent.

  Affinché Light Agent ottenga un elenco di SVM, è necessario immettere l'indirizzo del dispositivo sul quale è installato il bilanciatore del carico.

- Utilizzo dell'elenco di indirizzi SVM.

  Se è necessario specificare singole SVM a cui si desidera connettere Light Agent, è possibile preparare manualmente un elenco.

  È necessario elencare gli indirizzi delle SVM disponibili a cui Light Agent può connettersi.

Come configurare il rilevamento delle SVM da parte di Light Agent in Administration Console (MMC)

1. Aprire Kaspersky Security Center Administration Console.

2. Nella struttura della console, selezionare **Criteri**.

3. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

4. Nella finestra del criterio, selezionare **Modalità Light Agent → Impostazioni di rilevamento SVM**.

5. Selezionare un metodo di rilevamento delle SVM.

   - **Usa server di integrazione**. Immettere le impostazioni per la connessione al Server di integrazione in base all'infrastruttura:

     - **Singolo Server di integrazione**. Immettere le impostazioni di connessione al Server di integrazione: indirizzo IPv4 o nome di dominio completo (FQDN) del dispositivo.

     - **Cluster ad alta disponibilità di Server di integrazione**. Immettere l'indirizzo IP e la porta del bilanciatore del carico che fa parte del cluster.

   - **Usa un elenco personalizzato di indirizzi SVM**. Creare un elenco di SVM a cui Light Agent può connettersi. Specificare l'indirizzo IP in formato IPv4 o il nome di dominio completo (FQDN) di SVM. Ogni voce di elenco deve essere immessa su una nuova riga o separata dalla voce precedente da un carattere di punto e virgola (**;**).

     > Nell'elenco degli indirizzi SVM, specificare solo i nomi di dominio completi (FQDN) a cui corrisponde un singolo indirizzo IP. L'utilizzo di un nome di dominio completo che corrisponda a più indirizzi IP può causare errori nella soluzione.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare il rilevamento delle SVM da parte di Light Agent in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Modalità Light Agent** → **Impostazioni di rilevamento SVM**.

5. Selezionare un metodo di rilevamento delle SVM.

   - **Usa server di integrazione**. Immettere le impostazioni per la connessione al Server di integrazione in base all'infrastruttura:

     - **Singolo Server di integrazione**. Immettere le impostazioni di connessione al Server di integrazione: indirizzo IPv4 o nome di dominio completo (FQDN) del dispositivo.

     - **Cluster ad alta disponibilità di Server di integrazione**. Immettere l'indirizzo IP e la porta del bilanciatore del carico che fa parte del cluster.

- **Usa un elenco personalizzato di indirizzi SVM**. Creare un elenco di SVM a cui Light Agent può connettersi. Specificare l'indirizzo IP in formato IPv4 o il nome di dominio completo (FQDN) di SVM. Ogni voce di elenco deve essere immessa su una nuova riga o separata dalla voce precedente da un carattere di punto e virgola (**;**).

  Nell'elenco degli indirizzi SVM, specificare solo i nomi di dominio completi (FQDN) a cui corrisponde un singolo indirizzo IP. L'utilizzo di un nome di dominio completo che corrisponda a più indirizzi IP può causare errori nella soluzione.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare il rilevamento delle SVM da parte di Light Agent nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, in **Modalità Light Agent**, fare clic sul riquadro **Impostazioni di rilevamento SVM**.
3. Selezionare un metodo di rilevamento delle SVM.
   - **Usa server di integrazione**. Immettere le impostazioni per la connessione al Server di integrazione in base all'infrastruttura:
     - **Singolo Server di integrazione**. Immettere le impostazioni di connessione al Server di integrazione: indirizzo IPv4 o nome di dominio completo (FQDN) del dispositivo.
     - **Cluster ad alta disponibilità di Server di integrazione**. Immettere l'indirizzo IP e la porta del bilanciatore del carico che fa parte del cluster.
   - **Usa un elenco personalizzato di indirizzi SVM**. Creare un elenco di SVM a cui Light Agent può connettersi. Specificare l'indirizzo IP in formato IPv4 o il nome di dominio completo (FQDN) di SVM. Ogni voce di elenco deve essere immessa su una nuova riga o separata dalla voce precedente da un carattere di punto e virgola (**;**).

     Nell'elenco degli indirizzi SVM, specificare solo i nomi di dominio completi (FQDN) a cui corrisponde un singolo indirizzo IP. L'utilizzo di un nome di dominio completo che corrisponda a più indirizzi IP può causare errori nella soluzione.
4. Salvare le modifiche.

Configurazione dell'algoritmo di selezione delle SVM per Light Agent

L'infrastruttura dell'organizzazione può avere più SVM distribuite a cui i Light Agent possono connettersi. Per bilanciare il carico sulla rete e le risorse dell'infrastruttura virtuale, è necessario distribuire i Light Agent tra le SVM.

Algoritmi di selezione SVM

I Light Agent possono utilizzare i seguenti algoritmi di selezione SVM per la connessione: Algoritmo standard (predefinito) e Algoritmo esteso.

Algoritmi di selezione SVM

Algoritmo standard	Algoritmo esteso
Se viene utilizzato questo algoritmo, dopo l'installazione e l'avvio, Light Agent nella macchina virtuale sceglie di connettersi a una SVM *locale* per quanto riguarda Light Agent. Se non viene trovata una SVM locale adatta per la connessione, Light Agent seleziona una SVM a cui è connesso il minor numero di Light Agent, indipendentemente dalla posizione della SVM nell'infrastruttura virtuale. L'applicazione non determina se la SVM è locale rispetto a Light Agent se per il Server di protezione nella SVM è abilitata la modalità di protezione dell'infrastruttura di grandi dimensioni. In questo caso, è consigliabile utilizzare l'algoritmo esteso di selezione SVM e selezionare il Server di integrazione come metodo di individuazione SVM. Il fatto che una SVM sia considerata locale rispetto a un Light Agent dipende dal tipo di infrastruttura virtuale.	Se viene applicato questo algoritmo, è possibile definire le seguenti impostazioni di selezione SVM: • se considerare o ignorare la posizione delle SVM nell'infrastruttura quando si scelgono le SVM per la connessione • se viene considerata la posizione della SVM, il metodo per determinare la località della SVM rispetto a Light Agent Se i Light Agent ignorano la posizione delle SVM nell'infrastruttura, i Light Agent potranno connettersi a qualsiasi SVM disponibile per la connessione. Se i Light Agent devono considerare la posizione delle SVM nell'infrastruttura, è necessario selezionare il tipo di percorso SVM da considerare quando si determina la località della SVM rispetto a Light Agent. Il fatto che una SVM sia considerata locale rispetto a Light Agent dipende dal tipo di infrastruttura virtuale. Se i Light Agent considerano la posizione delle SVM nell'infrastruttura quando scelgono a quale SVM connettersi, possono connettersi solo alle SVM locali. Ad esempio, se si specifica un cluster di hypervisor come tipo di percorso SVM, tutte le SVM distribuite in questo cluster di hypervisor saranno considerate locali rispetto a Light Agent e Light Agent potrà connettersi solo a una di queste SVM. Se non sono disponibili SVM per la connessione nello stesso cluster in cui è in esecuzione Light Agent, Light Agent non si connette a una SVM. Quando selezionano le SVM, i Light Agent considerano anche il numero di Light Agent connessi per garantire che i Light Agent siano distribuiti equamente tra le SVM disponibili per la connessione. Se Light Agent utilizza l'algoritmo esteso di selezione SVM, il metodo di individuazione SVM è impostato su Elenco indirizzi SVM e nella SVM è abilitata la modalità di protezione dell'infrastruttura di grandi dimensioni, la connessione di un Light Agent a questa SVM è possibile solo se il percorso SVM viene ignorato.
Basis Dynamix Enterprise	
In un'infrastruttura virtuale basata su Basis Dynamix Enterprise, la SVM considerata locale rispetto a un Light Agent è la SVM distribuita nello stesso nodo della macchina virtuale in cui è installato Light Agent.	In un'infrastruttura virtuale basata su Basis Dynamix Enterprise, una SVM può essere considerata locale rispetto a Light Agent in uno qualsiasi dei seguenti casi: • Una SVM è distribuita nello stesso nodo della macchina virtuale in cui è installato Light Agent. • Una SVM è distribuita nella stessa zona della macchina virtuale in cui è installato Light Agent. • Una SVM è distribuita nello stesso data center della macchina virtuale in cui è installato Light Agent.
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer e Basis Dynamix Standard	

Algoritmo standard	Algoritmo esteso
In un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard, la SVM considerata locale rispetto a un Light Agent è la SVM distribuita sullo stesso hypervisor della macchina virtuale in cui è installato Light Agent.	In un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard, una SVM può essere considerata locale rispetto a Light Agent in uno qualsiasi dei seguenti casi: • Una SVM è distribuita sullo stesso hypervisor della macchina virtuale in cui è installato Light Agent. • Una SVM è distribuita nello stesso cluster di hypervisor della macchina virtuale in cui è installato Light Agent. • Una SVM è distribuita nello stesso data center della macchina virtuale in cui è installato Light Agent.
SVM OpenStack e VK Private Cloud	
In un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud, è possibile specificare come determinare la località della SVM rispetto a Light Agent utilizzando il parametro `StandardAlgorithmSvmLocality` nella sezione `HypervisorSpecificSettings:Openstack` del file di configurazione appsettings.json del Server di integrazione. A seconda della versione del Server di integrazione, il file si trova in uno dei seguenti percorsi: • /var/opt/kaspersky/viis/common/ per il Server di integrazione basato su Linux • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ per il Server di integrazione basato su Windows Il parametro `StandardAlgorithmSvmLocality` può assumere i seguenti valori: • `ServerGroup` – se viene selezionato questo valore, la SVM è considerata locale rispetto a Light Agent se si trova all'interno dello stesso gruppo di server della macchina virtuale in cui è installato Light Agent. Questo valore viene utilizzato per impostazione predefinita. • `Project` – se viene selezionato questo valore, la SVM è considerata locale rispetto a Light Agent se è distribuita all'interno dello stesso progetto OpenStack della macchina virtuale in cui è installato Light Agent. • `AvailabilityZone` – se viene selezionato questo valore, la SVM è considerata locale rispetto a Light Agent se si trova all'interno della stessa zona di disponibilità della macchina virtuale in cui è installato Light Agent.	In un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud, una SVM può essere considerata locale rispetto a Light Agent in uno qualsiasi dei seguenti casi: • Una SVM si trova nello stesso gruppo di server della macchina virtuale in cui è installato Light Agent. • Una SVM è distribuita nello stesso progetto OpenStack della macchina virtuale in cui è installato Light Agent. • Una SVM si trova nella stessa zona di disponibilità della macchina virtuale in cui è installato Light Agent.

Oltre agli algoritmi di connessione SVM, è possibile regolare la connessione dei Light Agent alle SVM tramite tag.

Configurazione dell'algoritmo di selezione SVM

Come configurare l'algoritmo di selezione delle SVM per Light Agent in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Modalità Light Agent → Algoritmo di selezione SVM**.
4. Selezionare l'algoritmo:
   - **Usa l'algoritmo di selezione SVM standard**. Light Agent seleziona le SVM, distribuite nello stesso hypervisor.
   - **Usa l'algoritmo di selezione SVM esteso**. Light Agent seleziona le SVM distribuite nel tipo di percorso delle SVM selezionato (per impostazione predefinita, **Hypervisor**).

5. Se necessario, selezionare il percorso SVM per l'algoritmo di selezione SVM esteso:

- **Hypervisor**. Light Agent seleziona una SVM a cui connettersi che soddisfi i criteri (a seconda del tipo di infrastruttura virtuale):

  - Le SVM sono distribuite sullo stesso hypervisor della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - La SVM si trova nello stesso gruppo di server della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud).

  - La SVM si trova nello stesso nodo della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale Basis Dynamix Enterprise).

  Se non sono disponibili SVM per la connessione sullo stesso hypervisor o nello stesso gruppo di server in cui si trova la macchina virtuale con Light Agent, Light Agent non si connette alla SVM.

- **Cluster**. Light Agent seleziona una SVM a cui connettersi che soddisfi i criteri (a seconda del tipo di infrastruttura virtuale):

  - Le SVM sono distribuite nello stesso cluster di hypervisor della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Le SVM sono distribuite nello stesso progetto OpenStack della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud).

  - La SVM si trova nella stessa zona della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale Basis Dynamix Enterprise).

  Se non sono disponibili SVM per la connessione nello stesso cluster di hypervisor o nello stesso progetto OpenStack in cui si trova la macchina virtuale con Light Agent, Light Agent non si connette alla SVM.

- **Data center**. Light Agent seleziona una SVM a cui connettersi che soddisfi i criteri (a seconda del tipo di infrastruttura virtuale):

  - Le SVM sono distribuite nello stesso data center della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Le SVM si trovano nella stessa zona di disponibilità della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud).

  - La SVM si trova nello stesso data center della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale Basis Dynamix Enterprise).

Se non sono disponibili SVM per la connessione nello stesso data center o zona di disponibilità in cui si trova la macchina virtuale con Light Agent, quest'ultimo non si connette alla SVM.

- **Ignora**. Light Agent ignora il percorso SVM per la connessione al server di protezione. Light Agent tiene conto di altri criteri: tag, numero di Light Agent connessi a una SVM e così via.

6. Salvare le modifiche.

Come configurare l'algoritmo di selezione delle SVM per Light Agent in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Modalità Light Agent** → **Algoritmo di selezione SVM**.
5. Selezionare l'algoritmo:

   - **Usa l'algoritmo di selezione SVM standard**. Light Agent seleziona le SVM, distribuite nello stesso hypervisor.
   - **Usa l'algoritmo di selezione SVM esteso**. Light Agent seleziona le SVM distribuite nel tipo di percorso delle SVM selezionato (per impostazione predefinita, **Hypervisor**).
6. Se necessario, selezionare il percorso SVM per l'algoritmo di selezione SVM esteso:

   - **Hypervisor**. Light Agent seleziona una SVM a cui connettersi che soddisfi i criteri (a seconda del tipo di infrastruttura virtuale):

     - Le SVM sono distribuite sullo stesso hypervisor della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).
     - La SVM si trova nello stesso gruppo di server della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud).
     - La SVM si trova nello stesso nodo della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale Basis Dynamix Enterprise).

     Se non sono disponibili SVM per la connessione sullo stesso hypervisor o nello stesso gruppo di server in cui si trova la macchina virtuale con Light Agent, Light Agent non si connette alla SVM.

- **Cluster**. Light Agent seleziona una SVM a cui connettersi che soddisfi i criteri (a seconda del tipo di infrastruttura virtuale):

  - Le SVM sono distribuite nello stesso cluster di hypervisor della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Le SVM sono distribuite nello stesso progetto OpenStack della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud).

  - La SVM si trova nella stessa zona della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale Basis Dynamix Enterprise).

  Se non sono disponibili SVM per la connessione nello stesso cluster di hypervisor o nello stesso progetto OpenStack in cui si trova la macchina virtuale con Light Agent, Light Agent non si connette alla SVM.

- **Data center**. Light Agent seleziona una SVM a cui connettersi che soddisfi i criteri (a seconda del tipo di infrastruttura virtuale):

  - Le SVM sono distribuite nello stesso data center della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Le SVM si trovano nella stessa zona di disponibilità della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud).

  - La SVM si trova nello stesso data center della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale Basis Dynamix Enterprise).

  Se non sono disponibili SVM per la connessione nello stesso data center o zona di disponibilità in cui si trova la macchina virtuale con Light Agent, quest'ultimo non si connette alla SVM.

- **Ignora**. Light Agent ignora il percorso SVM per la connessione al server di protezione. Light Agent tiene conto di altri criteri: tag, numero di Light Agent connessi a una SVM e così via.

7. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare l'algoritmo di selezione delle SVM per Light Agent nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .

2. Nella finestra delle impostazioni dell'applicazione, in **Modalità Light Agent**, fare clic sul riquadro **Impostazioni di rilevamento SVM**.

3. Selezionare l'algoritmo:

   - **Usa l'algoritmo di selezione SVM standard**. Light Agent seleziona le SVM, distribuite nello stesso hypervisor.

   - **Usa l'algoritmo di selezione SVM esteso**. Light Agent seleziona le SVM distribuite nel tipo di percorso delle SVM selezionato (per impostazione predefinita, **Hypervisor**).

4. Se necessario, selezionare il percorso SVM per l'algoritmo di selezione SVM esteso:

- **Hypervisor**. Light Agent seleziona una SVM a cui connettersi che soddisfi i criteri (a seconda del tipo di infrastruttura virtuale):

  - Le SVM sono distribuite sullo stesso hypervisor della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - La SVM si trova nello stesso gruppo di server della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud).

  - La SVM si trova nello stesso nodo della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale Basis Dynamix Enterprise).

  Se non sono disponibili SVM per la connessione sullo stesso hypervisor o nello stesso gruppo di server in cui si trova la macchina virtuale con Light Agent, Light Agent non si connette alla SVM.

- **Cluster**. Light Agent seleziona una SVM a cui connettersi che soddisfi i criteri (a seconda del tipo di infrastruttura virtuale):

  - Le SVM sono distribuite nello stesso cluster di hypervisor della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Le SVM sono distribuite nello stesso progetto OpenStack della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud).

  - La SVM si trova nella stessa zona della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale Basis Dynamix Enterprise).

  Se non sono disponibili SVM per la connessione nello stesso cluster di hypervisor o nello stesso progetto OpenStack in cui si trova la macchina virtuale con Light Agent, Light Agent non si connette alla SVM.

- **Data center**. Light Agent seleziona una SVM a cui connettersi che soddisfi i criteri (a seconda del tipo di infrastruttura virtuale):

  - Le SVM sono distribuite nello stesso data center della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale basata su Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer o Basis Dynamix Standard).

  - Le SVM si trovano nella stessa zona di disponibilità della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale in esecuzione sulla piattaforma OpenStack o VK Private Cloud).

  - La SVM si trova nello stesso data center della macchina virtuale in cui è installato Light Agent (in un'infrastruttura virtuale Basis Dynamix Enterprise).

Se non sono disponibili SVM per la connessione nello stesso data center o zona di disponibilità in cui si trova la macchina virtuale con Light Agent, quest'ultimo non si connette alla SVM.

- **Ignora**. Light Agent ignora il percorso SVM per la connessione al server di protezione. Light Agent tiene conto di altri criteri: tag, numero di Light Agent connessi a una SVM e così via.

5. Salvare le modifiche.

Distribuzione delle connessioni dei Light Agent alle SVM (tag)

Più Light Agent possono connettersi a una SVM. Per bilanciare le connessioni di Light Agent, è possibile specificare un elenco separato di SVM. Se si utilizza un server di integrazione per il rilevamento delle SVM, è possibile utilizzare *tag* per bilanciare le connessioni di Light Agent alle SVM. In altre parole, per un Light Agent è possibile assegnare un elenco di SVM per la connessione tramite un tag. A tale scopo, è necessario assegnare un tag al Light Agent e specificare questo tag nelle impostazioni SVM. Per informazioni dettagliate sulla specifica dei tag nelle impostazioni SVM, consultare la Guida di Kaspersky Security for Virtualization Light Agent.

Esempio: la soluzione Kaspersky Endpoint Detection and Response Optimum viene distribuita nell'infrastruttura per gli host di macchine virtuali designati. In questo caso, è possibile assegnare il tag `[EDROptimum]` a Light Agent per farlo connettere alle SVM a cui è stata aggiunta la chiave di licenza di EDR Optimum (EDR Optimum Add-on). In seguito a questa operazione, è possibile utilizzare la funzionalità EDR Optimum nella macchina virtuale con Light Agent. Quando si connette Light Agent a una SVM senza una chiave di licenza di EDR Optimum, la funzionalità Kaspersky Endpoint Detection and Response Optimum non è disponibile.

Come assegnare un tag di connessione alle SVM a un Light Agent in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Modalità Light Agent → Tag connessione SVM**.
4. Selezionare la casella di controllo **Usa tag di connessione** e immettere il tag della connessione a SVM.

   Come tag, è possibile immettere una stringa di testo con una lunghezza massima di 255 caratteri. È possibile utilizzare qualsiasi carattere tranne il carattere `;`.
5. Salvare le modifiche.

Come assegnare un tag di connessione alle SVM a un Light Agent in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Modalità Light Agent → Tag connessione SVM**.

5. Selezionare la casella di controllo **Usa tag connessione** e immettere il tag della connessione a SVM.

   Come tag, è possibile immettere una stringa di testo con una lunghezza massima di 255 caratteri. È possibile utilizzare qualsiasi carattere tranne il carattere `;`.

6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come assegnare un tag di connessione alle SVM a un Light Agent nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, in **Modalità Light Agent**, fare clic sul riquadro **Tag connessione SVM**.
3. Selezionare la casella di controllo **Usa tag connessione** e immettere il tag della connessione a SVM.

   Come tag, è possibile immettere una stringa di testo con una lunghezza massima di 255 caratteri. È possibile utilizzare qualsiasi carattere tranne il carattere `;`.

4. Salvare le modifiche.

Protezione della connessione tra un Light Agent e SVM

È possibile configurare il criptaggio della connessione tra i Light Agent e il server di protezione. A tale scopo, è necessario abilitare il criptaggio del canale dati tra il Light Agent e il server di protezione nelle impostazioni del server di protezione sulla SVM e nelle impostazioni di Light Agent.

Un Light Agent per cui è abilitata la protezione della connessione può connettersi solo alle SVM per cui è abilitato il criptaggio del canale dati tra Light Agent e server di protezione. Un Light Agent per cui la protezione della connessione è disabilitata può connettersi solo alle SVM per cui il criptaggio dei canali è disabilitato o è consentita una connessione non sicura tra il server di protezione e il Light Agent.

Per informazioni dettagliate sulla configurazione della protezione della connessione nel server di protezione, consultare la Guida di Kaspersky Security for Virtualization Light Agent.

La protezione della connessione tramite il criptaggio può ridurre le prestazioni di Kaspersky Security for Virtualization Light Agent.

Come configurare la protezione della connessione in un Light Agent in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Modalità Light Agent → Protezione della connessione**.
4. Selezionare la casella di controllo **Cripta il canale dati tra Light Agent e il server di protezione**.
5. Salvare le modifiche.

Come configurare la protezione della connessione in un Light Agent in Web Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Modalità Light Agent** → **Protezione della connessione**.
5. Selezionare la casella di controllo **Cripta il canale dati tra Light Agent e il server di protezione**.
6. Per applicare il criterio ai computer, chiudere le icone del lucchetto e salvare le modifiche.

Come configurare la protezione della connessione in un Light Agent nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, in **Modalità Light Agent**, fare clic sul riquadro **Protezione della connessione**.
3. Selezionare la casella di controllo **Cripta il canale dati tra Light Agent e il server di protezione**.
4. Salvare le modifiche.

Attivazione di Light Agent

Se Kaspersky Endpoint Security viene utilizzato in modalità Light Agent per proteggere gli ambienti virtuali, non è necessario attivare l'applicazione separatamente. Per attivare l'applicazione, è necessario aggiungere una chiave di licenza alla SVM. È possibile aggiungere una chiave di licenza a SVM utilizzando l'apposita attività nella console di Kaspersky Security Center. Non è possibile gestire le chiavi di licenza nell'interfaccia di Light Agent, tuttavia è possibile visualizzare le informazioni sulla licenza (vedere la figura seguente). È inoltre possibile visualizzare le informazioni sulla licenza di Light Agent dalla riga di comando (vedere le istruzioni di seguito). Light Agent ottiene queste informazioni dalla SVM. Per informazioni dettagliate sull'attivazione della soluzione e sulla gestione delle chiavi di licenza, consultare la Guida di Kaspersky Security for Virtualization Light Agent.

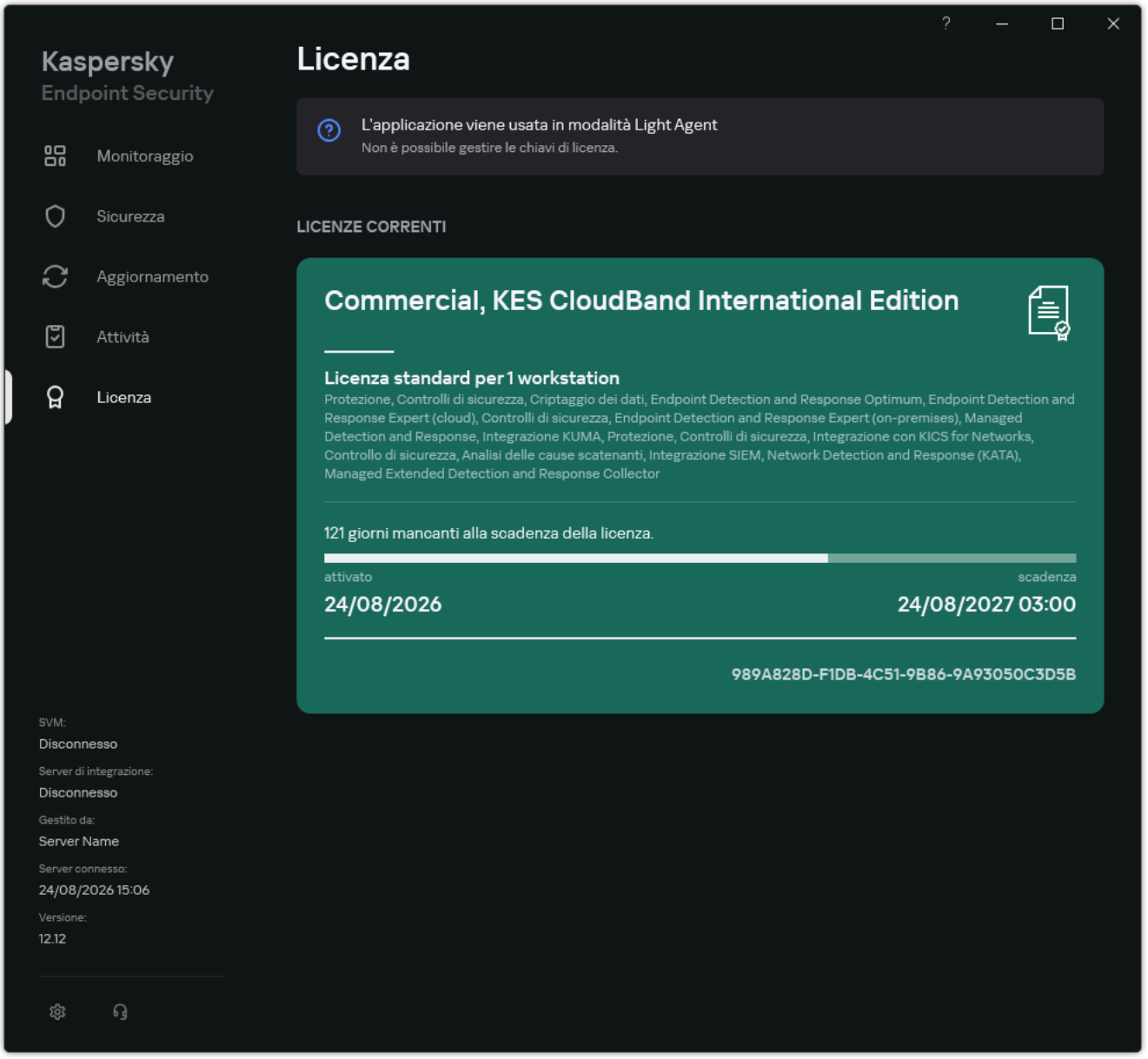
Per visualizzare le informazioni sulle licenze di Light Agent:

1. Eseguire l'interprete della riga di comando (cmd) come amministratore.
2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

3. Eseguire il seguente comando:

```
avp.com LICENSE /CHECK
```

In seguito a questa operazione, Kaspersky Endpoint Security mostra le informazioni sulla licenza: l'indirizzo della SVM a cui è connesso il Light Agent, il numero di giorni mancanti alla scadenza della licenza e altre informazioni. In caso di problemi durante l'attivazione di Light Agent, consultare la Knowledge Base dell'Assistenza tecnica.



Finestra Gestione delle licenze

Guida alla migrazione da KSVLA Light Agent a KES Light Agent

Kaspersky Security for Virtualization 5.2 Light Agent include il componente Light Agent for Windows 5.2 (di seguito denominato anche "KSVLA Light Agent"). In Kaspersky Security for Virtualization Light Agent 6.2, Kaspersky Endpoint Security in modalità Light Agent viene utilizzato come componente Light Agent. Per aggiornare la soluzione alla versione 6.2, è necessario eseguire la migrazione da Light Agent 5.2 a Kaspersky Endpoint Security in modalità Light Agent (di seguito denominato anche "KES Light Agent"). Per informazioni dettagliate sull'aggiornamento della versione della soluzione Kaspersky Security for Virtualization Light Agent, vedere la Guida di Kaspersky Security for Virtualization Light Agent.

Requisiti software

Prima di iniziare la migrazione da KSVLA Light Agent a KES Light Agent, assicurarsi che la macchina virtuale soddisfi i requisiti hardware e software di Kaspersky Endpoint Security for Windows. Gli elenchi delle versioni dei sistemi operativi supportate sono diversi per KES e KSWS. Ad esempio, KES non supporta i server in cui viene eseguito Windows Server 2003.

Requisiti software minimi per la migrazione da KSVLA Light Agent a KES Light Agent:

- Kaspersky Endpoint Security for Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (inclusi i componenti Server di protezione e Server di integrazione).
- Kaspersky Security Center 14.2

  Se è installata una versione precedente di Kaspersky Security Center, aggiornarla alla versione 14.2 o successiva. In questa versione di Kaspersky Security Center, la Conversione guidata di criteri e attività in batch consente di eseguire la migrazione dei criteri in un profilo anziché in un criterio. In questa versione di Kaspersky Security Center, la Conversione guidata di criteri e attività in batch consente inoltre di eseguire la migrazione di una gamma più ampia di impostazioni dei criteri.

Passaggi della migrazione

La migrazione da KSVLA Light Agent a KES Light Agent viene eseguita in modo semiautomatico. Ciò è necessario a causa delle diverse architetture delle applicazioni.

Eseguire la migrazione da KSVLA Light Agent a KES Light Agent nel seguente ordine:

1. **Eseguire la migrazione delle attività e dei criteri di KSVLA Light Agent**

   Per eseguire la migrazione delle impostazioni dei criteri, è necessario eseguire la Conversione guidata di criteri e attività in batch (la migrazione guidata). Dopo aver eseguito la migrazione delle impostazioni dei criteri, è necessario configurare manualmente le impostazioni che la migrazione guidata non può migrare automaticamente (ad esempio, le impostazioni di aggiornamento del database). Dopo la migrazione, si consiglia inoltre di verificare se la migrazione guidata ha eseguito correttamente la migrazione di tutte le impostazioni.

   > Se la protezione tramite password è abilitata per limitare l'accesso a KSVLA Light Agent, prima di installare KES Light Agent è necessario disabilitare la protezione tramite password nel criterio di KSVLA Light Agent. Non è possibile immettere la password di disinstallazione nelle impostazioni del pacchetto di installazione di KES Light Agent. Dopo aver completato l'installazione di KES Light Agent prima di KSVLA Light Agent, è necessario abilitare la protezione tramite password nel criterio di KES.

2. **Installare Kaspersky Endpoint Security in modalità Light Agent**

   È possibile installare KES Light Agent nei seguenti modi:

   - Installazione di KES Light Agent dopo la rimozione di KSVLA Light Agent (opzione consigliata)
   - Installazione di KES Light Agent prima di KSVLA Light Agent

3. **Verifica che l'applicazione funzioni correttamente dopo la migrazione**

   Dopo la migrazione da KSVLA Light Agent a KES Light Agent, assicurarsi che l'applicazione funzioni correttamente. Attivare il criterio convertito. Controllare lo stato della macchina virtuale nella console Kaspersky Security Center (deve essere *OK*). Verificare che non vengano segnalati errori per l'applicazione, controllare anche l'ora dell'ultima connessione alla SVM e lo stato di protezione della macchina virtuale. Non è necessario attivare Light Agent poiché la chiave di licenza viene aggiunta alla SVM.

Installazione di KES Light Agent anziché di KSVLA Light Agent

È possibile installare KES Light Agent nei seguenti modi:

- Installazione di KES Light Agent dopo la rimozione di KSVLA Light Agent (opzione consigliata)
- Installazione di KES Light Agent prima di KSVLA Light Agent

Rimozione di KSVLA Light Agent

È possibile rimuovere l'applicazione da remoto utilizzando l'attività *Installa l'applicazione in remoto*, in locale nella macchina virtuale o nel modello di macchina virtuale. Dopo la rimozione di KSVLA Light Agent, potrebbe essere necessario riavviare la macchina virtuale.

Dopo aver rimosso KSVLA Light Agent, installare KES Light Agent utilizzando qualsiasi metodo idoneo.

Se la protezione tramite password è abilitata per limitare l'accesso a KSVLA Light Agent, prima di installare KES Light Agent è necessario disabilitare la protezione tramite password nel criterio di KSVLA Light Agent. Non è possibile immettere la password di disinstallazione nelle impostazioni del pacchetto di installazione di KES Light Agent. Dopo aver completato l'installazione di KES Light Agent prima di KSVLA Light Agent, è necessario abilitare la protezione tramite password nel criterio di KES.

Quando si installa Kaspersky Endpoint Security, è necessario selezionare la modalità **Light Agent per proteggere gli ambienti virtuali**. Prima di installare KES Light Agent in una macchina virtuale, il programma di installazione rileva KSVLA Light Agent come software incompatibile e lo rimuove. La migrazione della configurazione di KSVLA Light Agent non è supportata. Quando si installa KES Light Agent, il set di componenti da installare è determinato dalla selezione nelle proprietà del pacchetto di installazione o nell'installazione guidata. Dopo la rimozione di KSVLA Light Agent, è necessario riavviare la macchina virtuale.

Le impostazioni e le attività di KSVLA Light Agent non vengono migrate quando si installa KES Light Agent. Per eseguire la migrazione delle impostazioni e delle attività, eseguire la Conversione guidata di criteri e attività in batch.

È possibile consultare l'elenco di componenti installati nella sezione **Sicurezza** dell'interfaccia dell'applicazione, con il comando `status` o nella console di Kaspersky Security Center nelle proprietà del computer. È possibile modificare il set di componenti dopo l'installazione utilizzando *Modifica i componenti dell'applicazione*.

Corrispondenza dei componenti di KSVLA Light Agent e KES Light Agent

I set di componenti di KSVLA Light Agent e KES Light Agent sono praticamente gli stessi. KES Light Agent ha più impostazioni rispetto a KSVLA Light Agent. Dopo la migrazione, le nuove impostazioni avranno valori predefiniti.

Corrispondenza dei componenti di KSVLA Light Agent e KES Light Agent

Light Agent 5.2	KES Light Agent
Kernel di scansione	Kernel dell'applicazione
Anti-Virus file	Protezione minacce file
Anti-Virus posta	Protezione minacce di posta
Anti-Virus Web	Protezione minacce Web
Firewall	Firewall
Prevenzione attacchi di rete	Protezione minacce di rete
Controllo privilegi applicazioni	Prevenzione Intrusioni Host
Controllo degli avvii delle applicazioni	Controllo applicazioni
Controllo Web	Controllo Web
Controllo dispositivi	Controllo dispositivi
System Watcher	In Kaspersky Endpoint Security, questo componente è suddiviso nei seguenti componenti: • Prevenzione Exploit • Rilevamento del Comportamento • Motore di Remediation
Monitoraggio integrità di sistema	Monitoraggio integrità di sistema

Light Agent 5.2	KES Light Agent
Integrazione con Kaspersky Endpoint Agent	*(non supportato)* A partire da Kaspersky Endpoint Security for Windows 11.9.0, il pacchetto di distribuzione di Kaspersky Endpoint Agent non fa più parte del kit di distribuzione.
Protezione AMSI	Protezione AMSI

Migrazione di attività e criteri di KSVLA Light Agent

È possibile eseguire la migrazione delle impostazioni dei criteri e delle attività di KSVLA Light Agent utilizzando la Conversione batch guidata criteri e attività (di seguito denominata anche "Migrazione guidata").

La migrazione guidata di KSVLA Light Agent è disponibile solo in Administration Console (MMC). Non è possibile migrare le impostazioni dei criteri e delle attività in Web Console e Cloud Console.

La migrazione di criteri e attività comporta le seguenti considerazioni speciali:

- Un nuovo criterio ha il nome *<Criterio> (convertito)*.
- Il nuovo criterio presenta lo stato *Criterio inattivo*.
- Il divieto di modifica delle impostazioni (il "lucchetto") non viene migrato. La migrazione guidata imposta i valori predefiniti.
- I profili criterio non vengono migrati. È necessario aggiungere manualmente i profili criterio.
- Gestione delle aree attendibili migliorata. In KSVLA Light Agent era possibile aggiungere esclusioni predefinite solo durante la creazione di un criterio. Successivamente, nelle proprietà del criterio, è possibile configurare le esclusioni predefinite aggiunte in precedenza o aggiungere manualmente le esclusioni. Non è possibile aggiungere esclusioni predefinite nelle proprietà dei criteri. In KES Light Agent, le esclusioni predefinite sono disponibili sia durante la creazione del criterio che nelle proprietà del criterio creato. È inoltre possibile selezionare le esclusioni predefinite nel pacchetto di installazione.
- La configurazione dell'interfaccia utente dell'applicazione in Kaspersky Endpoint Security è stata spostata dal programma di installazione al criterio. Se è ad esempio necessario nascondere l'interfaccia utente dell'applicazione, gestire le impostazioni dei criteri.
- I set di funzionalità per la configurazione del controllo degli accessi in base ai diritti (RBAC) sono diversi in Kaspersky Endpoint Security e KSVLA Light Agent. È necessario configurare da zero i diritti di accesso degli utenti alle aree funzionali.

Come utilizzare Conversione guidata criteri e attività per migrare le impostazioni dei criteri di KSVLA Light Agent

1. In Administration Console, selezionare Administration Server e fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
2. Selezionare **Tutte le attività → Conversione guidata in batch criteri e attività**.

Viene avviata la procedura Conversione guidata criteri e attività. Attenersi alle istruzioni della procedura guidata.

Passaggio 1. Selezione dell'applicazione con cui è necessario convertire i criteri e le attività

In questa fase, è necessario selezionare Kaspersky Endpoint Security for Windows. Procedere con il passaggio successivo.

Passaggio 2. Conversione dei criteri

Selezionare il criterio di Kaspersky Security for Virtualization 5.2 Light Agent for Windows che si desidera convertire. Procedere con il passaggio successivo.

A questo punto, la migrazione guidata inizia a convertire i criteri. Durante la conversione, la Migrazione guidata richiede di accettare l'Informativa di KSN. Un nuovo criterio ha il nome *<Criterio> (convertito)*.

Passaggio 3. Conversione delle attività

La migrazione guidata crea nuove attività per Kaspersky Endpoint Security for Windows. Nell'elenco delle attività, selezionare le attività di KSVLA Light Agent che si desidera creare per Kaspersky Endpoint Security. Le nuove attività verranno denominate *<Nome attività> (convertito)*. Procedere con il passaggio successivo.

Passaggio 4. Completamento della procedura guidata

Terminare la procedura guidata.

Dopo la migrazione di un criterio, è necessario aprire le proprietà del criterio, verificarne le impostazioni e salvare il criterio. Se non si completano questi passaggi, KES Light Agent potrebbe ignorare il criterio convertito.

Prestare particolare attenzione alla migrazione delle impostazioni di connessione SVM di Light Agent, degli elenchi di esclusione, delle applicazioni attendibili, degli indirizzi Web attendibili e delle regole di Controllo applicazioni.

Migrazione della configurazione [KSVLA Light Agent+KEA] alla configurazione [KES Light Agent+agente integrato]

Per supportare l'utilizzo di Kaspersky Endpoint Security for Windows come parte di EDR (KATA), EDR Optimum e Kaspersky Sandbox, all'applicazione è stato aggiunto un agente integrato. Non è più necessaria un'applicazione Kaspersky Endpoint Agent separata per utilizzare tali soluzioni.

Durante la migrazione da KSVLA Light Agent a KES Light Agent, le soluzioni EDR (KATA), EDR Optimum e Kaspersky Sandbox continuano a funzionare con gli agenti integrati di Kaspersky Endpoint Security. Inoltre, Kaspersky Endpoint Agent verrà rimosso dal computer.

Prima di eseguire la migrazione da KSVLA Light Agent a KES Light Agent, è necessario aggiornare tutti i componenti di Kaspersky Security for Virtualization alla versione 6.2, inclusi il Server di protezione e il Server di integrazione. Per informazioni dettagliate sull'aggiornamento della versione della soluzione Kaspersky Security for Virtualization Light Agent, vedere la Guida di Kaspersky Security for Virtualization Light Agent.

La migrazione della configurazione [KSVLA Light Agent+KEA] a [KES Light Agent+agente integrato] prevede i seguenti passaggi:

1. **Migrazione di criterio e attività**

   La migrazione dei criteri e delle attività di [KSVLA Light Agent+KEA] a [KES Light Agent+agente integrato] prevede i seguenti passaggi:

   1. Migrazione di criteri e attività da KSVLA Light Agenta KES Light Agent tramite la Conversione guidata criteri e attività (disponibile solo in Administration Console (MMC)).

      In seguito a questa operazione, verrà creato un nuovo criterio con il nome *<Criterio> (convertito)*. Vengono create anche nuove attività KES denominate *<Nome attività> (convertito)*.

   2. Migrazione di criteri e attività da KEA a KES tramite la migrazione guidata da Kaspersky Endpoint Agent (disponibile solo su Web Console e Cloud Console).

      Di conseguenza, viene creato un nuovo criterio denominato *<Nome del criterio Kaspersky Endpoint Security> & <Nome del criterio Kaspersky Endpoint Agent>*. Vengono create anche nuove attività e attività KES.

2. **Migrazione da KSVLA Light Agent a KES Light Agent**

   La migrazione da KSVLA Light Agent a KES Light Agent implica l'installazione di KES Light Agent anziché KSVLA Light Agent.

   In genere, gli amministratori abilitano la protezione tramite password per limitare l'accesso a KSVLA Light Agent e KEA. È possibile immettere la password di disinstallazione di KEA solo nelle proprietà dell'attività *Installa l'applicazione in remoto*. Per la migrazione, è necessario disabilitare la protezione tramite password per KSVLA Light Agent.

   Per eseguire la migrazione, è necessario selezionare i componenti necessari per supportare le soluzioni Detection and Response come parte di Kaspersky Endpoint Security. Dopo aver installato l'applicazione, Kaspersky Endpoint Security passa all'utilizzo dell'agente integrato e rimuove Kaspersky Endpoint Agent.

3. **Funzionalità di concessione di licenze**

   Se l'applicazione viene utilizzato in modalità Light Agent, non è necessario attivare l'applicazione. Per attivare l'applicazione, è necessario aggiungere una chiave di licenza alla SVM. È inoltre necessario aggiungere la chiave di licenza per l'attivazione di funzionalità aggiuntive (ad esempio EDR Optimum) nella SVM. In altre parole, durante la migrazione, la gestione delle licenze delle funzionalità viene eseguita automaticamente.

4. **Verifica dell'integrità di Kaspersky Endpoint Detection and Response Optimum e Kaspersky Sandbox**

Se dopo l'upgrade il computer presenta lo stato *Critico* nella console di Kaspersky Security Center:

- Accertarsi che nel computer sia installato Network Agent versione 13.2 o successiva.
- Controllare lo stato operativo dell'agente integrato visualizzando *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non installato*, installare il componente tramite l'attività *Modifica i componenti dell'applicazione*.
- Accertarsi di accettare l'Informativa di Kaspersky Security Network nel nuovo criterio di Kaspersky Endpoint Security for Windows.
- Assicurarsi che la funzionalità EDR Optimum sia attivata utilizzando il *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non incluso nella licenza*, accertarsi che la funzionalità di distribuzione della chiave di licenza automatica di EDR Optimum sia attivata.
- Controllare lo stato della connessione della macchina virtuale alla SVM. È possibile ottenere informazioni sullo stato della connessione di Light Agent alla SVM in Kaspersky Endpoint Security o utilizzando il comando dell'applicazione.

Gestione dell'applicazione dalla riga di comando

È possibile gestire Kaspersky Endpoint Security dalla riga di comando. È possibile visualizzare l'elenco dei comandi per la gestione dell'applicazione eseguendo il comando `avp.com HELP`. Per leggere la sintassi di un comando specifico, immettere `avp.com HELP <command>`.

I caratteri speciali nel comando devono essere preceduti da un carattere di escape. Per forzare i caratteri `&`, `|`, `(`, `)`, `<`, `>`, `^`, utilizzare il carattere `^` (ad esempio, per usare il carattere `&`, immettere `^&`). Per forzare il carattere `%` con un carattere di escape, inserire `%%`.

In alternativa al valore `1`, è possibile utilizzare i valori `yes`, `on`, `enable`, `enabled` e `true`. In alternativa al valore `0`, è possibile utilizzare i valori `no`, `off`, `disable`, `disabled` e `false`.

Setup. Installazione dell'applicazione

L'installazione dell'applicazione dalla riga di comando prevede i seguenti passaggi:

1. **Scelta di un pacchetto di distribuzione**

   Kaspersky fornisce pacchetti di distribuzione per diverse localizzazioni, compatibili con diverse architetture CPU e comprendenti vari moduli di criptaggio.

   Il kit di distribuzione include i seguenti pacchetti di distribuzione:

   - **AES256**

     Questo pacchetto di distribuzione è destinato all'installazione nei computer con architettura x86/x64. Questo pacchetto di distribuzione contiene strumenti crittografici che implementano l'algoritmo di criptaggio AES (Advanced Encryption Standard) con una lunghezza effettiva della chiave di 256 bit.

   - **AES56**

     Questo pacchetto di distribuzione è destinato all'installazione nei computer con architettura x86/x64. Questo pacchetto di distribuzione contiene strumenti di criptaggio che implementano l'algoritmo di criptaggio AES con una lunghezza della chiave effettiva di 56 bit.

   - **Arm64**

     Questo pacchetto di distribuzione è destinato all'installazione nei computer basati su Arm. Questo pacchetto di distribuzione non è destinato all'installazione nei server.

2. **Trasferimento del pacchetto di distribuzione dell'applicazione nell'archivio del computer**

   Il pacchetto di distribuzione è un archivio a estrazione automatica in formato EXE. Per visualizzare il contenuto del pacchetto di distribuzione, è necessario estrarre l'archivio in una cartella separata. Per installare l'applicazione, sono necessari tutti i file del pacchetto di distribuzione, incluso il file bases.cab.

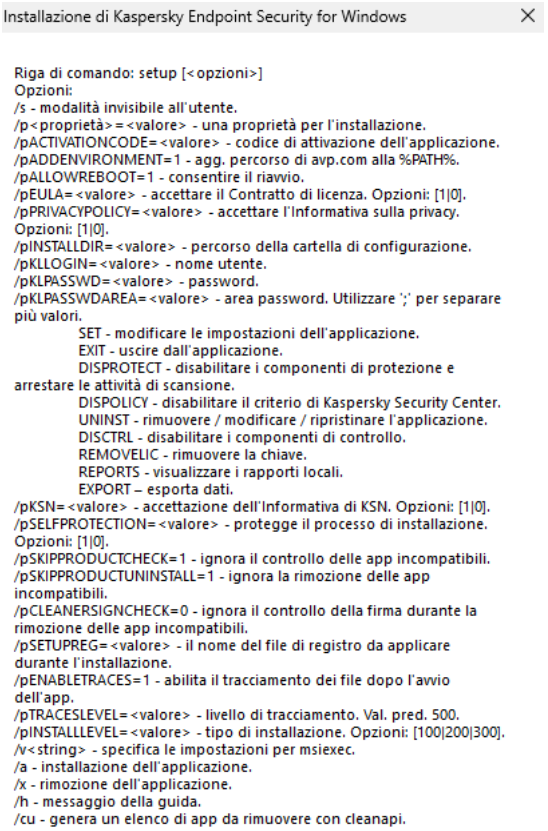
3. **Esecuzione del comando di installazione**

Kaspersky Endpoint Security può essere installato dalla riga di comando in uno dei seguenti modi:

- In modalità interattiva, utilizzando l'Installazione guidata dell'applicazione.
- In modalità automatica. Una volta avviata l'installazione in modalità automatica, l'intervento dell'utente nel processo di installazione non è necessario (disinstallazione automatica). Per installare l'applicazione in modalità automatica, utilizzare le chiavi `/s` e `/qn`.

Prima di installare l'applicazione in modalità automatica, aprire e leggere il Contratto di licenza con l'utente finale e il testo dell'Informativa sulla privacy. Il Contratto di licenza con l'utente finale e il testo dell'Informativa sulla privacy sono inclusi nel kit di distribuzione di Kaspersky Endpoint Security. È possibile procedere all'installazione dell'applicazione solo dopo aver letto, compreso e accettato i termini e le disposizioni del Contratto di licenza con l'utente finale, aver compreso e accettato che i dati vengano elaborati e trasmessi (anche a paesi di terzi) secondo quanto previsto dall'Informativa sulla privacy e aver letto e compreso l'Informativa sulla privacy. Se non si accettano i termini e le disposizioni del Contratto di licenza con l'utente finale e dell'Informativa sulla privacy, non installare o utilizzare Kaspersky Endpoint Security.

È possibile visualizzare l'elenco dei comandi per l'installazione dell'applicazione eseguendo il comando `/h`. Per assistenza sulla sintassi dei comandi di installazione, digitare `setup_kes.exe /h`. Successivamente, il programma di installazione mostra una finestra con una descrizione delle opzioni dei comandi (vedere la figura riportata di seguito).



Descrizione delle opzioni dei comandi di installazione

Per installare l'applicazione o eseguire l'upgrade di una versione precedente dell'applicazione:

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il pacchetto di distribuzione di Kaspersky Endpoint Security.

3. Eseguire il seguente comando:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

oppure

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

Di conseguenza, l'applicazione viene installata nel computer. È possibile verificare che l'applicazione sia installata e controllare le impostazioni dell'applicazione eseguendo il comando `status`.

Impostazioni di installazione dell'applicazione

`EULA=1`	Accettazione delle condizioni del Contratto di licenza con l'utente finale. Il testo del Contratto di licenza è incluso nel kit di distribuzione di Kaspersky Endpoint Security. L'accettazione delle condizioni del Contratto di licenza con l'utente finale è necessaria per installare l'applicazione o eseguire l'aggiornamento della versione.
`PRIVACYPOLICY=1`	Accettazione dell'Informativa sulla privacy. Il testo dell'Informativa sulla privacy è incluso nel kit di distribuzione di Kaspersky Endpoint Security. Per installare l'applicazione o eseguire l'upgrade della versione dell'applicazione, è necessario accettare la Informativa sulla privacy.
`KSN`	Accettazione o rifiuto della partecipazione a Kaspersky Security Network (KSN). Se per questo parametro non è impostato alcun valore, Kaspersky Endpoint Security richiederà di confermare il consenso o il rifiuto di partecipare a KSN al primo avvio di Kaspersky Endpoint Security. Valori disponibili: • `1` – accettazione della partecipazione a KSN. • `0` – rifiuto della partecipazione a KSN (valore predefinito). Il pacchetto di distribuzione di Kaspersky Endpoint Security è ottimizzato per l'utilizzo con Kaspersky Security Network. Se si è scelto di non per partecipare a Kaspersky Security Network, è necessario aggiornare Kaspersky Endpoint Security subito dopo il completamento dell'installazione.
`CONFIGPATH=<path to the configuration file>`	Installazione dell'applicazione con le impostazioni predefinite. A tale scopo, è necessario caricare un file che definisca le impostazioni di Kaspersky Endpoint Security. È possibile creare un file di configurazione nell'interfaccia locale dell'applicazione.
`ALLOWREBOOT=1`	Riavvio automatico del computer, se necessario dopo l'installazione o l'upgrade dell'applicazione. Se non viene impostato alcun valore per questo parametro, il riavvio automatico del computer viene bloccato. Il riavvio non è richiesto durante l'installazione di Kaspersky Endpoint Security. Il riavvio è richiesto solo se è necessario rimuovere applicazioni incompatibili prima dell'installazione. Potrebbe essere necessario il riavvio anche durante l'aggiornamento della versione dell'applicazione.
`SKIPPRODUCTCHECK=1`	Disabilitare la verifica della presenza di software installato. L'elenco del software che può causare problemi di compatibilità è disponibile nel file incompatible.txt incluso nel kit di distribuzione. Se non viene impostato alcun valore per questo parametro e viene rilevato software nell'elenco, l'installazione di Kaspersky Endpoint Security verrà terminata.

SKIPPRODUCTUNINSTALL=1	Disabilitare la rimozione automatica del software rilevato nell'elenco incompatible.txt. Se non viene impostato alcun valore per questo parametro, Kaspersky Endpoint Security tenta di rimuovere il software che potrebbe causare problemi di compatibilità. Non è possibile abilitare la rimozione automatica del software quando si installa Kaspersky Endpoint Security utilizzando il programma di installazione msiexec. Per rimuovere automaticamente il software che potrebbe causare problemi di compatibilità, utilizzare il file setup_kes.exe.
CLEANERSIGNCHECK=0|1	Verifica delle firme digitali dei file del software rilevati nell'elenco incompatible.txt. Per rimuovere il software, Kaspersky Endpoint Security esegue il file del programma di installazione del software. Se il file del programma di installazione non dispone di una firma digitale, Kaspersky Endpoint Security considera il file non attendibile e interrompe la rimozione del software per evitare l'esecuzione di codice potenzialmente dannoso. Se l'applicazione non è in grado di verificare la firma digitale del file del software rilevato, l'installazione di Kaspersky Endpoint Security viene interrotta con un errore. Il valore predefinito è diverso a seconda del metodo di installazione del software: • 0 indica che la verifica della firma digitale è disabilitata (valore predefinito se distribuito tramite Kaspersky Security Center). • 1 indica che la verifica della firma digitale è abilitata (valore predefinito se l'applicazione viene installata in locale).
STANDALONEMODE=1	Installazione dell'applicazione nella configurazione Endpoint Detection and Response Agent (EDR Agent) per l'integrazione con le soluzioni Kaspersky Endpoint Detection and Response (KATA) o Kaspersky Endpoint Detection and Response Expert (on-premises). Questa configurazione è necessaria se nell'organizzazione viene distribuita una Endpoint Protection Platform (EPP) di terzi insieme a una soluzione di classe Kaspersky Endpoint Detection and Response. Ciò rende Kaspersky Endpoint Security nella configurazione Endpoint Detection and Response Agent compatibile con le applicazioni EPP di terzi.
KLLOGIN	Impostare il nome utente per l'accesso alle funzionalità e alle impostazioni di Kaspersky Endpoint Security (componente Protezione tramite password). Il nome utente viene impostato insieme alle impostazioni KLPASSWD e KLPASSWDAREA. Per impostazione predefinita, viene utilizzato il nome utente KLAdmin.
KLPASSWD	Specificare una password per accedere a funzionalità e impostazioni di Kaspersky Endpoint Security (la password è specificata insieme ai parametri KLLOGIN e KLPASSWDAREA). Se è stata specificata una password, ma non è stato specificato un nome utente con il parametro KLLOGIN, per impostazione predefinita viene utilizzato il nome utente KLAdmin.
KLPASSWDAREA	Specificare l'ambito della password per accedere a Kaspersky Endpoint Security. Quando un utente tenta di eseguire un'azione inclusa in questo ambito, Kaspersky Endpoint Security richiede le credenziali dell'account utente (parametri KLLOGIN e KLPASSWD). Utilizzare il carattere ; per specificare più valori. Valori disponibili: • SET – modifica delle impostazioni dell'applicazione. • EXIT – chiusura dell'applicazione. • DISPROTECT – disabilitazione dei componenti della protezione e arresto delle attività di scansione. • DISPOLICY – disabilitazione del criterio di Kaspersky Security Center. • UNINST – rimozione dell'applicazione dal computer. • DISCTRL – disabilitazione dei componenti di controllo. • REMOVELIC – rimozione della chiave. • REPORTS – visualizzazione dei rapporti. • EXPORT – esportazione delle impostazioni dell'applicazione. Ad esempio, KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. L'account KLAdmin ha il diritto di eseguire qualsiasi azione protetta da password. Pertanto, non è possibile configurare l'ambito della password per l'account KLAdmin. Se si tenta di configurare l'ambito delle password per l'account KLAdmin, l'applicazione vieta le azioni specificate per il gruppo "Tutti".
PROTECTOSSERVICES	Protezione della funzionalità dei servizi del sistema operativo. La protezione dei servizi del sistema operativo impedisce alle applicazioni di terze parti di interferire con il funzionamento dei servizi del sistema operativo. Tali servizi includono, ad esempio, il servizio di avvio automatico delle applicazioni. • 1 significa che la protezione dei servizi del sistema operativo è abilitata (valore predefinito). • 0 significa che la protezione dei servizi del sistema operativo è disabilitata.
ENABLETRACES	Abilitazione o disabilitazione del tracciamento dell'applicazione. Dopo l'avvio, Kaspersky Endpoint Security salva i file di traccia nella cartella %ProgramData%\Kaspersky Lab\KES.14.2\Traces. Valori disponibili: • 1 - il tracciamento è abilitato. • 0 - il tracciamento è disabilitato (valore predefinito).

TRACESLEVEL	Livello di dettaglio delle tracce. Valori disponibili: • 100 (critico). Solo messaggi sugli errori irreversibili. • 200 (alto). Messaggi su tutti gli errori, inclusi gli errori irreversibili. • 300 (diagnostico). Messaggi su tutti gli errori e avvisi. • 400 (importante). Tutti i messaggi di errore, gli avvisi e le informazioni aggiuntive. • 500 (normale). Messaggi su tutti gli errori e avvisi, nonché informazioni dettagliate sul funzionamento dell'applicazione in modalità normale (impostazione predefinita). • 600 (basso). Tutti i messaggi.
ENABLEAZURESUPPORT	Abilitazione o disabilitazione della modalità di compatibilità di Azure WVD. Valori disponibili: • 1: la modalità di compatibilità di Azure WVD è abilitata. • 0: la modalità di compatibilità di Azure WVD è disabilitata (valore predefinito). Questa funzionalità garantisce la corretta visualizzazione dello stato della macchina virtuale di Azure nella console Kaspersky Anti Targeted Attack Platform. Per monitorare le prestazioni del computer, Kaspersky Endpoint Security invia dati di telemetria ai server KATA. La telemetria include un ID del computer (Sensor ID). La modalità di compatibilità Azure WVD consente di assegnare un Sensor ID univoco permanente a queste macchine virtuali. Se la modalità di compatibilità è disattivata, l'Sensor ID può cambiare dopo il riavvio del computer a causa del funzionamento delle macchine virtuali di Azure. Ciò può causare la visualizzazione di duplicati di macchine virtuali sulla console.
AMPPL	Consente di abilitare o disabilitare la protezione dei processi Kaspersky Endpoint Security tramite la tecnologia AM-PPL (Antimalware Protected Process Light). Per ulteriori informazioni sulla tecnologia AM-PPL, visitare il sito Web Microsoft. La tecnologia AM-PPL è disponibile per i sistemi operativi Windows 10 versione 1703 (RS2) o successiva e Windows Server 2019. Valori disponibili: • 1 – la protezione dei processi Kaspersky Endpoint Security tramite la tecnologia AM-PPL è abilitata. • 0 – la protezione dei processi Kaspersky Endpoint Security tramite la tecnologia AM-PPL è disabilitata.
UPGRADEMODE	Modalità di upgrade dell'applicazione: • Seamless indica l'upgrade dell'applicazione con un riavvio del computer (valore predefinito). • Force indica l'upgrade dell'applicazione senza un riavvio. È possibile eseguire l'upgrade dell'applicazione senza riavvio a partire dalla versione 11.10.0. Per eseguire l'upgrade a una versione precedente dell'applicazione, è necessario riavviare il computer. È inoltre possibile installare le patch senza riavvio a partire dalla versione 11.11.0. Il riavvio non è richiesto durante l'installazione di Kaspersky Endpoint Security. Pertanto, la modalità di upgrade dell'applicazione verrà specificata nelle impostazioni dell'applicazione. È possibile modificare questo parametro nel criterio o nelle impostazioni dell'applicazione. Quando si effettua l'upgrade di un'applicazione già installata, la priorità del parametro della riga di comando è inferiore a quella del parametro specificato nelle impostazioni dell'applicazione o nel file setup.ini. Ad esempio, se è specificata la modalità di upgrade Force nella riga di comando e la modalità Seamless è specificata nelle impostazioni dell'applicazione, l'upgrade verrà installato con un riavvio del computer (Seamless).
RESTAPI	Gestione dell'applicazione tramite REST API. Per gestire l'applicazione tramite REST API, è necessario specificare il nome utente (parametro RESTAPI_User). Valori disponibili: • 1 - la gestione tramite REST API è consentita. • 0 – la gestione tramite l'API REST è bloccata (valore predefinito). Per gestire l'applicazione tramite REST API, è necessario consentire la gestione utilizzando sistemi amministrativi. A tale scopo, impostare il parametro AdminKitConnector=1. Se si gestisce l'applicazione tramite REST API, è impossibile gestire l'applicazione utilizzando i sistemi di amministrazione di Kaspersky.
RESTAPI_User	Nome utente dell'account di dominio Windows utilizzato per la gestione dell'applicazione tramite REST API. La gestione dell'applicazione tramite REST API è disponibile solo per questo utente. Immettere il nome utente nel formato <DOMAIN>\<UserName> (ad esempio RESTAPI_User=COMPANY\Administrator). È possibile selezionare un solo utente per l'utilizzo dell'API REST. L'aggiunta di un nome utente è un prerequisito per la gestione dell'applicazione tramite REST API.
RESTAPI_Port	Porta utilizzata per la gestione dell'applicazione tramite REST API. La porta 6782 è utilizzata per impostazione predefinita. Assicurarsi che la porta sia libera.
RESTAPI_Certificate	Certificato per l'identificazione delle richieste (ad esempio, RESTAPI_Certificate=C:\cert.pem). L'interazione sicura di Kaspersky Endpoint Security con il client REST richiede la configurazione dell'identificazione delle richieste. A tale scopo, è necessario installare un certificato e successivamente firmare il payload di ogni richiesta.
ADMINKITCONNECTOR	Gestione dell'applicazione tramite sistemi di amministrazione. I sistemi di amministrazione includono ad esempio Kaspersky Security Center. Oltre ai sistemi di amministrazione di Kaspersky, è possibile utilizzare soluzioni di terzi. A tale scopo, Kaspersky Endpoint Security fornisce un'API. Valori disponibili: • 1 - la gestione dell'applicazione con l'ausilio di sistemi di amministrazione è consentita (valore predefinito). • 0 - la gestione dell'applicazione è consentita solo tramite l'interfaccia locale.

`EnableUniqueSensorID`	Creazione di un identificativo univoco del computer (Sensor ID) durante l'installazione o l'aggiornamento dell'applicazione. Sensor ID viene utilizzato nella soluzione Kaspersky Anti Targeted Attack Platform per identificare i computer che inviano la telemetria al server. Durante la creazione di Sensor ID, l'applicazione utilizza un algoritmo che tiene conto della configurazione del computer, ad esempio il numero di serie della scheda madre. In alcuni casi, ad esempio quando si utilizza l'applicazione in un ambiente virtuale, Sensor ID potrebbe essere duplicato. Di conseguenza, Kaspersky Anti Targeted Attack Platform non è in grado di identificare il computer da cui viene inviata la telemetria. Per creare un Sensor ID univoco, è necessario impostare il parametro `EnableUniqueSensorID=1`. In seguito a questa operazione, l'applicazione utilizzerà un algoritmo diverso per creare Sensor ID, che tiene conto degli altri dati relativi al computer. Questo garantisce un Sensor ID univoco. Per impostazione predefinita, il parametro non è impostato. L'applicazione eredita Sensor ID nei seguenti casi: • aggiornamento della versione dell'applicazione; • migrazione della configurazione [KES+KEA] alla configurazione [KES+agente integrato]. Nell'ambito della riparazione dell'applicazione, il programma di installazione tenta di ereditare l'Sensor ID. Se l'Sensor ID non può essere ripristinato, l'applicazione crea un nuovo Sensor ID.
`SKIPKB5007186CHECK=1`	Disattivazione del controllo dell'aggiornamento del sistema operativo installato KB5007186. Prima di installare l'applicazione, il programma di installazione controlla gli aggiornamenti dei sistemi operativi installati. L'aggiornamento KB5007186 è nell'elenco degli aggiornamenti del sistema operativo che possono causare problemi all'applicazione. Per informazioni dettagliate, consultare la Knowledge Base dell'Assistenza tecnica. Se questo aggiornamento viene individuato, il programma di installazione interrompe pertanto l'installazione. Per procedere con l'installazione, impostare `SKIPKB5007186CHECK=1`.

Esempio

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Dopo l'installazione di Kaspersky Endpoint Security, la licenza di prova viene attivata a meno che non sia stato fornito un codice di attivazione nel file setup.ini. Una licenza di prova in genere è utilizzabile per un periodo di tempo limitato. Dopo la scadenza della licenza di prova, tutte le funzionalità di Kaspersky Endpoint Security vengono disabilitate. Per continuare a utilizzare l'applicazione, è necessario attivare l'applicazione con una licenza commerciale utilizzando l'Attivazione guidata dell'applicazione o un comando speciale.

Durante l'installazione dell'applicazione o l'upgrade della versione dell'applicazione in modalità automatica, è supportato l'utilizzo dei seguenti file:

- setup.ini – impostazioni generali dell'installazione dell'applicazione.

  Per applicare le impostazioni del file setup.ini, inserire il file nella cartella contenente il pacchetto di distribuzione di Kaspersky Endpoint Security.

- install.cfg – impostazioni dell'esecuzione di Kaspersky Endpoint Security

  Per applicare le impostazioni dal file di configurazione install.cfg, è necessario specificare il percorso del file nel seguente comando di installazione dell'applicazione: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – chiavi di registro.

  Le chiavi del Registro di sistema del file setup.reg vengono scritte nel Registro di sistema solo se il valore `setup.reg` è impostato per il parametro `SetupReg` nel file setup.ini. Il file setup.reg viene generato dagli esperti di Kaspersky. Non è consigliabile modificare i contenuti del file. Per applicare le impostazioni del file setup.reg, inserire il file nella cartella contenente il pacchetto di distribuzione di Kaspersky Endpoint Security. È inoltre possibile inserire il file setup.reg in una cartella diversa. In tal caso, è necessario specificare il percorso del file nel seguente comando di installazione dell'applicazione: `SETUPREG=<path to the setup.reg file>`

Setup /x. Rimozione dell'applicazione

Kaspersky Endpoint Security può essere disinstallato dalla riga di comando in uno dei seguenti modi:

- In modalità interattiva, utilizzando l'Installazione guidata dell'applicazione.
- In modalità automatica. Una volta avviata la disinstallazione in modalità automatica, l'intervento dell'utente nel processo di rimozione non è necessario (installazione automatica). Per disinstallare l'applicazione in modalità automatica, utilizzare gli interruttori `/s` e `/qn`.

Per disinstallare l'applicazione in modalità automatica:

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il pacchetto di distribuzione di Kaspersky Endpoint Security.
3. Eseguire il seguente comando:
   - Se il processo di rimozione non è protetto da password:

     ```
     setup_kes.exe /s /x
     ```

     oppure

     ```
     msiexec.exe /x <GUID> /qn
     ```

     Per `<GUID>` si intende l'ID univoco dell'applicazione. È possibile trovare il GUID dell'applicazione nella Knowledge Base dell'Assistenza tecnica oppure utilizzando il seguente comando:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Se il processo di rimozione è protetto da password:

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     oppure

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

È inoltre possibile utilizzare il parametro `SAVEQB` per salvare i file scansionati dall'applicazione e inseriti nel backup. Le copie di backup dei file vengono archiviate nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`. Per impostazione predefinita, il salvataggio dei file in Backup è disabilitato (`SAVEQB=0`).

Esempio

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Recupero dell'applicazione

Durante il ripristino, l'applicazione controlla e ripristina l'integrità di tutti i moduli dell'applicazione e delle chiavi del Registro di sistema danneggiati creati durante il processo di installazione dell'applicazione.

Kaspersky Endpoint Security può essere ripristinato dalla riga di comando in uno dei seguenti modi:

- In modalità interattiva, utilizzando l'Installazione guidata dell'applicazione.
- In modalità automatica. Una volta avviato il ripristino in modalità automatica, l'intervento dell'utente nel processo di installazione non è necessario.

Se il programma di installazione di Kaspersky Endpoint Security è in esecuzione in modalità di ripristino e l'applicazione non richiede un ripristino, il programma di installazione non apporta modifiche.

Se il programma di installazione Kaspersky Endpoint Security è in esecuzione in modalità di ripristino e l'applicazione non è installata, viene avviato il processo di installazione.

Per ripristinare l'applicazione in modalità automatica:

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il pacchetto di distribuzione di Kaspersky Endpoint Security.
3. Eseguire il seguente comando:
   - Se il processo di ripristino non è protetto da password:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     Per `<GUID>` si intende l'ID univoco dell'applicazione. È possibile trovare il GUID dell'applicazione nella Knowledge Base dell'Assistenza tecnica oppure utilizzando il seguente comando:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Se il processo di ripristino è protetto da password:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Esempio

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

Comandi AVP

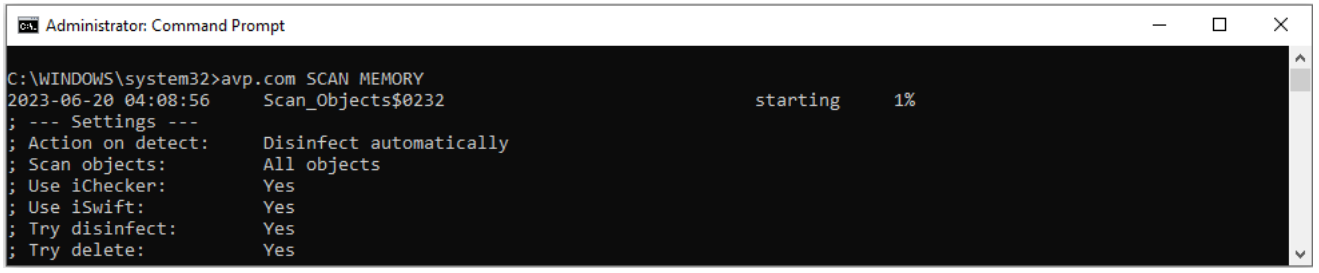
Per gestire Kaspersky Endpoint Security dalla riga di comando:

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

   È possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% durante l'installazione dell'applicazione.
3. Utilizzare il seguente modello per eseguire il comando:

   ```
   avp.com <command> [options]
   ```

In seguito a questa operazione, Kaspersky Endpoint Security eseguirà il comando (vedere la figura seguente).



Gestione dell'applicazione dalla riga di comando

SCAN. Scansione malware

Esecuzione dell'attività *Scansione malware*.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

Ambito della scansione	
`<files to scan>`	Un elenco di file e cartelle separato da spazi. I percorsi lunghi devono essere racchiusi tra virgolette. I percorsi brevi (formato MS-DOS) non devono essere racchiusi tra virgolette. Ad esempio: • `"C:\Program Files (x86)\Example Folder"` – percorso lungo. • `C:\PROGRA~2\EXAMPL~1` – percorso breve.

`/ALL`	Eseguire l'attività *Scansione malware*. Kaspersky Endpoint Security esamina i seguenti oggetti: • Memoria del kernel • Oggetti caricati all'avvio del sistema operativo • Settori di avvio • Backup del sistema operativo • Tutti i dischi rigidi e le unità rimovibili In Kaspersky Endpoint Security for Windows 12.12, l'e-mail è esclusa dall'ambito della scansione dell'applicazione. La scansione dei messaggi e-mail in entrata e in uscita viene eseguita dal componente Protezione minacce di posta. Se si utilizza una versione precedente del plug-in di gestione, l'applicazione esclude la posta elettronica dall'ambito di scansione, anche se il criterio la include.
`/MEMORY`	Esaminare la memoria del kernel
`/STARTUP`	Esaminare gli oggetti caricati all'avvio del sistema operativo
`/REMDRIVES`	Esaminare le unità rimovibili.
`/FIXDRIVES`	Esaminare i dischi rigidi.
`/NETDRIVES`	Esaminare le unità di rete.
`/QUARANTINE`	Esaminare i file nel backup di Kaspersky Endpoint Security.
`/@:<file list.lst>`	Esaminare i file e le cartelle da un elenco. Ciascun file nell'elenco deve essere in una nuova riga. I percorsi lunghi devono essere racchiusi tra virgolette. I percorsi brevi (formato MS-DOS) non devono essere racchiusi tra virgolette. Ad esempio: • `"C:\Program Files (x86)\Example Folder"` – percorso lungo. • `C:\PROGRA~2\EXAMPL~1` – percorso breve.

Azione se viene rilevata una minaccia	
`/i0`	**Informa**. Se questa opzione è selezionata, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti all'elenco delle minacce attive in caso di rilevamento di tali file.
`/i1`	**Disinfetta (se la disinfezione non riesce, informa)**. Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive.
`/i2`	**Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato. Questa azione è selezionata per impostazione predefinita.
`/i3`	**Se la disinfezione non riesce, elimina**. Elimina anche i file composti (ad esempio gli archivi) se il file infetto non può essere disinfettato o eliminato.
`/i4`	**Elimina**. Elimina anche i file composti (ad esempio gli archivi) se il file infetto non può essere eliminato.

Tipi di file	
`/fe`	**File esaminati per estensione**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Il formato del file viene quindi determinato in base all'estensione.
`/fi`	**File esaminati per formato**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Prima di esaminare un file alla ricerca di codice dannoso, viene analizzata l'intestazione interna del file per determinarne il formato (ad esempio, .txt, .doc o .exe). La scansione cerca inoltre i file con estensioni file particolari.
`/fa`	**Tutti i file**. Se questa impostazione è abilitata, l'applicazione esamina tutti i file senza eccezioni (tutti i formati e le estensioni). Rappresenta l'impostazione predefinita.

Esclusioni dalla scansione	
`-e:a`	Gli archivi RAR, ARJ, ZIP, CAB, LHA, JAR e ICE sono esclusi dall'ambito della scansione.
`-e:<file mask>`	I file che corrispondono alla maschera file sono esclusi dall'ambito della scansione. Ad esempio: • La maschera `*.exe` includerà tutti i percorsi dei file con estensione exe. • La maschera `example*` includerà tutti i percorsi dei file denominati EXAMPLE.
`-e:<seconds>`	I file la cui scansione richiede più tempo rispetto al limite specificato (in secondi) sono esclusi dall'ambito della scansione.
`-es:<megabytes>`	I file di dimensioni superiori al limite specificato (in megabyte) sono esclusi dall'ambito della scansione.

Salvataggio degli eventi in una modalità file di rapporto (solo per i profili di Scansione, Updater e Rollback)	
`/R:<report file>`	Salva solo gli eventi critici nel file di rapporto.
`/RA:<report file>`	Salva tutti gli eventi in un file di rapporto.

Tecnologie di scansione	
`/iChecker=on|off`	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
`/iSwift=on|off`	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.

Impostazioni avanzate	
`/C:<file with scan settings>`	File con le impostazioni dell'attività *Scansione malware*. Il file deve essere creato manualmente e salvato in formato TXT. Il file può avere i seguenti contenuti: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Esempio

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Aggiornamento di database e moduli software dell'applicazione

Esecuzione dell'attività *Aggiornamento di database e moduli dell'applicazione*.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Questo comando non può essere eseguito se l'applicazione è installata in modalità Light Agent.

Sintassi del comando

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Impostazioni attività di aggiornamento	
`local`	Avvio dell'attività *Aggiornamento di database e moduli dell'applicazione* creata automaticamente dopo l'installazione dell'applicazione. È possibile modificare le impostazioni dell'attività *Aggiornamento di database e moduli dell'applicazione* nell'interfaccia locale dell'applicazione o nella console di Kaspersky Security Center. Se questa impostazione non è configurata, Kaspersky Endpoint Security avvia l'attività *Aggiornamento di database e moduli dell'applicazione* con le impostazioni predefinite o con le impostazioni specificate nel comando. È possibile configurare le impostazioni dell'attività *Aggiornamento di database e moduli dell'applicazione* come segue: • `UPDATE` avvia l'attività *Aggiornamento di database e moduli dell'applicazione* con le impostazioni predefinite: la sorgente degli aggiornamenti è rappresentata dai server degli aggiornamenti Kaspersky, l'account è System e altre impostazioni predefinite. • `UPDATE local` avvia l'attività *Aggiornamento di database e moduli dell'applicazione* creata automaticamente dopo l'installazione (attività predefinita). • `UPDATE <update settings>` avvia l'attività *Aggiornamento di database e moduli dell'applicazione* con impostazioni definite manualmente (vedere di seguito).

Sorgente degli aggiornamenti	
`"<update source>"`	Indirizzo di un server HTTP o FTP o di una cartella condivisa con il pacchetto degli aggiornamenti. È possibile specificare solo una sorgente aggiornamenti. Se la sorgente degli aggiornamenti non è specificata, Kaspersky Endpoint Security utilizza la sorgente predefinita: server degli aggiornamenti di Kaspersky.

Salvataggio degli eventi in una modalità file di rapporto (solo per i profili di Scansione, Updater e Rollback)	
`/R:<report file>`	Salva solo gli eventi critici nel file di rapporto.
`/RA:<report file>`	Salva tutti gli eventi in un file di rapporto.

Impostazioni avanzate	
`/C:<file with update settings>`	File con le impostazioni dell'attività *Aggiornamento di database e moduli dell'applicazione*. Il file deve essere creato manualmente e salvato in formato TXT. Il file può avere i seguenti contenuti: `["<update source>"] [/R[A]:<report file>]`.

Esempio

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Ultimo rollback degli aggiornamenti

Rollback dell'ultimo aggiornamento del database anti-virus. Questo consente di eseguire il rollback dei database e dei moduli dell'applicazione alla versione precedente, se necessario, ad esempio quando la nuova versione dei database contiene una firma non valida che determina il blocco di un'applicazione sicura da parte di Kaspersky Endpoint Security.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Questo comando non può essere eseguito se l'applicazione è installata in modalità Light Agent.

Sintassi del comando

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Salvataggio degli eventi in una modalità file di rapporto (solo per i profili di Scansione, Updater e Rollback)	
`/R:<report file>`	Salva solo gli eventi critici nel file di rapporto.
`/RA:<report file>`	Salva tutti gli eventi in un file di rapporto.

Esempio

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Tracciamento

I file di traccia rimangono memorizzati nel computer finché l'applicazione è in uso e vengono eliminati definitivamente quando l'applicazione viene rimossa. I file di traccia, tranne i file di traccia dell'Agente di Autenticazione, vengono archiviati nella cartella `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. Per impostazione predefinita il tracciamento è disabilitato.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Livello di traccia	
`<tracing level>`	Livello di dettaglio delle tracce. Valori disponibili: • `100` (critico). Solo messaggi sugli errori irreversibili. • `200` (alto). Messaggi su tutti gli errori, inclusi gli errori irreversibili. • `300` (diagnostico). Messaggi su tutti gli errori e avvisi. • `400` (importante). Tutti i messaggi di errore, gli avvisi e le informazioni aggiuntive. • `500` (normale). Messaggi su tutti gli errori e avvisi, nonché informazioni dettagliate sul funzionamento dell'applicazione in modalità normale (impostazione predefinita). • `600` (basso). Tutti i messaggi.

Impostazioni avanzate	
`all`	Eseguire un comando con i parametri `file` e `mem` parameters.
`file`	Salva un file di traccia (nessun limite di dimensioni).
`rot`	Salva le tracce in un numero limitato di set di file di dimensioni limitate e sovrascrivi i file meno recenti quando viene raggiunta la dimensione massima.
`mem`	Salva le tracce nei file di dump.

Esempio

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Avvio di un profilo

Avvio di un profilo (ad esempio, avvio di un aggiornamento dei database o abilitazione di un componente di protezione).

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com START <profile> [/R[A]:<report file>]
```

Profilo	
`<profile>`	Nome del profilo. Un *Profilo* è un componente, un'attività o una funzionalità di Kaspersky Endpoint Security. È possibile visualizzare l'elenco dei profili disponibili eseguendo il comando `HELP START`.

Salvataggio degli eventi in una modalità file di rapporto (solo per i profili di Scansione, Updater e Rollback)	
`/R:<report file>`	Salva solo gli eventi critici nel file di rapporto.
`/RA:<report file>`	Salva tutti gli eventi in un file di rapporto.

Esempio

```
avp.com START Scan_Objects
```

STOP. Arresto di un profilo

Arresto dell'esecuzione del profilo (ad esempio, arresto di una scansione delle unità rimovibili o disabilitazione di un componente della protezione).

Per eseguire questo comando, Protezione tramite password deve essere abilitato. L'utente deve disporre delle autorizzazioni **Disabilita componenti della protezione** e **Disabilita componenti di controllo**.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Profilo	
`<profile>`	Nome del profilo. Un *Profilo* è un componente, un'attività o una funzionalità di Kaspersky Endpoint Security. È possibile visualizzare l'elenco dei profili disponibili eseguendo il comando `HELP STOP`.

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

STATUS. Stato del profilo

Visualizzazione delle informazioni sullo stato per i profili delle applicazioni (ad esempio, `running` o `completed`). È possibile visualizzare l'elenco dei profili disponibili eseguendo il comando `HELP STATUS`.

Kaspersky Endpoint Security visualizza anche informazioni sullo stato dei profili di servizio. È possibile che vengano richieste informazioni sullo stato dei profili di servizio quando si contatta l'Assistenza tecnica di Kaspersky.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com STATUS [<profile>]
```

Se si immette il comando senza un profilo, Kaspersky Endpoint Security mostra lo stato di tutti i profili dell'applicazione.

STATISTICS. Statistiche sul funzionamento del profilo

Visualizzazione delle statistiche per un profilo dell'applicazione (ad esempio la durata della scansione o il numero di minacce rilevate). È possibile visualizzare l'elenco dei profili disponibili eseguendo il comando `HELP STATISTICS`.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com STATISTICS <profile>
```

RESTORE. Ripristino di file da Backup

Ripristino di un file dal Backup nella cartella originale. Se esiste già un file con lo stesso nome nel percorso specificato, l'applicazione richiederà di confermare la sostituzione del file. Il file che viene ripristinato viene copiato mantenendo il nome originale.

Per eseguire questo comando, Protezione tramite password deve essere abilitato. L'utente deve avere l'autorizzazione **Ripristina da Backup**.

Backup archivia le copie di backup dei file eliminati o modificati durante la disinfezione. Una *copia di backup* è una copia del file creata prima della disinfezione o dell'eliminazione del file. Le copie di backup dei file vengono archiviate in un formato speciale e non rappresentano una minaccia.

Le copie di backup dei file vengono archiviate nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Agli utenti del gruppo Amministratori è concessa l'autorizzazione completa per l'accesso a questa cartella. All'utente il cui account è stato utilizzato per installare Kaspersky Endpoint Security vengono concessi diritti di accesso limitati alla cartella.

Kaspersky Endpoint Security non consente la possibilità di configurare le autorizzazioni per l'accesso dell'utente alle copie di backup dei file.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Impostazioni avanzate	
`/REPLACE`	Sovrascrivi un file esistente.
`<file name>`	Il nome del file da ripristinare.

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Esportazione delle impostazioni dell'applicazione

Esportazione delle impostazioni di Kaspersky Endpoint Security in un file. Se il comando contiene solo il nome del file in cui si desidera esportare le impostazioni, l'applicazione posiziona il file come segue:

- Se il percorso di avp.com viene aggiunto alla variabile di sistema %PATH%, l'applicazione inserisce il file nella cartella `C:\Windows\SysWOW64`.
- Se si esegue il comando dalla cartella di installazione dell'applicazione, l'esportazione avrà esito negativo poiché l'autoprotezione dell'applicazione blocca la creazione di un nuovo file nella cartella dell'applicazione. Per esportare le impostazioni dell'applicazione in un file, immettere il percorso del file.

Per eseguire questo comando, Protezione tramite password deve essere abilitato. L'utente deve avere l'autorizzazione **Esporta impostazioni**.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Profilo	
`<profile>`	Nome del profilo. Un *Profilo* è un componente, un'attività o una funzionalità di Kaspersky Endpoint Security. È possibile visualizzare l'elenco dei profili disponibili eseguendo il comando `HELP EXPORT`.

File da esportare	
`<file name>`	Il nome del file nel quale verranno esportate le impostazioni dell'applicazione. È inoltre possibile immettere il percorso del file. È possibile esportare le impostazioni di Kaspersky Endpoint Security in un file di configurazione DAT o CFG, in un file di testo TXT o in un documento XML.

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Importazione delle impostazioni dell'applicazione

Importazione delle impostazioni di Kaspersky Endpoint Security da un file creato con il comando `EXPORT`.

Per eseguire questo comando, Protezione tramite password deve essere abilitato. L'utente deve avere l'autorizzazione **Configura le impostazioni dell'applicazione**.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

File da importare	
`<file name>`	Il nome del file dal quale verranno importate le impostazioni dell'applicazione. È possibile importare le impostazioni di Kaspersky Endpoint Security da un file di configurazione DAT o CFG, da un file di testo TXT o da un documento XML.

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Applicazione di un file chiave

Attivazione di Kaspersky Endpoint Security tramite un file chiave. Se l'applicazione è già attivata, la chiave verrà aggiunta come chiave di riserva.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Questo comando non può essere eseguito se l'applicazione è installata in modalità Light Agent.

Sintassi del comando

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

File chiave	
`<file name>`	Nome file chiave.

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente. Queste credenziali devono essere immesse solo se Protezione tramite password è abilitato.

Esempio

```
avp.com ADDKEY file.key
```

LICENSE. Gestione delle licenze

Gestione delle chiavi di licenza di Kaspersky Endpoint Security, EDR Optimum o EDR Expert (componente aggiuntivo Kaspersky Endpoint Detection and Response).

Per eseguire questo comando e rimuovere una chiave di licenza, Protezione tramite password deve essere abilitato. L'utente deve avere l'autorizzazione **Rimuovi chiave**.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Questo comando non può essere eseguito se l'applicazione è installata in modalità Light Agent.

Sintassi del comando

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Operazione	
`/ADD <file name>`	Attivazione di Kaspersky Endpoint Security tramite un file chiave. Se l'applicazione è già attivata, la chiave verrà aggiunta come chiave di riserva.
`/ADD <activation code>`	Attiva Kaspersky Endpoint Security tramite un codice di attivazione. Se l'applicazione è già attivata, la chiave verrà aggiunta come chiave di riserva.
`/REFRESH`	Aggiorna lo stato della licenza di Kaspersky Endpoint Security. Di conseguenza, l'applicazione riceve informazioni aggiornate sullo stato della licenza dai server di attivazione di Kaspersky.

`/REFRESH <license ID>`	Aggiornare lo stato delle licenze utilizzando l'ID della licenza. Utilizzando questo comando è possibile aggiornare lo stato del componente aggiuntivo EDR, del componente aggiuntivo MDR, del componente aggiuntivo KUMA o di altre licenze. È possibile ottenere l'ID della licenza dal certificato di licenza. Di conseguenza, l'applicazione riceve informazioni aggiornate sullo stato della licenza dai server di attivazione di Kaspersky.
`/CHECK`	Recupero delle informazioni sulla licenza Kaspersky Endpoint Security mostra le informazioni su tutte le chiavi di licenza aggiunte, incluse chiavi di riserva, EDR Add-on, MDR Add-on, chiavi di KUMA Add-on e altre chiavi. Kaspersky Endpoint Security mostra le seguenti informazioni sulla licenza: • nome della licenza; • identificativo della licenza; • indirizzo del server di protezione (SVM) a cui è connessa la macchina virtuale in cui è installata l'applicazione in modalità Light Agent; • tipo di licenza: prova, commerciale, beta, abbonamento; • data e ora di attivazione dell'applicazione; • data e ora di scadenza della licenza; • numero di giorni fino alla scadenza della licenza.
`/CHECK <license ID>`	Recuperare le informazioni sulla licenza in base all'ID. È possibile utilizzare questo comando per ottenere informazioni sulla licenza. È possibile ottenere l'ID della licenza dal certificato di licenza.
`/DEL /login=<user name> /password= <password>`	Rimuove la chiave di licenza dell'applicazione. Verrà rimossa anche la chiave di riserva.
`/DEL <license ID> /login=<user name> /password=<password>`	Eliminare la chiave utilizzando l'ID della licenza. Utilizzando questo comando è possibile eliminare una chiave da componente aggiuntivo EDR, componente aggiuntivo MDR, componente aggiuntivo KUMA o altre licenze. È possibile ottenere l'ID della licenza dal certificato di licenza.

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Esempio

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Acquisto di una licenza

Apertura del sito Web Kaspersky per acquistare o rinnovare la licenza.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Questo comando non può essere eseguito se l'applicazione è installata in modalità Light Agent.

PBATESTRESET. Ripristino dei risultati del controllo del disco prima di criptare il disco

Ripristino dei risultati del controllo di compatibilità per Criptaggio dell'intero disco (FDE), comprese le tecnologie Criptaggio disco Kaspersky e Criptaggio unità BitLocker.

Prima di eseguire Criptaggio dell'intero disco, l'applicazione esegue una serie di controlli per verificare che il computer possa essere criptato. Se il computer non supporta Criptaggio dell'intero disco, Kaspersky Endpoint Security registra le informazioni sull'incompatibilità. Al successivo tentativo di criptaggio, l'applicazione non esegue questo controllo e avvisa che non è possibile eseguire il criptaggio. Se la configurazione hardware del computer è cambiata, i risultati del controllo compatibilità precedentemente registrati dall'applicazione devono essere ripristinati per ricontrollare la compatibilità del disco rigido di sistema con le tecnologie Criptaggio disco Kaspersky o Crittografia unità BitLocker.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

EXIT. Chiusura dell'applicazione

Chiusura di Kaspersky Endpoint Security. L'applicazione verrà scaricata dalla RAM del computer.

Per eseguire questo comando, Protezione tramite password deve essere abilitato. L'utente deve avere l'autorizzazione **Chiudi l'applicazione**.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Disabilitazione del criterio

Disabilitazione di un criterio di Kaspersky Security Center nel computer. Tutte le impostazioni di Kaspersky Endpoint Security sono disponibili per la configurazione, incluse le impostazioni con un lucchetto chiuso nel criterio ( ).

Per eseguire questo comando, Protezione tramite password deve essere abilitato. L'utente deve avere l'autorizzazione **Disabilita il criterio di Kaspersky Security Center**.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Abilitazione del criterio

Abilitazione di un criterio di Kaspersky Security Center nel computer. Le impostazioni dell'applicazione verranno configurate in base al criterio.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

DISABLE. Disabilitazione della protezione

Disabilitazione di Protezione minacce file in un computer con una licenza Kaspersky Endpoint Security scaduta. Non è possibile eseguire questo comando in un computer dove l'applicazione non è attivata o senza una licenza valida.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

SPYWARE. Rilevamento spyware

Gestione del rilevamento dello spyware. Rilevamento spyware è abilitato per impostazione predefinita.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com SPYWARE on|off
```

KSN. Passaggio da KSN a KPSN e viceversa

Selezione di una soluzione Kaspersky per determinare la reputazione di file o siti Web. Kaspersky Endpoint Security supporta le seguenti soluzioni di infrastruttura per l'utilizzo dei database di reputazione di Kaspersky:

- *Kaspersky Security Network (KSN)* è la soluzione utilizzata dalla maggior parte delle applicazioni Kaspersky. I partecipanti KSN ricevono le informazioni da Kaspersky e inviano a Kaspersky le informazioni sugli oggetti rilevati nel computer dell'utente per un'analisi aggiuntiva da parte degli analisti di Kaspersky e per essere incluse nei database statistici e della reputazione.

- *Kaspersky Private Security Network (KPSN)* è una soluzione che consente agli utenti di computer che ospitano Kaspersky Endpoint Security o altre applicazioni Kaspersky di ottenere l'accesso ai database di reputazione di Kaspersky e ad altri dati statistici senza inviare dati a Kaspersky dai propri computer. KPSN è progettato per i clienti aziendali che non sono in grado di partecipare a Kaspersky Security Network per uno dei seguenti motivi:

  - Le workstation locali non sono connesse a Internet.

  - La trasmissione dei dati al di fuori del paese o al di fuori della LAN aziendale è vietato dalla legge o sottoposto a restrizioni in base ai criteri di protezione aziendali.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Questo comando non può essere eseguito se l'applicazione è installata in modalità Light Agent.

Sintassi del comando

```
avp.com KSN /global | /private <file name>
```

File di configurazione di Kaspersky Security Network	
`<file name>`	Nome del file di configurazione che contiene le impostazioni di Kaspersky Private Security Network. Questo file ha l'estensione PKCS7 o PEM.

Esempio

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Esempio

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Disabilitazione della protezione della connessione al server

Esecuzione dell'attività *Protezione della connessione ad Administration Server*, che rimuove la password della connessione del computer ad Administration Server. In questo modo, l'attività disabilita la protezione della connessione di Administration Server.

Per eseguire questo comando, Protezione tramite password deve essere abilitato.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Password	
`/password=<password>`	La password dell'account utente di KL Admin o la password dall'attività *Protezione della connessione ad Administration Server*. Se il parametro non è specificato, Kaspersky Endpoint Security richiede di immettere una password nella riga successiva.

Comandi KESCLI

I comandi KESCLI consentono di ricevere informazioni sullo stato di protezione del computer utilizzando il componente OPSWAT e consentono di eseguire attività standard come *Scansione malware* e *Aggiornamento di database e moduli dell'applicazione*.

È possibile visualizzare l'elenco dei comandi KESCLI utilizzando il comando `kescli --help` o il comando abbreviato `kescli -h`.

Per gestire Kaspersky Endpoint Security dalla riga di comando:

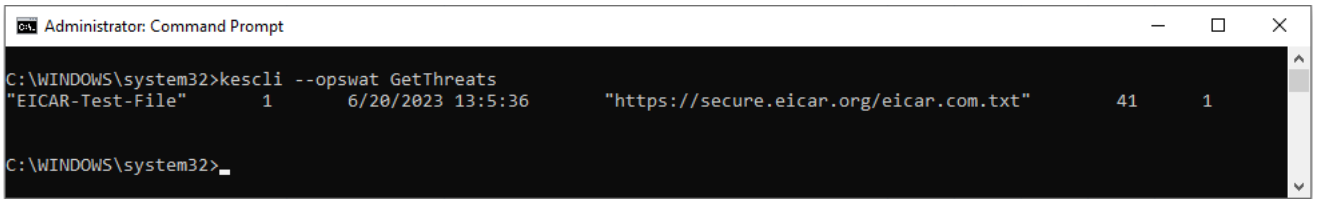
1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

   È possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% durante l'installazione dell'applicazione.

3. Utilizzare il seguente modello per eseguire il comando:

```
kescli <comando> [opzioni]
```

In seguito a questa operazione, Kaspersky Endpoint Security eseguirà il comando (vedere la figura seguente).



Gestione dell'applicazione dalla riga di comando

Scan. Scansione malware

Esecuzione dell'attività *Scansione malware* (Scansione completa).

Per eseguire l'attività, per l'amministratore deve essere selezionato Consenti utilizzo delle attività locali.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

Sintassi del comando

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

È possibile controllare lo stato di completamento dell'attività *Scansione malware* utilizzando il comando `GetScanState` e visualizzare la data e l'ora dell'ultimo completamento della scansione tramite il comando `GetLastScanTime`.

Ambito della scansione	
`<scan scope>`	Elenco di file e cartelle separato da `;`. Ad esempio, `"C:\Program Files (x86)\Example Folder"`.

Azione se viene rilevata una minaccia	
`0`	**Informa**. Se questa opzione è selezionata, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti all'elenco delle minacce attive in caso di rilevamento di tali file.
`1`	**Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato. Questa azione è selezionata per impostazione predefinita.

Esempio

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Stato di completamento della scansione

Visualizzazione delle informazioni sullo stato del completamento dell'attività *Scansione malware* (*Scansione completa*):

- `1` – la scansione è in corso.
- `0` – la scansione non è in esecuzione.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

Sintassi del comando

```
kescli --opswat GetScanState
```

GetLastScanTime. Definizione del tempo di completamento della scansione

Visualizzazione delle informazioni su data e ora dell'ultimo completamento dell'attività *Scansione malware* (*Scansione completa*).

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

Sintassi del comando

```
kescli --opswat GetLastScanTime
```

GetThreats. Ottenimento dei dati sulle minacce rilevate

Visualizzazione di un elenco delle minacce rilevate (*Rapporto sulle minacce*). Questo rapporto contiene informazioni sulle minacce e sull'attività dei virus negli ultimi 30 giorni precedenti alla creazione del rapporto.

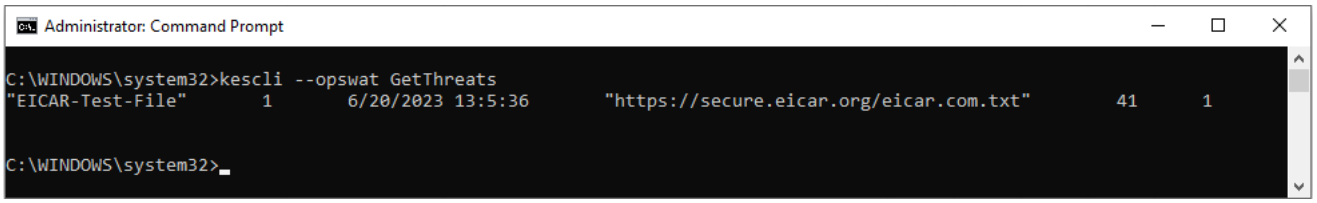
Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

Sintassi del comando

```
kescli --opswat GetThreats
```

Quando questo comando viene eseguito, Kaspersky Endpoint Security invierà una risposta nel seguente formato:

<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>



Gestione dell'applicazione dalla riga di comando

Tipo di oggetto	
0	Non noto (Unknown).
1	Virus (Virware).
2	Programmi trojan (Trojware).
3	Programmi dannosi (Malware).
4	Programmi pubblicitari (Adware).
5	Programmi di auto-dialer (Pornware).
6	Applicazioni utilizzabili da un criminale informatico per danneggiare il computer o i dati dell'utente (Riskware).
7	Oggetti compressi il cui metodo di compressione potrebbe essere utilizzato per proteggere codice dannoso (Packed).
20	Oggetti sconosciuti (Xfiles).
21	Applicazioni note (Software).
22	File nascosti (Hidden).
23	Applicazioni che richiedono attenzione (Pupware).
24	Comportamento anomalo (Anomaly).
30	Non determinato (Undetect).
40	Banner pubblicitari (Banner).
50	Attacco di rete (Attack).
51	Accesso al Registro di sistema (Registry).
52	Attività sospette (Suspicion).
60	Vulnerabilità (Vulnerability).
70	Phishing (Phishing).
80	Allegato di posta elettronica indesiderato (Attachment).
90	Malware rilevato da Kaspersky Security Network (Urgent).
100	Collegamento sconosciuto (Suspic URL).
110	Altro malware (Behavioral).

Azione se viene rilevata una minaccia	
0	Non noto (unknown).
1	La minaccia è stata risolta (ok).
2	L'oggetto è stato infettato e non è stato disinfettato (infected).
5	L'oggetto si trova in un archivio e non è stato disinfettato (archive).
9	L'oggetto è stato disinfettato (disinfected).
10	L'oggetto non è stato disinfettato (not disinfected).

11	L'oggetto è stato eliminato (`deleted`).
13	È stata creata una copia di backup dell'oggetto (`backupped`).
15	L'oggetto è stato spostato in Backup (`quarantined`).
23	L'oggetto è stato eliminato al riavvio del computer (`delete on reboot`).
25	L'oggetto è stato disinfettato al riavvio del computer (`disinfect on reboot`).
29	L'oggetto è stato spostato in Backup da un utente (`added by user`).
30	L'oggetto è stato aggiunto alle esclusioni (`added to exclude`).
31	L'oggetto è stato spostato in Backup al riavvio del computer (`quarantine on reboot`).
36	Falso positivo (`false alarm`).
38	Il processo è stato terminato (`terminated`).
40	L'oggetto non è stato rilevato (`not found`).
41	Impossibile risolvere la minaccia (`untreatable`).
42	L'oggetto è stato ripristinato (`rolled back`).
43	L'oggetto è stato creato a seguito dell'attività di una minaccia (`produced by threat`).
44	L'oggetto è stato ripristinato al riavvio del computer (`roll back on reboot`).
0xffffffff	L'oggetto non è stato elaborato (`discarded`).

Livello di pericolosità della minaccia	
`0`	Sconosciuto
`1`	Alto
`2`	Media
`4`	Basso
`8`	Info (inferiore a *Basso*)

UpdateDefinitions. Aggiornamento di database e moduli software dell'applicazione

Esecuzione dell'attività *Aggiornamento di database e moduli dell'applicazione*. Kaspersky Endpoint Security utilizza l'origine predefinita: i server degli aggiornamenti Kaspersky.

> Per eseguire l'attività, per l'amministratore deve essere selezionato Consenti utilizzo delle attività locali.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

> Questo comando non può essere eseguito se l'applicazione è installata in modalità Light Agent.

Sintassi del comando

```
kescli --opswat UpdateDefinitions
```

È possibile visualizzare la data e l'ora di rilascio dei database antivirus correnti utilizzando il comando `GetDefinitionsetState`.

GetDefinitionState. Determinazione della data e dell'ora dell'ultimo aggiornamento dei database

Visualizzazione delle informazioni sulla data e l'ora dell'ultimo aggiornamento dei database anti-virus in uso.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

Sintassi del comando

```
kescli --opswat GetDefinitionState
```

EnableRTP. Abilitazione della protezione

Abilitazione dei componenti della protezione di Kaspersky Endpoint Security nel computer: Protezione minacce file, Protezione minacce Web, Protezione minacce di posta, Protezione minacce di rete, Prevenzione Intrusioni Host.

Per abilitare i componenti della protezione, l'amministratore deve assicurarsi che le impostazioni dei criteri pertinenti possano essere modificate (gli attributi di sono aperti).

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

Sintassi del comando

```
kescli --opswat EnableRTP
```

Di conseguenza, i componenti della protezione vengono abilitati anche se è stata vietata la modifica delle impostazioni dell'applicazione con Protezione tramite password.

È possibile controllare lo stato operativo di Protezione minacce file utilizzando il comando `GetRealTimeProtectionState`.

GetRealTimeProtectionState. Stato di Protezione minacce file

Visualizzazione delle informazioni sullo stato del componente Protezione minacce file:

- `1` – il componente è abilitato.
- `0` – il componente è disabilitato.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

Sintassi del comando

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Stato di criptaggio del disco

Visualizzazione delle informazioni sullo stato del criptaggio del disco:

- `1` indica che il disco è protetto dalla tecnologia di criptaggio del disco Kaspersky o BitLocker.
- `0` indica che il disco non è criptato.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

Sintassi del comando

```
kescli --opswat GetEncryptionState
```

Version. Identificazione della versione dell'applicazione

Visualizzazione della versione di Kaspersky Endpoint Security for Windows.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

Sintassi del comando

```
kescli --Version
```

È inoltre possibile utilizzare il comando abbreviato `-v`.

Comandi di gestione di Detection and Response

È possibile utilizzare la riga di comando per gestire le funzionalità integrate delle soluzioni Detection and Response (ad esempio, Kaspersky Sandbox o Kaspersky Endpoint Detection and Response Optimum). È possibile gestire le soluzioni Detection and Response se la gestione tramite Kaspersky Security Center Console non è possibile. È possibile visualizzare l'elenco dei comandi per la gestione dell'applicazione eseguendo il comando `HELP`. Per leggere la sintassi di un comando specifico, immettere `HELP <command>`.

Per gestire le funzionalità integrate delle soluzioni Detection and Response con la riga di comando:

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.
3. Utilizzare il seguente modello per eseguire il comando:

   ```
   avp.com <command> [options]
   ```

   In seguito a questa operazione, Kaspersky Endpoint Security eseguirà il comando.

SANDBOX. Gestione di Sandbox

Comandi per la gestione del componente Sandbox:

- Abilitazione o disabilitazione del componente Sandbox.

  I componenti Sandbox consentono di interagire con la soluzione Kaspersky Sandbox e il componente KATA Sandbox, che fa parte di Kaspersky Anti Targeted Attack Platform.

- Configurazione del componente Kaspersky Sandbox:

  - Connessione del computer ai server di Sandbox.

    I server utilizzano immagini virtuali distribuite dei sistemi operativi Microsoft Windows per eseguire gli oggetti che devono essere sottoposti a scansione. È possibile immettere un indirizzo IP (IPv4 o IPv6) o un nome di dominio completo. Per i dettagli sulla distribuzione delle immagini virtuali e sulla configurazione dei server Sandbox, fare riferimento alla Guida di Kaspersky Sandbox e alla Guida di Kaspersky Anti Targeted Attack Platform.

  - Configurazione del timeout della connessione per il server.

    Timeout della connessione per il server Sandbox (per Kaspersky Sandbox) o il server di Central Node (per KATA). Allo scadere del timeout configurato, Kaspersky Endpoint Security invia una richiesta al server successivo. È possibile aumentare il timeout della connessione per il server se la velocità di connessione è lenta o se la connessione è instabile. Il timeout della richiesta consigliato è di 0,5 secondi o meno.

  - Configurazione di una connessione attendibile tra il computer e i server.

    Per configurare una connessione attendibile con il server Sandbox (per Kaspersky Sandbox) o il server di Central Node (per KATA), è necessario preparare un certificato TLS. È quindi necessario aggiungere il certificato nel computer utilizzando un criterio. È inoltre necessario aggiungere il certificato al server Sandbox (per Kaspersky Sandbox) o al server di Central Node (per KATA).

  - Configurazione della modalità di integrazione.

    È necessario selezionare una soluzione di cui fa parte Sandbox, ovvero Kaspersky Sandbox o KATA Sandbox. *Kaspersky Sandbox* è una soluzione Detection and Response indipendente di Kaspersky. *KATA Sandbox* è un componente della soluzione Kaspersky Anti Targeted Attack Platform. Se integrato con KATA Sandbox, il componente può funzionare nelle seguenti modalità:

    - **Manualmente**. L'utente invia manualmente il file per la scansione dal menu di scelta rapida (**Invia a Sandbox**).
    - **Automaticamente**. L'applicazione rileva automaticamente gli oggetti e li invia a Sandbox per la scansione.
    - **Combinato**.

- Visualizzazione delle impostazioni correnti del componente.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Operazione	
`stop`	Disabilitare il componente Sandbox.
`start`	Abilitare il componente Sandbox.
`set`	Configurare il componente Sandbox. Non è possibile configurare le seguenti impostazioni: • Aggiungere i server di Sandbox (`--servers`) • Aggiungere un certificato TLS (`--pinned-certificate`) • Aggiungere un contenitore crittografico (`--client-certificate`) • Specificare una password per il contenitore crittografico (`--client-certificate-password`); • Impostare la connessione al server (`--timeout`) • Selezionare una modalità di integrazione (`--mode`): • `KSB`: integrazione con Kaspersky Sandbox; • `KATAManual`: integrazione manuale con KATA Sandbox; • `KATAAuto`: integrazione automatica con KATA Sandbox; • `KATAFull`: integrazione combinata con KATA Sandbox.

`show`	Mostra le impostazioni correnti del componente. Si riceve la seguente risposta:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB /login=login /password=password
```

PREVENTION. Gestione della prevenzione dell'esecuzione

Disabilitazione del componente Prevenzione dell'esecuzione o visualizzazione delle impostazioni correnti del componente, incluso l'elenco delle regole di prevenzione dell'esecuzione.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com prevention disable
```

```
avp.com prevention /show
```

Dopo aver eseguito il comando `prevention /show`, si otterrà la seguente risposta:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

Valori restituiti dal comando:

- `-1` indica che il comando non è supportato dalla versione dell'applicazione installata nel computer.
- `0` indica che il comando è stato eseguito correttamente.
- `1` indica che un argomento obbligatorio non è stato passato al comando.
- `2` indica che si è verificato un errore generale.
- `4` indica la presenza di un errore di sintassi.
- `9`: operazione errata (ad esempio, tentativo di disabilitare il componente quando è già disabilitato).

ISOLATION. Gestione dell'isolamento di rete

Disabilitazione dell'isolamento di rete del computer o visualizzazione delle impostazioni correnti del componente. Le impostazioni dei componenti includono anche un elenco di connessioni di rete aggiunte alle esclusioni.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

Come risultato dell'esecuzione del comando `stat`, si riceverà la seguente risposta: `Network isolation on|off`.

RESTORE. Ripristino dei file dalla quarantena

Ripristino di un file dalla Quarantena nella cartella originale. *Quarantena* è una memoria locale speciale sul computer. L'utente può mettere in quarantena i file che considera pericolosi per il computer. I file in quarantena vengono archiviati in uno stato criptato e non minacciano la sicurezza del dispositivo. Kaspersky Endpoint Security utilizza la Quarantena solo quando è integrato con le soluzioni Kaspersky Detection and Response. In altri casi, Kaspersky Endpoint Security inserisce il file pertinente in Backup. Per ulteriori dettagli sulla gestione di Quarantena come parte delle soluzioni, consultare la Guida di Kaspersky Sandbox Help, la Guida di Kaspersky Endpoint Detection and Response Optimum, la Guida di Kaspersky Endpoint Detection and Response Expert, la Guida di Kaspersky Anti Targeted Attack Platform e la Guida di Kaspersky Endpoint Detection and Response Expert (on-premises).

Per eseguire questo comando, Protezione tramite password deve essere abilitato. L'utente deve avere l'autorizzazione **Ripristina da Backup**.

L'oggetto viene messo in quarantena con l'account di sistema (SYSTEM).

Il ripristino dei file dalla quarantena implica le seguenti considerazioni speciali:

- Se la cartella di destinazione è stata eliminata o l'utente non dispone dei diritti di accesso a tale cartella, l'applicazione inserisce il file nella cartella `%DataRoot%\QB\Restored`. Quindi, è necessario spostare manualmente il file nella cartella di destinazione.
- L'applicazione distingue tra maiuscole e minuscole nel nome del file ripristinato. Se non si osserva la distinzione tra maiuscole e minuscole quando si immette il nome file, l'applicazione non ripristina il file.
- Se la cartella di destinazione contiene già un file con lo stesso nome, l'applicazione annulla il ripristino del file.
- Se si utilizza la soluzione KATA (EDR), l'applicazione salva una copia del file nella Quarantena dopo il ripristino del file. È possibile svuotare manualmente la Quarantena. Per le soluzioni EDR Optimum ed EDR Expert, l'applicazione elimina il file dopo il ripristino.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Impostazioni avanzate	
`/REPLACE`	Sovrascrivi un file esistente.
`<file name>`	Il nome del file da ripristinare.

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Valori restituiti dal comando:

- `-1` indica che il comando non è supportato dalla versione dell'applicazione installata nel computer.
- `0` indica che il comando è stato eseguito correttamente.
- `1` indica che un argomento obbligatorio non è stato passato al comando.
- `2` indica che si è verificato un errore generale.
- `4` indica la presenza di un errore di sintassi.

IOCSCAN. Scansione degli indicatori di compromissione (IOC)

Esecuzione dell'attività *Scansione IOC*. Un *indicatore di compromissione (IOC)* è una serie di dati su un oggetto o un'attività che indica un accesso non autorizzato al computer (compromissione dei dati). Ad esempio, molti tentativi non riusciti di accesso al sistema possono costituire un indicatore di compromissione. L'attività *Scansione IOC* consente di trovare indicatori di compromissione sul computer e di adottare misure di risposta alle minacce.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

La scansione IOC viene interrotta dopo 128 corrispondenze con gli indicatori di compromissione descritti nei file IOC. Ciò è necessario per limitare il numero di voci nel rapporto delle attività di scansione IOC, per semplificarne l'analisi e per evitare l'overlow del rapporto a causa di indicatori di compromissione formulati in modo impreciso, che potrebbero generare un numero elevato di corrispondenze.

Sintassi del comando

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

File IOC	
`<full path to the IOC file>`	Percorso completo del file IOC che si desidera utilizzare per la scansione. È possibile specificare più file IOC separati da spazi. Il percorso completo del file IOC deve essere inserito senza l'argomento `/path`. Ad esempio, `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Percorso della cartella con i file IOC che si desidera utilizzare per la scansione. I *file IOC* sono file che contengono le serie di indicatori che l'applicazione tenta di abbinare per eseguire un rilevamento. I file IOC devono essere conformi allo standard OpenIOC. Ad esempio, `C:\Users\Admin\Desktop\IOC`

Tipo di dati per la scansione IOC	
`/process=on|off`	Analizza i dati dei processi durante l'esecuzione della scansione IOC (termine ProcessItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non analizza i processi in esecuzione sul computer durante l'esecuzione della scansione. Se il file IOC contiene i termini IOC del documento IOC ProcessItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza i dati dei processi solo se il documento IOC ProcessItem è descritto nel file IOC specificato per la scansione.
`/hint=<full path to the executable file of the process|full path to the file>`	Analizza i dati dei file durante l'esecuzione della scansione IOC (termini ProcessItem and FileItem). È possibile selezionare un file in uno dei seguenti modi: • `<full path to the executable file of the process>` - termine ProcessItem; • `<full path to the file>` - termine FileItem.
`/registry=on|off`	Analizza i dati del registro di sistema di Windows durante l'esecuzione di una scansione IOC (termine RegistryItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non esegue la scansione del registro di sistema di Windows. Se il file IOC contiene i termini del documento IOC RegistryItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza il registro di sistema di Windows solo se il documento IOC RegistryItem è descritto nel file IOC specificato per la scansione. Per il tipo di dati RegistryItem, Kaspersky Endpoint Security esamina una serie di chiavi del Registro di sistema.
`/dnsentry=on|off`	Analizza i dati sui record nella cache DNS locale durante l'esecuzione della scansione IOC (termine DnsEntryItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non esegue la scansione della cache DNS locale. Se il file IOC contiene i termini del documento IOC DnsEntryItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza la cache DNS locale solo se il documento IOC DnsEntryItem è descritto nel file IOC specificato per la scansione.
`/arpentry=on|off`	Analizza i dati sui record nella tabella ARP durante l'esecuzione della scansione IOC (termine ArpEntryItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non esegue la scansione della tabella ARP. Se il file IOC contiene i termini del documento IOC ArpEntryItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza la tabella ARP solo se il documento IOC ArpEntryItem è descritto nel file IOC specificato per la scansione.
`/ports=on|off`	Analizza i dati sulle porte aperte per l'ascolto durante l'esecuzione della scansione IOC (termine PortItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non esegue la scansione della tabella delle connessioni attive sul dispositivo. Se il file IOC contiene i termini del documento IOC PortItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza la tabella delle connessioni attive solo se il documento IOC PortItem è descritto nel file IOC specificato per la scansione.
`/services=on|off`	Analizza i dati sui servizi installati nel dispositivo durante l'esecuzione della scansione IOC (termine ServiceItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non esegue la scansione dei dati sui servizi installati nel dispositivo. Se il file IOC contiene i termini del documento IOC ServiceItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza i dati del servizio solo se il documento ServiceItem IOC è descritto nel file IOC specificato per la scansione.
`/system=on|off`	Analizza i dati dell'ambiente durante l'esecuzione della scansione IOC (termine SystemInfoItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non analizza i dati dell'ambiente. Se il file IOC contiene i termini del documento IOC SystemInfoItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza i dati dell'ambiente solo se il documento IOC SystemInfoItem è descritto nel file IOC specificato per la scansione.
`/users=on|off`	Analizza i dati sugli utenti durante l'esecuzione della scansione IOC (termine UserItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non analizza i dati sugli utenti creati nel sistema. Se il file IOC contiene i termini del documento IOC UserItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza i dati sugli utenti creati nel sistema solo se il documento IOC UserItem è descritto nel file IOC specificato per la scansione.

`/volumes=on|off`	Analizza i dati sui volumi durante l'esecuzione della scansione IOC (termine VolumeItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non esegue la scansione dei dati sui volumi nel dispositivo. Se il file IOC contiene i termini del documento IOC VolumeItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza i dati del volume solo se il documento IOC VolumeItem è descritto nel file IOC specificato per la scansione.
`/eventlog=on|off`	Analizza i dati sui record nel registro eventi di Windows durante l'esecuzione della scansione IOC (termine EventLogItem). Se il valore dell'argomento è `off`, Kaspersky Endpoint Security non esegue la scansione dei record nel registro eventi di Windows. Se il file IOC contiene i termini del documento IOC EventLogItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza il registro eventi di Windows se il documento IOC EventLogItem è descritto nel file IOC specificato per la scansione. Per il termine IOC EventLogItem\source, utilizzare il valore **Nome provider** dello schema XML dell'evento.
`/datetime=<event publication date>`	Prendere in considerazione la data in cui l'evento è stato pubblicato nel registro eventi di Windows quando si determina l'ambito di scansione IOC per il documento IOC corrispondente. Quando si esegue una scansione IOC, Kaspersky Endpoint Security esegue la scansione delle voci del registro eventi di Windows pubblicate durante il periodo dall'ora e dalla data specificate al momento in cui viene eseguita l'attività. Kaspersky Endpoint Security consente di specificare la data di pubblicazione dell'evento come valore dell'argomento. La scansione viene eseguita solo per gli eventi pubblicati nel registro eventi di Windows dopo la data specificata e prima dell'esecuzione della scansione. Se l'argomento non è specificato, Kaspersky Endpoint Security esegue la scansione degli eventi con qualsiasi data di pubblicazione. L'impostazione `TaskSettings::BaseSettings::EventLogItem::datetime` non può essere modificata. L'impostazione viene utilizzata solo se il documento IOC EventLogItem è descritto nel file IOC specificato per la scansione.
`/channel=<list of channels>`	Elenco dei nomi dei canali (registro) per i quali si desidera eseguire una scansione IOC. Se l'argomento è specificato, Kaspersky Endpoint Security esegue la scansione dei record pubblicati nei registri specificati. Il documento IOC deve avere il termine EventLogItem descritto. Il nome del registro viene specificato come stringa in conformità con il nome del registro (canale) specificato nelle proprietà del registro (il parametro Full Name) o nelle proprietà dell'evento (il parametro `<Channel></Channel>` nello schema XML dell'evento). È possibile specificare più canali separati da spazi. Se l'argomento non è specificato, Kaspersky Endpoint Security esegue la scansione dei record per i canali `Application`, `System`, `Security`.
`/files=on|off`	Analizza i dati del file durante l'esecuzione della scansione IOC (termine FileItem). Se il valore dell'argomento è `off` Kaspersky Endpoint Security non analizza i dati dei file. Se il file IOC contiene i termini del documento IOC FileItem, vengono ignorati (rilevati come nessuna corrispondenza). Se l'argomento non è specificato, Kaspersky Endpoint Security analizza i dati dei file solo se il documento IOC FileItem è descritto nel file IOC specificato per la scansione.
`/drives=<all|system|critical|custom>`	Imposta l'ambito della scansione IOC durante l'analisi dei dati per il documento IOC FileItem. È possibile impostare i seguenti valori per l'ambito della scansione: • `<all>` per tutti gli ambiti di file disponibili. • `<system>` per i file nelle cartelle in cui è installato il sistema operativo. • `<critical>` per i file temporanei nelle cartelle utente e di sistema. • `<custom>` per i file in ambiti definiti dall'utente (`/scope=<list of folders to scan>`). Se l'argomento non è specificato, la scansione viene eseguita per le aree critiche.
`/excludes=<list of exclusions>`	Imposta l'ambito di esclusione durante l'analisi dei dati per il documento IOC FileItem. È possibile specificare più percorsi separati da spazi.
`/scope=<list of folders to scan>`	Ambito della scansione IOC definito dall'utente durante l'analisi dei dati per il documento IOC FileItem (`/drives=custom`). È possibile specificare più percorsi separati da spazi.

`/retro /<number of days>`	*Scansione IOC retrospettiva* è una modalità dell'attività *Scansione IOC* in cui Kaspersky Endpoint Security esegue la scansione degli indicatori di compromissione utilizzando i dati per un determinato periodo di tempo. Questa modalità è destinata alla ricerca di indicatori di compromissione tramite la telemetria del computer protetto, ad esempio attività di rete, processi, file e altri dati di telemetria. È possibile impostare un periodo di tempo compreso tra 1 e 14 giorni. Per impostazione predefinita, l'applicazione esegue la scansione degli indicatori di compromissione per un giorno.
`/network=on|off`	Analisi dei dati di rete (il termine NetworkItem).
`/url=on|off`	Analisi dei dati nei registri del browser (il termine UrlHistoryItem). La scansione IOC retrospettiva analizza i registri dei seguenti browser: Google Chrome, Mozilla Firefox, Microsoft Edge (versione 79 o successiva).
`/email`	Analisi di oggetti di posta (il termine EmailItem).
`/route`	Analisi delle tabelle di instradamento e inoltro (il termine RouteEntryItem).

Valori restituiti dal comando:

- `-1` indica che il comando non è supportato dalla versione dell'applicazione installata nel computer.
- `0` indica che il comando è stato eseguito correttamente.
- `1` indica che un argomento obbligatorio non è stato passato al comando.
- `2` indica che si è verificato un errore generale.
- `4` indica la presenza di un errore di sintassi.

Se il comando è stato eseguito correttamente (valore restituito `0`) e sono stati rilevati indicatori di compromissione sul percorso, Kaspersky Endpoint Security restituisce le seguenti informazioni sui risultati dell'attività alla riga di comando:

`Uuid`	ID del file IOC dall'intestazione della struttura del file IOC (il tag `<ioc id="">`)
`Name`	Descrizione del file IOC dall'intestazione della struttura del file IOC (il tag `<description></description>`)
`Matched Indicator Items`	Elenco degli ID di tutti gli indicatori abbinati.
`Matched objects`	Dati per ogni documento IOC per cui è stata rilevata una corrispondenza.

MDRLICENSE. Attivazione MDR

Aggiunta del file di configurazione BLOB per attivare Managed Detection and Response. Il file BLOB contiene l'ID client e le informazioni sulla licenza per Kaspersky Managed Detection and Response. Il file BLOB si trova nell'archivio ZIP del file di configurazione MDR. È possibile ottenere l'archivio ZIP in Kaspersky Managed Detection and Response Console. Per informazioni dettagliate su un file BLOB, consultare la Guida di Kaspersky Managed Detection and Response.

I privilegi di amministratore sono necessari per eseguire operazioni con un file BLOB. Anche le impostazioni di Managed Detection and Response nel criterio devono essere disponibili per la modifica ( ).

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Operazione	
`/ADD <file name>`	Applicare il file di configurazione BLOB per l'integrazione con Kaspersky Managed Detection and Response (formato file P7). È possibile applicare un solo file BLOB. Se un file BLOB è già stato aggiunto al computer, il file verrà sostituito.
`/DEL`	Eliminare il file di configurazione BLOB.

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

Esempio

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. Integrazione EDR (KATA)

Comandi per la gestione del componente Endpoint Detection and Response (KATA):

- Abilitazione o disabilitazione del componente EDR (KATA).

  Il componente EDR (KATA) offre interoperabilità con la soluzione Kaspersky Anti Targeted Attack Platform.

- Configurazione della connessione ai server Kaspersky Anti Targeted Attack Platform.

- Visualizzazione delle impostazioni correnti del componente.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
```

```
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

Operazione	
`stop`	Disabilita il componente EDR (KATA).
`start`	Abilita il componente EDR (KATA).
`set`	Configura il componente EDR (KATA). Non è possibile configurare le seguenti impostazioni: • Aggiungere i server di Central Node (`servers=<server address>:<port>`) • Aggiungere un certificato TLS (`server-certificate=<path to the TLS certificate>`) • Impostare il timeout di connessione al server Central Node (`/timeout=<Central Node server connection timeout (s)>`) • Impostare il periodo per la sincronizzazione con il server Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Mostra le impostazioni correnti del componente.

EDRExpertOnPrem. Integrazione con EDR Expert (on-premises)

Comandi per la gestione dell'agente integrato per configurare l'integrazione con Kaspersky Endpoint Detection and Response Expert (on-premises):

- Abilitazione o disabilitazione dell'agente EDR Expert (on-premises) integrato.
- Configurazione delle impostazioni di connessione per i server EDR Expert (on-premises).
- Visualizzazione delle impostazioni correnti dell'agente integrato.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com START EDRExpertOnPrem
```

```
avp.com STOP EDRExpertOnPrem
```

```
avp.com EDRExpertOnPrem /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate>
[/client-certificate=<path to the PFX archive> /client-certificate-password=<password to the PFX archive>]
[/timeout=<server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
/telemetry-servers=<server address:port> /telemetry-server-certificate=<path to the TLS certificat> [telemetry-
client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>]
[/telemetry-timeout=<server connection timeout (s)>] [/events-send-period=<seconds>] [/events-limit=<0|1>]
[/events-per-hour=<number of events>] [/max-packet-length=<number of packets>] [/telemetry-only-tagged-events=
<0|1>] login=<user name> password=<password>
```

```
avp.com EDRExpertOnPrem /show
```

Operazione	Descrizione
`stop`	Disabilitare l'agente EDR Expert (on-premises) integrato.
`start`	Abilitare l'agente EDR Expert (on-premises) integrato.
`set`	Configurare l'agente EDR Expert (on-premises) integrato. È possibile configurare le seguenti impostazioni di connessione per i *server di risposta*: • `servers=<server address>:<port>`. Indirizzo del server di risposta (FQDN, IPv4, IPv6). • `server-certificate=<path to the TLS certificate>`. Certificato TLS per stabilire una connessione attendibile con il server. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). • `client-certificate=<path to the PFX archive> client-certificate-password=<password to the PFX archive>`. Utilizzare un contenitore crittografico per l'autenticazione a due vie. Un *contenitore crittografico* è un archivio PFX contenente un certificato e una chiave privata in formato PKCS#12. Per abilitare tale autenticazione, è necessario creare un contenitore crittografico presso un'autorità di certificazione esterna. • `timeout=<server connection timeout (s)>`. Timeout massimo del server di KUMA. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server. • `sync-period=<server synchronization period (min)>`. Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security riceve le attività di risposta alle minacce e invia i risultati delle attività. È possibile configurare le seguenti impostazioni di connessione per i *server di raccolta della telemetria*: • `telemetry-servers=<server address:port>`. Indirizzo del server di raccolta della telemetria (FQDN, IPv4, IPv6). • `telemetry-server-certificate=<path to the TLS certificat>`. Certificato TLS per stabilire una connessione attendibile con il server. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). • `telemetry-client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>`. Utilizzare un contenitore crittografico per l'autenticazione a due vie. Un *contenitore crittografico* è un archivio PFX contenente un certificato e una chiave privata in formato PKCS#12. Per abilitare tale autenticazione, è necessario creare un contenitore crittografico presso un'autorità di certificazione esterna. • `telemetry-timeout=<server connection timeout (s)>`. Timeout massimo del server di KUMA. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server. • `events-send-period=<seconds>`. Ritardo massimo nell'invio degli eventi. L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione. L'impostazione predefinita è 30 secondi. • `events-limit=<0|1>`. Limitare il numero di richieste. Questa funzionalità consente di ottimizzare il carico sul server. Se questa funzionalità è abilitata, l'applicazione limita la trasmissione degli eventi. Se il numero di eventi supera i limiti configurati, Kaspersky Endpoint Security interrompe l'invio degli eventi. • `events-per-hour=<number of events>`. Numero massimo di eventi all'ora L'applicazione analizza il flusso di dati di telemetria e limita l'invio degli eventi se il flusso di eventi supera il limite configurato di eventi all'ora. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora. L'impostazione predefinita è 3000 eventi all'ora. Se l'applicazione è installata in un server, il flusso di dati di telemetria è maggiore. Per i server, è consigliabile aumentare il valore a 60.000 eventi all'ora. • `max-packet-length=<number of packets>`. Lunghezza massima del pacchetto. L'applicazione si sincronizza con il server quando il buffer si riempie di eventi. L'impostazione predefinita è 1024 eventi. • `telemetry-only-tagged-events=<0|1>`. Invio della telemetria solo con IOA. *Indicatore di attacco (IOA)* è una regola che contiene una descrizione di un comportamento sospetto nel sistema che potrebbe indicare un attacco mirato. L'applicazione confronta il comportamento in corso nel sistema con queste regole e registra gli eventi indicativi di un attacco mirato. L'applicazione utilizza la tecnologia di *scansione in streaming*, che consente il monitoraggio in tempo reale di tali eventi. È possibile configurare le seguenti impostazioni generali: • `mode=EDRKATA | EDRExpertOnPrem`. Passaggio da una soluzione all'altra: • `EDRKATA`. Endpoint Detection and Response Expert (versione 7.1 o precedente). • `EDRExpertOnPrem`. Endpoint Detection and Response Expert (versione 8.0 o successiva). Valore predefinito. • `login=<user name> password=<password>`. Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.
`show`	Mostra le impostazioni correnti del componente.

KUMA. Integrazione di KUMA

Comandi per la gestione dell'agente KUMA integrato:

- Abilitazione o disabilitazione dell'integrazione KUMA.

  L'agente KUMA integrato fornisce interoperabilità con la soluzione Kaspersky Unified Monitoring and Analysis Platform.

- Configurazione della connessione ai server di Kaspersky Unified Monitoring and Analysis Platform.
- Visualizzazione delle impostazioni correnti del componente.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

Operazione	
`stop`	Disabilita l'integrazione KUMA.
`start`	Abilita l'integrazione KUMA.
`set`	Configura l'agente KUMA predefinito. Non è possibile configurare le seguenti impostazioni: • Aggiungere i server di KUMA (`/servers=<protocol>://<server address>:<port>`) L'applicazione supporta i seguenti protocolli di connessione al server: `tcp`, `udp`, `http`, `https`. • Aggiungere un certificato TLS (`/server-certificate=<path to the TLS certificate>`) • Impostare la connessione al server (`/timeout=<KUMA server connection timeout (s)>`) • Aggiungere un contenitore crittografico (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Configurare il ritardo di trasmissione degli eventi (`/maximum-data-transfer-time=<maximum events transmission delay (sec)`)
`show`	Mostra le impostazioni correnti del componente.

Autenticazione	
`/login=<user name> /password=<password>`	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA. Esecuzione della scansione YARA

Esecuzione dell'attività *Esegui scansione YARA*. L'applicazione esegue la scansione di file e oggetti alla ricerca di indicatori di attacchi mirati nell'infrastruttura IT aziendale utilizzando i database delle regole YARA. Le *regole YARA* sono descrizioni delle firme di attacchi mirati e intrusioni nell'infrastruttura IT aziendale utilizzate da Kaspersky Endpoint Security per eseguire la scansione degli oggetti.

Per eseguire una scansione YARA, è necessario preparare i file YARA che descrivono le regole. Durante la creazione dei file YARA, considerare i seguenti requisiti:

- Kaspersky Endpoint Security supporta i file YARA con le estensioni .YARA o .YAR, che sono conformi allo standard aperto YARA 4.2.3 per la descrizione degli indicatori di compromissione.
- Per l'attività possono essere specificati solo file con regole YARA. L'attività *Esegui scansione YARA* non supporta altri tipi di regole.
- Se sono stati aggiunti file YARA che Kaspersky Endpoint Security non supporta o se le regole contengono errori di sintassi, l'attività viene interrotta e viene visualizzato il messaggio di errore corrispondente.
- Gli identificatori di tutti i file YARA utilizzati in una singola attività Scansione IOC devono essere univoci. Se sono presenti file YARA con lo stesso identificatore, potrebbe influire sui risultati dell'esecuzione dell'attività.
- Una scansione YARA viene interrotta dopo 128 corrispondenze con gli indicatori descritti nelle regole YARA. Ciò è necessario per limitare il numero di voci nel rapporto di scansione YARA, in modo da semplificare l'analisi e proteggere il rapporto dall'overflow a causa di regole YARA formulate in modo impreciso che possono generare un elevato numero di corrispondenze.

Kaspersky consiglia di creare una regola per ogni file YARA. Questo rende i risultati della scansione più leggibili.

Una scansione YARA potrebbe richiedere molto tempo. A seconda delle dimensioni dell'unità, delle impostazioni delle attività e del numero di oggetti sul disco, una scansione YARA può durare da alcuni minuti a diverse ore. L'applicazione non mostra un indicatore di avanzamento. Non è possibile arrestare o annullare una scansione YARA. È consigliabile attendere fino a quando non saranno disponibili i risultati di una scansione YARA.

Sintassi del comando

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

File YARA	
`<full path to the YARA file>`	Percorso completo del file YARA che si desidera utilizzare per la scansione. È possibile specificare i percorsi di più file YARA separati da spazi. Argomento richiesto se il valore `/path=<path to the folder with YARA files>` non è specificato. Esempio: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	Percorso completo di una cartella con i file YARA che si desidera utilizzare per la scansione. Argomento richiesto se il valore `<full path to the YARA file>` non è specificato. Esempio: `/path=C:\Users\Admin\Desktop\YARA`

Impostazioni avanzate	
`/fastScan=<on|off>`	Scansione YARA rapida. Per ogni oggetto, l'applicazione registra un'occorrenza dell'indicatore rilevato. L'applicazione nasconde inoltre i duplicati degli indicatori rilevati nel registro. Scansione YARA rapida consente di eseguire più rapidamente la scansione di file di grandi dimensioni. Se questa impostazione non viene specificata, l'applicazione esegue una scansione YARA standard. In questa modalità, l'applicazione registra i duplicati degli indicatori rilevati.
`/maxRules=<maximum number of scan rules>`	Limite del numero di regole attivate che causano l'arresto della scansione YARA da parte dell'applicazione quando vengono raggiunte. Se il valore di questa impostazione non è specificato o seviene specificato `0`, l'applicazione esegue la scansione YARA senza limitazioni.
`/timeOut=<stop scan after the specified time in seconds>`	Quanto tempo può richiedere una scansione YARA, in secondi. Allo scadere di questo tempo, l'applicazione arresta la scansione YARA. Se il valore di questa impostazione non è specificato o seviene specificato `0`, l'applicazione esegue la scansione YARA senza limitazioni.
`/recursive=<on|off>`	Questo argomento avvia una scansione ricorsiva delle sottocartelle all'interno della scansione personalizzata `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Questo argomento avvia una scansione YARA dei file nell'elenco di cartelle specificato. È possibile specificare più valori separati da spazi. Kaspersky Endpoint Security supporta i caratteri `*` e `?` quando si inserisce la maschera di un percorso di cartella. Se questa impostazione non viene specificata, l'applicazione esegue una scansione YARA di tutti i dischi locali ad eccezione delle condivisioni di rete, delle unità cloud e dei supporti rimovibili.
`/scanMemory=<on|off>`	Scansione della memoria di tutti i processi in esecuzione.
`/scanProcess=<process name>`	Esegue la scansione della memoria solo per i processi specificati. Specificare i percorsi completi separati da spazi dei file eseguibili dei processi. È inoltre possibile utilizzare i caratteri `*` e `?` per immettere una maschera.
`/maxSize=<file size in bytes>`	Limita le dimensioni del file per la scansione YARA. L'applicazione ignora i file di grandi dimensioni.
`/includes=<list of objects to be scanned>>`	Modifica dell'ambito della scansione. È possibile specificare più valori separati da spazi. Sono disponibili i seguenti valori: • Nome file • Estensione file L'ambito della scansione deve essere specificato con il parametro `/scanFolders`. Esempio: `/scanFolders C:\*.* /includes=*.exe *.dll`: l'applicazione esegue la scansione di tutti i file con le estensioni .EXE e .DLL nel disco C.
`/excludes=<list of objects to be scanned>`	Esclusione di file dalla scansione YARA. È possibile specificare più valori separati da spazi. Sono disponibili i seguenti valori: • Percorso del file • Maschera del percorso del file Le esclusioni devono essere specificate con il parametro `/scanFolders`. Esempio: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml`: l'applicazione ignora il file readme.txt, tutti i file della cartella C:\trusted e tutti i file con estensione .XML nella cartella radice sul disco C.
`/scanAutoruns=<on|off>`	Scansione YARA degli oggetti con punti di esecuzione automatica.
`/excludeAutoruns=<list of autorun point areas to skip>`	Esclusione degli oggetti con punti di esecuzione automatica dall'ambito della scansione. Specificare i percorsi completi separati da spazi dei file eseguibili dei processi. È inoltre possibile utilizzare i caratteri `*` e `?` per immettere una maschera.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Se si specifica il percorso di una cartella, l'applicazione salva i risultati della scansione nel percorso specificato in un file denominato yara_<nome computer>_<ora completamento scansione>.txt. Se si specifica il percorso a un file TXT specifico, l'applicazione salva i risultati della scansione in tale file. Ad esempio, `/logFolder=C:\test` o `/logFolder=C:\test\abc.txt`. I risultati della scansione vengono inviati alla riga di comando indipendentemente dal fatto che l'opzione `/logFolder` sia specificata.

Valori restituiti dal comando:

- `-1` indica che il comando non è supportato dalla versione dell'applicazione installata nel computer.
- `0` indica che il comando è stato eseguito correttamente.
- `1` indica che un argomento obbligatorio non è stato passato al comando.
- `2` indica che si è verificato un errore generale.
- `4` indica la presenza di un errore di sintassi.
- `5` significa che uno o più file con le regole YARA specificate nel parametro non sono stati trovati.

Se il comando è stato eseguito correttamente (valore restituito `0`) e sono stati rilevati indicatori di compromissione sul percorso, Kaspersky Endpoint Security restituisce le seguenti informazioni sui risultati dell'attività alla riga di comando:

`Started at <time>` `Finished at <time>`	Ora di inizio e ora di completamento di una scansione.
`Host name: <computer name>`	Nome del computer in cui è stato rilevato l'oggetto.
`Result: <error>`	Codice di errore dell'errore che si è verificato durante l'esecuzione dell'attività. Se non sono presenti errori, l'applicazione esegue un output `0x00000000`.
`Comment: <comment text>`	Descrizione dell'errore che si è verificato durante l'esecuzione dell'attività. Ad esempio, `Operation timeout`.
`Object Name:` o `Process:` (durante la scansione della memoria di processo)	Il nome dell'oggetto o del processo in cui è stata attivata la regola YARA.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hash dell'oggetto in cui è stata attivata la regola YARA.
`Rule Name`	Nome della regola YARA attivata.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Metadati specificati nella regola YARA.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Trovate corrispondenze all'interno dell'oggetto che soddisfano le condizioni della regola YARA:
	• Offset nella memoria di processo o nel file in cui è stata rilevata una corrispondenza (`Offset`).
	• Il nome della stringa corrispondente nella regola YARA (`String name`).
	• La stringa corrispondente nella memoria di processo o nel file (`String data`).

TELEMETRYFILTERS. Filtraggio degli eventi da inviare a KUMA

Per impostazione predefinita, l'invio di eventi al server KUMA è disabilitato. Per garantire il corretto funzionamento di KUMA, è necessario abilitare l'invio della telemetria. È possibile selezionare un'origine evento tra i registri standard: *Application*, *Security* o *System*. Per migliorare le prestazioni e ottimizzare la trasmissione dei dati al server KUMA, è possibile aggiungere o escludere manualmente singoli eventi dalla telemetria. È ad esempio possibile escludere gli eventi Sysmon.

È possibile esportare l'elenco delle esclusioni in un file JSON dalla riga di comando.

Se il comando contiene solo il nome del file in cui si desidera esportare le impostazioni, l'applicazione posiziona il file come segue:

- Se il percorso di avp.com viene aggiunto alla variabile di sistema %PATH%, l'applicazione inserisce il file nella cartella `C:\Windows\SysWOW64`.
- Se si esegue il comando dalla cartella di installazione dell'applicazione, l'esportazione avrà esito negativo poiché l'autoprotezione dell'applicazione blocca la creazione di un nuovo file nella cartella dell'applicazione. Per esportare le impostazioni dell'applicazione in un file, immettere il percorso del file.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Operazione	
`export`	Esportazione dei filtri degli eventi da inviare a KUMA.
`import`	Importazione dei filtri degli eventi da inviare a KUMA. Se esistono già regole di filtraggio degli eventi nel computer, Kaspersky Endpoint Security le sostituisce durante l'importazione.

File da esportare o importare	
`<file name>`	Nome del file con i filtri degli eventi da inviare a KUMA. È inoltre possibile immettere il percorso del file. È possibile esportare i filtri per l'invio a KUMA in un file JSON.

Comandi di gestione di Light Agent

È possibile gestire l'applicazione in modalità Light Agent per proteggere gli ambienti virtuali dalla riga di comando. È possibile gestire l'applicazione in modalità Light Agent se la gestione tramite la console di Kaspersky Security Center non è possibile. È possibile visualizzare l'elenco dei comandi per la gestione dell'applicazione eseguendo il comando `HELP`. Per leggere la sintassi di un comando specifico, immettere `HELP <command>`.

Per gestire l'applicazione in modalità Light Agent dalla riga di comando:

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.
3. Utilizzare il seguente modello per eseguire il comando:

   ```
   avp.com <command> [options]
   ```

   In seguito a questa operazione, Kaspersky Endpoint Security eseguirà il comando.

L'applicazione installata in modalità Light Agent supporta quasi tutti i comandi AVP dell'applicazione installata in modalità Standard. In modalità Light Agent, le attività di aggiornamento dei database anti-virus e le attività di gestione delle chiavi di licenza sono limitate.

KSVLAINFO. Determinazione della modalità Light Agent

Determinazione della modalità Light Agent.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com KSVLAINFO
```

Il comando restituisce le seguenti informazioni alla console:

- Modalità Light Agent per la protezione degli ambienti virtuali: abilitata o disabilitata.

  Se la modalità Light Agent è abilitata, l'applicazione viene utilizzata come parte della soluzione Kaspersky Security for Virtualization Light Agent.

- Modalità di protezione VDI: abilitata o disabilitata.

  La modalità di protezione VDI consente di ottimizzare le prestazioni di Kaspersky Endpoint Security nelle macchine virtuali non persistenti. Se la modalità di protezione VDI è abilitata, gli aggiornamenti che richiedono il riavvio della macchina virtuale protetta non vengono installati nelle macchine virtuali non permanenti. Quando riceve gli aggiornamenti che richiedono il riavvio, Light Agent installato in una macchina virtuale non permanente invia un messaggio a Kaspersky Security Center in cui si indica che il modello di macchina virtuale protetta deve essere aggiornato.

- Tipo di macchina virtuale protetta: persistente o non persistente.

- Ruolo della macchina virtuale protetta nell'infrastruttura virtuale: server o workstation.

- Identificativo: UUID.

VIISINFO. Stato della connessione di Light Agent al server di integrazione

Visualizzazione delle informazioni sulla connessione del Light Agent al server di integrazione.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com VIISINFO
```

Il comando restituisce le seguenti informazioni alla console:

- Indirizzo e porta del server di integrazione a cui è connesso Light Agent.
- Stato della connessione del server di integrazione.
- Data e ora dell'ultima connessione del Light Agent al server di integrazione.

SVMINFO. Stato della connessione di Light Agent al server di protezione

Visualizzazione delle informazioni sulla connessione del Light Agent al server di protezione.

Per eseguire il comando, passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security. È inoltre possibile aggiungere il percorso del file eseguibile alla variabile di sistema %PATH% ed eseguire il comando senza passare alla cartella dell'applicazione.

Sintassi del comando

```
avp.com SVMINFO
```

Il comando restituisce le seguenti informazioni alla console:

- Indirizzo della SVM a cui è connesso il Light Agent e posizione della SVM nell'infrastruttura virtuale relativa al Light Agent: locale o non locale.
- Metodo di rilevamento delle SVM utilizzato da Light Agent: utilizzando un server di integrazione o un elenco personalizzato di indirizzi SVM.
- Elenco di indirizzi SVM se l'elenco di indirizzi SVM è selezionato come metodo di rilevamento delle SVM.
- Tag per la connessione di Light Agent alla SVM.
- Algoritmo di selezione delle SVM: standard o esteso. Se viene utilizzato l'algoritmo di selezione della SVM estesa, viene visualizzato anche il tipo di percorso della SVM nell'infrastruttura virtuale.
- Stato di protezione della connessione tra Light Agent e server di protezione.

Codici di errore

Possono verificarsi errori quando si utilizza l'applicazione dalla riga di comando. Quando si verificano errori, Kaspersky Endpoint Security mostra un messaggio di errore, ad esempio `Error: Cannot start task 'EntAppControl'`. Kaspersky Endpoint Security può inoltre mostrare informazioni aggiuntive sotto forma di un codice, ad esempio `error=8947906D` (vedere la tabella seguente).

Codice di errore	Descrizione
09479001	La chiave è già in uso
0947901D	La licenza è scaduta. Gli aggiornamenti dei database non sono disponibili
89479002	Chiave non trovata
89479003	Firma digitale mancante o danneggiata
89479004	I dati sono danneggiati
89479005	Il file chiave è danneggiato
89479006	La licenza è scaduta
89479007	File chiave non specificato
89479008	File chiave non valido
89479009	Salvataggio dati non riuscito
8947900A	Lettura dati non riuscita
8947900B	Errore di I/O
8947900C	Database non trovati
8947900E	Libreria di gestione delle licenze non caricata
8947900F	Database danneggiati o aggiornati manualmente
89479010	I database sono danneggiati
89479011	Impossibile utilizzare un file chiave non valido per aggiungere una chiave di riserva
89479012	Errore di sistema
89479013	Lista vietati delle chiavi danneggiata
89479014	La firma del file non corrisponde alla firma digitale di Kaspersky
89479015	Impossibile utilizzare una chiave per una licenza di prova come chiave per una licenza commerciale
89479016	È necessaria la licenza per il beta testing per utilizzare la versione beta dell'applicazione
89479017	Il file chiave non è compatibile con questa applicazione. Non è possibile attivare Kaspersky Endpoint Security for Windows con il file chiave di un'altra applicazione. Controllare l'applicazione installata
89479018	Chiave di licenza bloccata da Kaspersky
89479019	L'applicazione è già stata utilizzata con una licenza di prova. Impossibile aggiungere nuovamente una chiave per una licenza di prova
8947901A	Il file chiave è danneggiato
8947901B	Firma digitale mancante, danneggiata o non corrispondente alla firma digitale di Kaspersky
8947901C	Impossibile aggiungere una chiave se la licenza non commerciale corrispondente è scaduta
8947901E	La data di creazione o utilizzo del file chiave non è valida. Controllare la data di sistema
8947901F	Impossibile aggiungere una chiave per la licenza di prova. Un'altra chiave per la licenza di prova è già attiva
89479020	Lista vietati delle chiavi danneggiata o mancante
89479021	Descrizione dell'aggiornamento mancante o danneggiata
89479022	La chiave non è idonea per questa applicazione
89479023	Impossibile utilizzare un file chiave non valido per aggiungere una chiave di riserva
89479025	Errore di invio della richiesta al server di attivazione. Possibili motivi: errore della connessione Internet o problemi temporanei del server di attivazione. Provare ad attivare l'applicazione più tardi (dopo 1 o 2 ore) con il codice di attivazione. Se il problema persiste, contattare il provider della connessione Internet
89479026	La richiesta contiene un codice di attivazione errato
89479027	Impossibile ottenere lo stato della risposta

Codice di errore	Descrizione
89479028	Errore di salvataggio del file temporaneo
89479029	Il codice di attivazione è stato immesso in modo errato o nel computer è impostata una data di sistema non valida. Controllare la data di sistema nel computer
8947902A	La chiave non è compatibile con questa applicazione o la licenza è scaduta
8947902B	Impossibile ricevere il file chiave. È stato inserito un codice di attivazione errato
8947902C	Il server di attivazione ha restituito l'errore 400
8947902D	Il server di attivazione ha restituito l'errore 401
8947902E	Il server di attivazione ha restituito l'errore 403
8947902F	La risorsa necessaria non è disponibile sul server di attivazione. Il server di attivazione ha restituito l'errore 404. Verificare le impostazioni della connessione Internet
89479030	Il server di attivazione ha restituito l'errore 405
89479031	Il server di attivazione ha restituito l'errore 406
89479032	È richiesta l'autenticazione sul proxy. Controllare le impostazioni di rete
89479033	Timeout della richiesta
89479034	Il server di attivazione ha restituito l'errore 409
89479035	La risorsa necessaria non è disponibile sul server di attivazione. Il server di attivazione ha restituito l'errore 410. Verificare le impostazioni della connessione Internet
89479036	Il server di attivazione ha restituito l'errore 411
89479037	Il server di attivazione ha restituito l'errore 412
89479038	Il server di attivazione ha restituito l'errore 413
89479039	Il server di attivazione ha restituito l'errore 414
8947903A	Il server di attivazione ha restituito l'errore 415
8947903C	Errore interno del server
8947903D	Funzionalità non supportata
8947903E	Risposta del gateway non valida. Controllare le impostazioni di rete
8947903F	Risorsa temporaneamente non disponibile
89479040	Timeout della risposta del gateway. Controllare le impostazioni di rete
89479041	Il protocollo non è supportato dal server
89479043	Errore HTTP sconosciuto
89479044	ID risorsa non valido
89479046	URL non valida
89479047	Cartella di destinazione non valida
89479048	Errore di allocazione della memoria
89479049	Errore durante la conversione dei parametri in una stringa ANSI (URL, cartella, agente)
8947904A	Errore durante la creazione del thread di lavoro
8947904B	Thread di lavoro già in esecuzione
8947904C	Thread di lavoro non in esecuzione
8947904D	File chiave non trovato sul server di attivazione
8947904E	La chiave è bloccata
8947904F	Errore interno del server di attivazione
89479050	Dati insufficienti nella richiesta di attivazione

Codice di errore	Descrizione
89479053	La licenza che corrisponde alla chiave aggiunta è già scaduta
89479054	La data di sistema impostata nel computer non è valida. Controllare il valore della data di sistema
89479055	La licenza di prova è scaduta
89479056	Periodo di attivazione dell'applicazione scaduto
89479057	È stato superato il limite di attivazioni dell'applicazione per il codice specificato
89479058	Procedura di attivazione completata con errore di sistema
89479059	Impossibile utilizzare una chiave per una licenza di prova come chiave per una licenza commerciale
8947905C	È richiesto il codice di attivazione
89479062	Impossibile connettersi al server di attivazione
89479064	Il server di attivazione non è disponibile. Verificare le impostazioni della connessione Internet e ritentare l'attivazione
89479065	La licenza è scaduta
89479066	Impossibile sostituire la chiave attiva con una chiave scaduta
89479067	Impossibile aggiungere una chiave di riserva se la licenza corrispondente scade prima della licenza corrente
89479068	Chiave di abbonamento aggiornata mancante
8947906A	Codice di attivazione non valido
8947906B	Chiave già attiva
8947906C	I tipi di licenze relativi alle chiavi attive e di riserva non corrispondono
8947906D	Componente non supportato dalla licenza
8947906E	Impossibile aggiungere la chiave di abbonamento come chiave di riserva
89479213	Errore generico del livello di trasporto
89479214	Impossibile connettersi al server di attivazione
89479215	Formato indirizzo Web non valido
89479216	Impossibile convertire l'indirizzo del server proxy
89479217	Impossibile convertire l'indirizzo del server. Verificare le impostazioni della connessione Internet
89479218	Tentativo di connessione al server non riuscito
89479219	Accesso negato in remoto
8947921A	Timeout dell'operazione
8947921B	Errore durante l'invio della richiesta HTTP
8947921C	Errore di connessione SSL
8947921D	Operazione interrotta da callback
8947921E	Numero di reindirizzamenti eccessivo
8947921F	Controllo del destinatario non riuscito
89479220	Risposta vuota dal server
89479221	Errore durante l'invio dei dati
89479222	Errore durante la ricezione dei dati
89479223	Problema relativo al certificato SSL
89479224	Problema relativo al criptaggio SSL
89479225	Problema relativo all'autorità di certificazione SSL
89479226	Contenuto non valido del pacchetto di rete

Codice di errore	Descrizione
89479227	Accesso negato all'account
89479228	File di certificato SSL non valido
89479229	Impossibile arrestare la connessione SSL
8947922A	Errore ricorrente
8947922B	File non valido con certificati revocati
8947922C	Errore di richiesta del certificato SSL
89479401	Errore sconosciuto del server
89479402	Errore interno del server
89479403	Nessuna chiave disponibile per il codice di attivazione immesso
89479404	Chiave attiva bloccata
89479405	Parametri obbligatori della richiesta di attivazione mancanti
89479406	Numero cliente o password non validi
89479407	Codice di attivazione non valido
89479408	Il codice di attivazione non è compatibile con questa applicazione. Non è possibile attivare Kaspersky Endpoint Security for Windows con il codice di attivazione di un'altra applicazione. Controllare l'applicazione installata
89479409	È richiesto il codice di attivazione
8947940B	Periodo di attivazione scaduto
8947940C	È stato superato il numero massimo di attivazioni consentite per il codice specificato
8947940D	ID richiesta in formato non valido
8947940E	Codice di attivazione già in uso
8947940F	Impossibile rinnovare il codice di attivazione
89479410	Codice di attivazione non valido per questa area geografica
89479411	Impossibile utilizzare il codice di attivazione specificato per questa versione localizzata dell'applicazione
89479412	Il codice di attivazione è utilizzabile per la nuova versione dell'applicazione. Ottenere un codice di attivazione differente per attivare la versione installata dell'applicazione
89479413	Il server di attivazione ha restituito l'errore 643
89479414	Il server di attivazione ha restituito l'errore 644
89479415	Il server di attivazione ha restituito l'errore 645
89479416	Il server di attivazione ha restituito l'errore 646
89479417	È necessaria la versione 1.0 del server di attivazione
89479418	Formato del codice di attivazione errato
89479419	L'ora del computer non è sincronizzata con l'ora del server di attivazione
8947941A	Versione dell'applicazione errata
8947941B	Abbonamento scaduto
8947941C	Numero di attivazioni superato
8947941D	Firma del ticket non valida
8947941E	Sono necessari ulteriori dati
8947941F	Verifica dei dati non riuscita
89479420	Abbonamento inattivo
89479421	Il server di attivazione è in fase di manutenzione

Codice di errore	Descrizione
89479501	Errore imprevisto
89479502	È stato trasferito un parametro non valido, ad esempio un elenco vuoto di indirizzi di server di attivazione
89479503	Codice di attivazione non valido (hash non valido)
89479504	ID utente non valido
89479505	Password utente non valida
89479506	Risposta non valida dal server di attivazione
89479507	La richiesta di attivazione è stata interrotta
89479509	Il server di attivazione ha restituito un elenco di inoltro vuoto

Appendice. Profili dell'applicazione

Un *Profilo* è un componente, un'attività o una funzionalità di Kaspersky Endpoint Security. I profili vengono utilizzati per gestire l'applicazione dalla riga di comando. È possibile utilizzare i profili per eseguire i comandi `START`, `STOP`, `STATUS`, `STATISTICS` e `EXPORT`. Utilizzando i profili è possibile configurare le impostazioni dell'applicazione (ad esempio `STOP DeviceControl`) o eseguire attività (ad esempio, `START Scan_My_Computer`).

Sono disponibili i seguenti profili:

- `AdaptiveAnomaliesControl` – Controllo adattivo delle anomalie
- `AMSI` - Protezione AMSI.
- `AntiCryptor`
- `BehaviorDetection` - Rilevamento del Comportamento.
- `DeviceControl` – Controllo dispositivi
- `EntAppControl` – Controllo applicazioni
- `File_Monitoring` o `FM` – Protezione minacce file
- `Firewall` o `FW` – Firewall
- `HIPS` - Prevenzione Intrusioni Host.
- `IDS` – Protezione minacce di rete
- `IntegrityCheck` – Controllo integrità
- `LogInspector` – Log Inspection
- `Mail_Monitoring` o `EM` – Protezione minacce di posta
- `Rollback` – Ripristino degli aggiornamenti (il profilo non può essere applicato se l'applicazione è installata in Modalità Light Agent)
- `Scan_ContextScan` – Scansione dal menu di scelta rapida

- `Scan_IdleScan` – Scansione in background
- `Scan_Memory` – Scansione memoria kernel
- `Scan_My_Computer` – Scansione completa
- `Scan_Objects` – Scansione personalizzata
- `Scan_Qscan` – Scansione degli oggetti caricati all'avvio del sistema operativo
- `Scan_Removable_Drive` – Scansione unità rimovibili
- `Scan_Startup` or `STARTUP` – Scansione delle aree critiche
- `Updater` – Aggiorna (il profilo non può essere applicato se l'applicazione è installata in modalità Light Agent).
- `Web_Monitoring` o `WM` – Protezione minacce Web
- `WebControl` – Controllo Web

Kaspersky Endpoint Security supporta anche i profili di servizio. I profili di servizio possono essere richiesti quando si contatta l'Assistenza tecnica di Kaspersky.

Gestione dell'applicazione tramite REST API

Kaspersky Endpoint Security consente di configurare le impostazioni dell'applicazione, eseguire una scansione, aggiornare i database anti-virus ed eseguire altre attività utilizzando soluzioni di terzi. A tale scopo, Kaspersky Endpoint Security fornisce un'API. L'API REST di Kaspersky Endpoint Security funziona su HTTP ed è costituita da una serie di metodi di richiesta/risposta. Sostanzialmente è possibile gestire Kaspersky Endpoint Security tramite una soluzione di terzi e non tramite l'interfaccia dell'applicazione locale o Kaspersky Security Center Administration Console.

Per iniziare a utilizzare REST API, è necessario installare Kaspersky Endpoint Security con il supporto dell'API REST. Il client REST e Kaspersky Endpoint Security devono essere installati nello stesso computer.

Per garantire un'interazione sicura tra Kaspersky Endpoint Security e il client REST:

- Configurare la protezione del client REST dall'accesso non autorizzato in base ai suggerimenti dello sviluppatore del client REST. Configurare la protezione delle cartelle del client REST dalla scrittura tramite DACL (Discretionary Access Control List).
- Per eseguire il client REST, utilizzare un account separato con diritti di amministratore. Vietare l'accesso interattivo al sistema per questo account.

L'applicazione è gestita tramite REST API all'indirizzo http://127.0.0.1 o http://localhost. Non è possibile gestire in remoto Kaspersky Endpoint Security tramite REST API.

APRI LA DOCUMENTAZIONE DELL'API REST

Installazione dell'applicazione con REST API

Per gestire l'applicazione tramite l'API REST, è necessario installare Kaspersky Endpoint Security con il supporto dell'API REST. Se si gestisce Kaspersky Endpoint Security tramite REST API, non è possibile gestire l'applicazione utilizzando Kaspersky Security Center.

Preparazione dell'installazione dell'applicazione con supporto della REST API

L'interazione sicura di Kaspersky Endpoint Security con il client REST richiede la configurazione dell'identificazione delle richieste. A tale scopo, è necessario installare un certificato e successivamente firmare il payload di ogni richiesta.

Per creare un certificato, è possibile utilizzare OpenSSL, ad esempio.

Esempio:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Utilizzare l'algoritmo di criptaggio RSA con una lunghezza della chiave pari o superiore a 2048 bit.

Di conseguenza, si otterrà un certificato `cert.pem` e una chiave privata `key.pem`.

Installazione dell'applicazione con supporto della REST API

Per installare Kaspersky Endpoint Security con il supporto dell'API REST:

1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.
2. Passare alla cartella contenente il pacchetto di distribuzione per Kaspersky Endpoint Security versione 11.2.0 o successiva.
3. Installare Kaspersky Endpoint Security con le seguenti impostazioni:
   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     Nome utente per la gestione dell'applicazione mediante REST API. Immettere il nome utente nel formato `<DOMAIN>\<UserName>` (ad esempio `RESTAPI_User=COMPANY\Administrator`). È possibile gestire l'applicazione tramite REST API solo con questo account. È possibile selezionare un solo utente per l'utilizzo dell'API REST.
   - `RESTAPI_Port=<port>`

     Porta utilizzata per la gestione dell'applicazione tramite REST API. La porta 6782 è utilizzata per impostazione predefinita. Assicurarsi che la porta sia libera. Parametro opzionale.
   - `RESTAPI_Certificate=<path to certificate>`

     Certificato per l'identificazione delle richieste (ad esempio, `RESTAPI_Certificate=C:\cert.pem`).

     È possibile installare il certificato dopo aver installato l'applicazione o aggiornare il certificato dopo la scadenza del certificato.

     Come installare un certificato per l'identificazione della richiesta REST API

     1. Disabilitazione di Auto-difesa di Kaspersky Endpoint Security

        Il meccanismo Auto-difesa impedisce la modifica o l'eliminazione dei file dell'applicazione sul disco rigido, dei processi in memoria e delle voci del Registro di sistema.
     2. Passare alla chiave di registro che contiene le impostazioni della REST API:
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. Immettere il percorso del certificato, ad esempio `Certificate = C:\Folder\cert.pem`.
     4. Abilitare Auto-difesa di Kaspersky Endpoint Security.
     5. Riavviare l'applicazione.
   - `AdminKitConnector=1`

     Gestione dell'applicazione tramite sistemi di amministrazione. La gestione è consentita per impostazione predefinita.

È inoltre possibile utilizzare il file setup.ini per definire le impostazioni per l'utilizzo dell'API REST.

Esempio:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
/pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
```

Successivamente sarà possibile gestire l'applicazione tramite l'API REST. Per verificarne il funzionamento, aprire la documentazione dell'API REST utilizzando una richiesta GET.

Esempio:
```
GET http://localhost:6782/kes/v1/api-docs
```

Se l'applicazione è stata installata con il supporto della REST API, Kaspersky Endpoint Security crea automaticamente una regola di autorizzazione nelle impostazioni di Controllo Web per l'accesso alle risorse Web (*Regola di servizio per la REST API*). Questa regola è necessaria per consentire al client REST di accedere a Kaspersky Endpoint Security in qualsiasi momento. Ad esempio, se è stato limitato l'accesso dell'utente alle risorse Web, ciò non influirà sulla gestione dell'applicazione tramite la REST API. Si consiglia di non eliminare la regola o modificare le impostazioni di *Regola di servizio per la REST API*. Se la regola è stata eliminata, Kaspersky Endpoint Security la ripristinerà dopo aver riavviato l'applicazione.

Utilizzo dell'API

Non è possibile limitare l'accesso all'applicazione tramite REST API utilizzando Protezione tramite password. Non è ad esempio possibile impedire a un utente di disabilitare la protezione tramite REST API. È possibile configurare Protezione tramite password utilizzando REST API e limitare l'accesso dell'utente all'applicazione mediante l'interfaccia locale.

Per gestire l'applicazione tramite REST API, è necessario eseguire il client REST con l'account specificato durante l'installazione dell'applicazione con il supporto dell'API REST. È possibile selezionare un solo utente per l'utilizzo dell'API REST.

APRI LA DOCUMENTAZIONE DELL'API REST

La gestione dell'applicazione tramite REST API prevede i seguenti passaggi:

1. Ottenere i valori correnti delle impostazioni dell'applicazione. A tale scopo, inviare una richiesta GET.

   Esempio:
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. L'applicazione invierà una risposta con la struttura e i valori delle impostazioni. Kaspersky Endpoint Security supporta i formati XML e JSON.

   Esempio:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Modificare le impostazioni dell'applicazione. Utilizzare la struttura delle impostazioni ricevuta in risposta alla richiesta GET.

   Esempio:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. Salvare le impostazioni dell'applicazione (il payload) in un file JSON (payload.json).

5. Firmare il file JSON nel formato PKCS7.

   Esempio:

   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
   signed_payload.pem
   ```

   A questo punto, si ottiene un file firmato con il payload della richiesta (`signed_payload.pem`).

6. Modificare le impostazioni dell'applicazione. A tale scopo, inviare una richiesta POST e allegare il file firmato con il payload della richiesta (`signed_payload.pem`).

L'applicazione applica le nuove impostazioni e invia una risposta con i risultati della configurazione dell'applicazione (la risposta può essere vuota). È possibile verificare che le impostazioni siano aggiornate tramite una richiesta GET.

Fonti di informazioni sull'applicazione

Questa sezione descrive le fonti delle informazioni sull'applicazione.

È possibile scegliere la fonte delle informazioni più adatta a seconda dell'importanza e dell'urgenza del problema.

Pagina di Kaspersky Endpoint Security nel sito Web di Kaspersky

Nella pagina di Kaspersky Endpoint Security è possibile visualizzare informazioni generali sull'applicazione, le relative funzioni e caratteristiche.

La pagina di Kaspersky Endpoint Security contiene un collegamento al negozio online. Tramite il negozio online è possibile acquistare o rinnovare l'applicazione.

Pagina di Kaspersky Endpoint Security nella Knowledge Base

La *Knowledge Base* è una sezione del sito Web dell'Assistenza tecnica.

La pagina di Kaspersky Endpoint Security nella Knowledge Base contiene articoli che forniscono informazioni utili, suggerimenti e risposte a domande frequenti su come acquistare, installare e utilizzare l'applicazione.

Gli articoli della Knowledge Base possono rispondere a domande relative non solo a Kaspersky Endpoint Security ma anche ad altre applicazioni di Kaspersky. Gli articoli nella Knowledge Base possono anche contenere notizie provenienti dall'Assistenza tecnica.

Discussione delle applicazioni Kaspersky nel Forum

Se la domanda non richiede una risposta urgente, è possibile sottoporla agli esperti di Kaspersky e ad altri utenti nel nostro Forum.

Nel Forum, è possibile visualizzare gli argomenti esistenti, lasciare i propri commenti e creare nuovi argomenti di discussione.

Come contattare l'assistenza tecnica

Se non è possibile trovare una soluzione per il problema nella documentazione o in altre fonti di informazioni su Kaspersky Endpoint Security, è consigliabile contattare l'Assistenza tecnica. L'Assistenza tecnica risponde ai quesiti in merito all'installazione e all'utilizzo di Kaspersky Endpoint Security.

Kaspersky garantisce il supporto per Kaspersky Endpoint Security durante il ciclo di vita dell'applicazione (fare riferimento alla pagina del ciclo di vita dell'applicazione). Prima di contattare l'Assistenza tecnica, consultare le regole dell'assistenza.

È possibile contattare l'Assistenza tecnica in uno dei seguenti modi:

- Visitando il sito Web dell'Assistenza tecnica
- Inviando una richiesta all'Assistenza tecnica di Kaspersky attraverso il portale Kaspersky CompanyAccount

Dopo avere segnalato un problema agli specialisti dell'Assistenza tecnica di Kaspersky, questi possono richiedere di creare un *file di traccia*. Il file di traccia consente di monitorare tutti i passaggi del processo di esecuzione dei comandi dell'applicazione e di determinare in quale fase dell'esecuzione dell'applicazione si è verificato l'errore.

Gli specialisti dell'Assistenza tecnica possono anche richiedere ulteriori informazioni sul sistema operativo, dati sui processi in esecuzione nel computer, rapporti dettagliati sull'esecuzione dei componenti dell'applicazione.

Durante l'esecuzione della diagnostica, gli esperti dell'Assistenza tecnica possono richiedere di modificare le impostazioni dell'applicazione:

- Attivazione della funzionalità di ricezione delle informazioni di diagnostica estese.
- Configurare i singoli componenti dell'applicazione modificando le impostazioni speciali che non sono accessibili tramite l'interfaccia utente standard.
- Modifica delle impostazioni per l'archiviazione delle informazioni di diagnostica.
- Configurazione dell'intercettazione e della registrazione del traffico di rete.

Gli esperti dell'Assistenza tecnica forniranno tutte le informazioni necessarie per l'esecuzione di tali operazioni (descrizione della procedura, impostazioni da modificare, file di configurazione, script, funzionalità aggiuntive della riga di comando, moduli di debug, utilità per utilizzi speciali e così via) e informeranno l'utente dell'ambito dei dati utilizzati per le operazioni di debug. Le informazioni di diagnostica estese vengono salvate nel computer dell'utente. I dati non vengono trasmessi automaticamente a Kaspersky.

Le operazioni elencate vanno eseguite solo dietro supervisione degli specialisti dell'Assistenza tecnica, in base alle relative istruzioni. La modifica delle impostazioni dell'applicazione in autonomia e con modalità non descritte nella Guida in linea o secondo i suggerimenti dell'Assistenza tecnica può causare rallentamenti e arresti anomali del sistema operativo, ridurre il livello di protezione del computer e danneggiare la disponibilità e l'integrità delle informazioni elaborate.

Contenuto e archiviazione dei file di traccia

L'utente è personalmente responsabile della sicurezza dei dati archiviati nel computer, in particolare del monitoraggio e della limitazione dell'accesso ai dati fino al momento dell'invio a Kaspersky.

I file di traccia sono memorizzati nel computer finché l'applicazione è in uso e vengono eliminati definitivamente quando l'applicazione viene rimossa.

I file di traccia, tranne i file di traccia dell'Agente di Autenticazione, vengono archiviati nella cartella `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

I file di traccia sono denominati come segue: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

È possibile visualizzare i dati salvati nei file di traccia.

Tutti i file di traccia contengono i seguenti dati comuni:

- Ora dell'evento
- Numero del thread di esecuzione

  Il file di traccia dell'Agente di Autenticazione non contiene questa informazione.

- Componente dell'applicazione che ha causato l'evento
- Livello di gravità di evento (evento informativo, avviso, evento critico, errore)
- Descrizione dell'evento, inclusi l'esecuzione di un comando da parte di un componente dell'applicazione e il risultato dell'esecuzione di questo comando.

Contenuto dei file di traccia SRV.log, GUI.log e ALL.log

I file di traccia `SRV.log`, `GUI.log` e `ALL.log` possono archiviare le seguenti informazioni oltre ai dati generali:

- I dati personali, compresi il cognome, il nome e il secondo nome, se tali dati sono inclusi nel percorso dei file sul computer locale.
- Dati sull'hardware installato nel computer (ad esempio i dati del firmware BIOS/UEFI). Questi dati vengono scritti nei file di traccia durante l'esecuzione di Criptaggio disco Kaspersky.
- Il nome utente e la password se sono stati trasmessi in formato non criptato. Questi dati possono essere registrati nei file di traccia durante la scansione del traffico Internet.
- Il nome utente e la password, se sono contenuti nelle intestazioni HTTP.

- Il nome dell'account Microsoft Windows se il nome dell'account è incluso nel nome di un file.
- L'indirizzo e-mail dell'utente o un indirizzo Web che contiene il nome dell'account e la password, se sono contenuti nel nome dell'oggetto rilevato.
- I siti Web visitati e i reindirizzamenti da tali siti Web. Questi dati vengono scritti nei file di traccia quando l'applicazione esegue la scansione dei siti Web.
- L'indirizzo del server proxy, il nome del computer, la porta, l'indirizzo IP e il nome utente utilizzati per accedere al server proxy. Questi dati vengono scritti nei file di traccia se l'applicazione utilizza un server proxy.
- Gli indirizzi IP remoti a cui il computer ha stabilito connessioni.
- L'oggetto del messaggio, l'ID, il nome del mittente e l'indirizzo della pagina Web del mittente del messaggio in un social network. Questi dati vengono scritti nei file di traccia se il componente Controllo Web è abilitato.
- Dati relativi al traffico di rete. Questi dati vengono scritti su file di traccia se i componenti di monitoraggio del traffico sono abilitati (ad esempio Controllo Web).
- Dati ricevuti dai server Kaspersky (ad esempio la versione dei database anti-virus).
- Stati dei componenti Kaspersky Endpoint Security e relativi dati operativi.
- Dati sull'attività dell'utente nell'applicazione.
- Eventi del sistema operativo.

Contenuto dei file di traccia HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Oltre ai dati generali, il file di traccia `HST.log` contiene informazioni sull'esecuzione di un'attività di aggiornamento dei database e dei moduli dell'applicazione.

Oltre ai dati generali, il file di traccia `BL.log` contiene informazioni sugli eventi che si verificano durante l'esecuzione dell'applicazione, nonché i dati richiesti per la risoluzione dei problemi dell'applicazione. Questo file viene creato se l'applicazione è avviata con il parametro avp.exe –bl.

Oltre ai dati generali, il file di traccia `Dumpwriter.log` contiene informazioni di servizio richieste per la risoluzione dei problemi che si verificano durante la scrittura del file di dump dell'applicazione.

Oltre ai dati generali, il file di traccia `WD.log` contiene informazioni sugli eventi che si verificano durante l'esecuzione del servizio avpsus, inclusi gli eventi relativi all'aggiornamento dei moduli dell'applicazione.

Oltre ai dati generali, il file di traccia `AVPCon.dll.log` contiene informazioni sugli eventi che si verificano durante l'esecuzione del modulo di connettività di Kaspersky Security Center.

Contenuti dei file di traccia delle prestazioni

I file di traccia delle prestazioni sono denominati come segue:
`KES<14.2_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Oltre ai dati generali, i file di traccia delle prestazioni contengono informazioni sul carico del processore, informazioni sul tempo di caricamento del sistema operativo e delle applicazioni e informazioni sui processi in esecuzione.

Contenuti dei file di traccia del componente Protezione AMSI

In aggiunta ai dati generali, il file di traccia `AMSI.log` contiene informazioni sui risultati delle scansioni eseguite sulle richieste dalle applicazioni di terze parti.

Contenuti dei file di traccia del componente Protezione minacce di posta

Oltre ai dati generali, il file di traccia `mcou.OUTLOOK.EXE.log` può contenere parti di messaggi e-mail, inclusi gli indirizzi e-mail.

Contenuti dei file di traccia del componente Scansione dal menu di scelta rapida

Il file di traccia `shellex.dll.log` contiene informazioni sul completamento dell'attività di scansione e sui dati richiesti per eseguire il debug dell'applicazione, in aggiunta alle informazioni generali.

Contenuti dei file di traccia del plug-in Web dell'applicazione

I file di traccia del plug-in Web dell'applicazione sono archiviati nel computer in cui viene distribuito Kaspersky Security Center Web Console, nella cartella `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

I file di traccia del plug-in Web dell'applicazione vengono denominati come segue: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. Web Console inizia a scrivere i dati dopo l'installazione ed elimina i file di traccia dopo la rimozione di Web Console.

I file di traccia del plug-in Web dell'applicazione contengono le seguenti informazioni, in aggiunta ai dati generali:

- Password dell'utente KLAdmin per sbloccare l'interfaccia di Kaspersky Endpoint Security (Protezione tramite password).
- Password provvisoria per sbloccare l'interfaccia di Kaspersky Endpoint Security (Protezione tramite password).
- Nome utente e password per il server di posta SMTP (Notifiche e-mail).
- Nome utente e password per il server proxy Internet (Server proxy).
- Nome utente e password per l'attività *Modifica i componenti dell'applicazione*.
- Percorsi e credenziali dell'account specificati nelle attività e nelle proprietà dei criteri di Kaspersky Endpoint Security.

Contenuto del file di traccia dell'Agente di Autenticazione

Il file di traccia dell'Agente di Autenticazione è archiviato nella cartella System Volume Information e viene denominato nel modo seguente: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

In aggiunta ai dati generali, il file di traccia dell'Agente di Autenticazione contiene informazioni sull'esecuzione dell'Agente di Autenticazione e sulle azioni eseguite dall'utente con l'Agente di Autenticazione.

Tracciamento del funzionamento dell'applicazione

Il *tracciamento dell'applicazione* è un record dettagliato delle azioni eseguite dall'applicazione e dei messaggi sugli eventi che si verificano durante l'esecuzione dell'applicazione. Durante il processo di tracciamento, l'applicazione crea un set di file con dati sul funzionamento dei diversi componenti dell'applicazione (ad esempio SRV.log, WD.log e altri).

Il tracciamento dell'applicazione deve essere eseguito sotto la supervisione dell'Assistenza tecnica di Kaspersky.

Per creare il file di traccia dell'applicazione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra visualizzata, fare clic sul pulsante **Strumenti di assistenza**.
3. Utilizzare l'interruttore **Abilita tracciamento dell'applicazione** per abilitare o disabilitare il tracciamento del funzionamento dell'applicazione.
4. Nell'elenco a discesa **Tracciamento**, selezionare una modalità di tracciamento dell'applicazione:
   - **Con limitazione della dimensione**. Salva le tracce in un numero limitato di set di file di dimensioni limitate e sovrascrivi i file meno recenti quando viene raggiunta la dimensione massima. Se questa modalità è selezionata, è possibile definire il numero massimo di set di file per la rotazione e la dimensione massima per ogni set di file.

     Per impostazione predefinita, l'applicazione salva cinque set di file di traccia. La dimensione di ciascun set di file è 3072 MB. In questo modo, sono necessari 15 GB di spazio libero su disco per salvare i file di traccia.
   - **Senza limitazioni**. Salva un file di traccia (nessun limite di dimensioni).
5. Nell'elenco a discesa **Livello** selezionare il livello di traccia:
   - **Normale** significa che il file di traccia salva i messaggi su tutti gli errori, gli avvisi e le informazioni sul normale funzionamento dell'applicazione (impostazione predefinita).
   - **Dettagliato** significa che il file di traccia salva tutte le informazioni sull'esecuzione dell'applicazione.

   Sono disponibili livelli di tracciamento aggiuntivi se si gestiscono le impostazioni di tracciamento dell'applicazione nella riga di comando. È consigliabile richiedere il livello di traccia necessario a uno specialista dell'Assistenza tecnica. In mancanza di indicazioni da parte dell'Assistenza tecnica, impostare il livello di traccia su **Normale**.

Se il tracciamento dell'applicazione è stato abilitato nella riga di comando ed è stato impostato un livello di tracciamento diverso da **Normale** o **Dettagliato**, l'elenco a discesa **Livello** è impostato su **Normale**.

6. Per interrompere il processo di tracciamento, tornare alla finestra **Strumenti di assistenza** e disabilitare il tracciamento.

È inoltre possibile creare i file di traccia durante l'installazione dell'applicazione dalla riga di comando, anche utilizzando il file setup.ini.

Di conseguenza, nella cartella `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` vengono creati file di traccia delle operazioni dell'applicazione. Dopo la creazione dei file di traccia, inviare i file all'Assistenza tecnica di Kaspersky.

Kaspersky Endpoint Security elimina automaticamente i file di traccia quando l'applicazione viene rimossa. I file possono essere rimossi anche manualmente. A tale scopo, è necessario disabilitare il tracciamento e arrestare l'applicazione.

Tracciamento delle prestazioni dell'applicazione

Kaspersky Endpoint Security consente di ricevere le informazioni sui problemi operativi dei computer durante l'utilizzo dell'applicazione. È ad esempio possibile ricevere informazioni sui ritardi nel caricamento del sistema operativo dopo l'installazione dell'applicazione. A tale scopo, Kaspersky Endpoint Security crea file di traccia delle prestazioni. Per *tracciamento delle prestazioni* si intende la registrazione delle azioni eseguite dall'applicazione allo scopo di diagnosticare i problemi di prestazioni di Kaspersky Endpoint Security. Per ricevere le informazioni, Kaspersky Endpoint Security utilizza il servizio ETW (Event Tracing for Windows). L'Assistenza tecnica di Kaspersky si occupa della diagnosi dei problemi di Kaspersky Endpoint Security e di stabilire le cause di tali problemi.

Il tracciamento dell'applicazione deve essere eseguito sotto la supervisione dell'Assistenza tecnica di Kaspersky.

Per creare un file di traccia delle prestazioni:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra visualizzata, fare clic sul pulsante **Strumenti di assistenza**.
3. Utilizzare l'interruttore **Abilita tracciamento delle prestazioni** per abilitare o disabilitare il tracciamento delle prestazioni dell'applicazione.
4. Nell'elenco a discesa **Tracciamento**, selezionare una modalità di tracciamento dell'applicazione:
   - **Con limitazione della dimensione**. Salva le tracce in un numero limitato di file di dimensioni limitate e sovrascrivi i file meno recenti quando viene raggiunta la dimensione massima. Se questa modalità è selezionata, è possibile definire la dimensione massima per ogni file.
   - **Senza limitazioni**. Salva un file di traccia (nessun limite di dimensioni).

5. Nell'elenco a discesa **Livello** selezionare il livello di traccia:

   - **Superficiale**. Kaspersky Endpoint Security analizza i più importanti processi del sistema operativo relativi alle prestazioni.

   - **Dettagliato**. Kaspersky Endpoint Security analizza tutti i processi del sistema operativo relativi alle prestazioni.

6. Nell'elenco a discesa **Tipo di tracciamento** selezionare il tipo di tracciamento:

   - **Informazioni di base**. Kaspersky Endpoint Security analizza i processi mentre è in esecuzione il sistema operativo. Utilizzare questo tipo di tracciamento se un problema persiste dopo il caricamento del sistema operativo, ad esempio un problema di accesso a Internet nel browser.

   - **Al riavvio**. Kaspersky Endpoint Security analizza i processi solo durante il caricamento del sistema operativo. Al termine del caricamento del sistema operativo, Kaspersky Endpoint Security interrompe il tracciamento. Utilizzare questo tipo di tracciamento se il problema riguarda un ritardo nel caricamento del sistema operativo.

7. Riavviare il computer e provare a riprodurre il problema.

8. Per interrompere il processo di tracciamento, tornare alla finestra Strumenti di supporto e disabilitare il tracciamento.

Di conseguenza, nella cartella `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` viene creato un file di traccia delle prestazioni. Dopo la creazione del file di traccia, inviare il file all'Assistenza tecnica di Kaspersky.

Scrittura di dump

Un file di dump contiene tutte le informazioni sulla memoria di lavoro dei processi di Kaspersky Endpoint Security nel momento in cui è stato creato il file di dump.

I file di dump salvati possono contenere dati riservati. Per controllare l'accesso ai dati, è necessario verificare singolarmente la sicurezza dei file di dump.

I file di dump sono memorizzati nel computer finché l'applicazione è in uso e vengono eliminati definitivamente quando l'applicazione viene rimossa. I file di dump sono archiviati nella cartella `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

Come abilitare la scrittura di dump in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.

2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.

3. Nella finestra del criterio, selezionare **Impostazioni generali** → **Impostazioni applicazione**.

4. Nel blocco **Informazioni di debug**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, utilizzare la casella di controllo **Abilita scrittura di dump** per abilitare o disabilitare la scrittura di dump delle applicazioni.

6. Salvare le modifiche.

Come abilitare la scrittura di dump in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse** → **Criteri**.

2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.

3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni generali** → **Assistenza tecnica**.

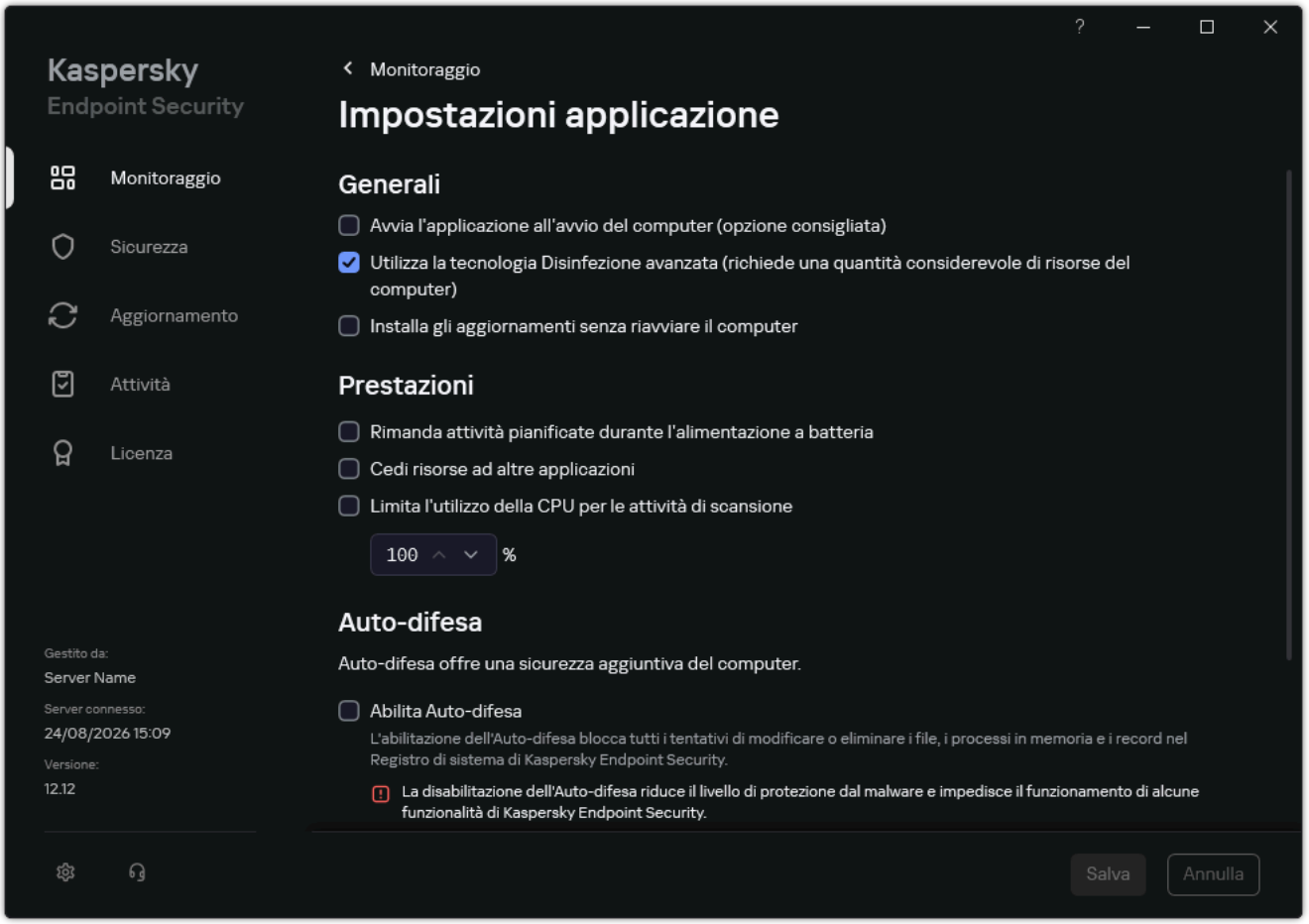
5. Nella sezione **Informazioni di debug**, utilizzare la casella di controllo **Scrittura dump ABILITATA** per abilitare o disabilitare la scrittura di dump delle applicazioni.

6. Salvare le modifiche.

Come abilitare la scrittura di dump nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.

2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.



Impostazioni di Kaspersky Endpoint Security for Windows

3. Nella sezione **Informazioni di debug**, utilizzare la casella di controllo **Abilita scrittura di dump** per abilitare o disabilitare la scrittura di dump delle applicazioni.

4. Salvare le modifiche.

Protezione dei file di dump e dei file di traccia

I file di dump e i file di traccia contengono informazioni sul sistema operativo e possono anche contenere dati dell'utente. Per evitare l'accesso non autorizzato a tali dati, è possibile abilitare la protezione dei file di dump e di traccia.

Se la protezione dei file di dump e di traccia è abilitata, i file sono accessibili per i seguenti utenti:

- I file di dump sono accessibili per l'amministratore di sistema e l'amministratore locale, nonché per l'utente che ha abilitato la scrittura dei file di dump e di traccia.
- I file di traccia sono accessibili solo per l'amministratore di sistema e l'amministratore locale.

Come abilitare la protezione dei file di dump e dei file di traccia in Administration Console (MMC)

1. Nella struttura Kaspersky Security Center Administration Console, selezionare **Criteri**.
2. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
3. Nella finestra del criterio, selezionare **Impostazioni generali → Impostazioni applicazione**.
4. Nel blocco **Informazioni di debug**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, utilizzare la casella di controllo **Abilita protezione dei file di dump e di traccia** per abilitare o disabilitare la protezione dei file.
6. Salvare le modifiche.

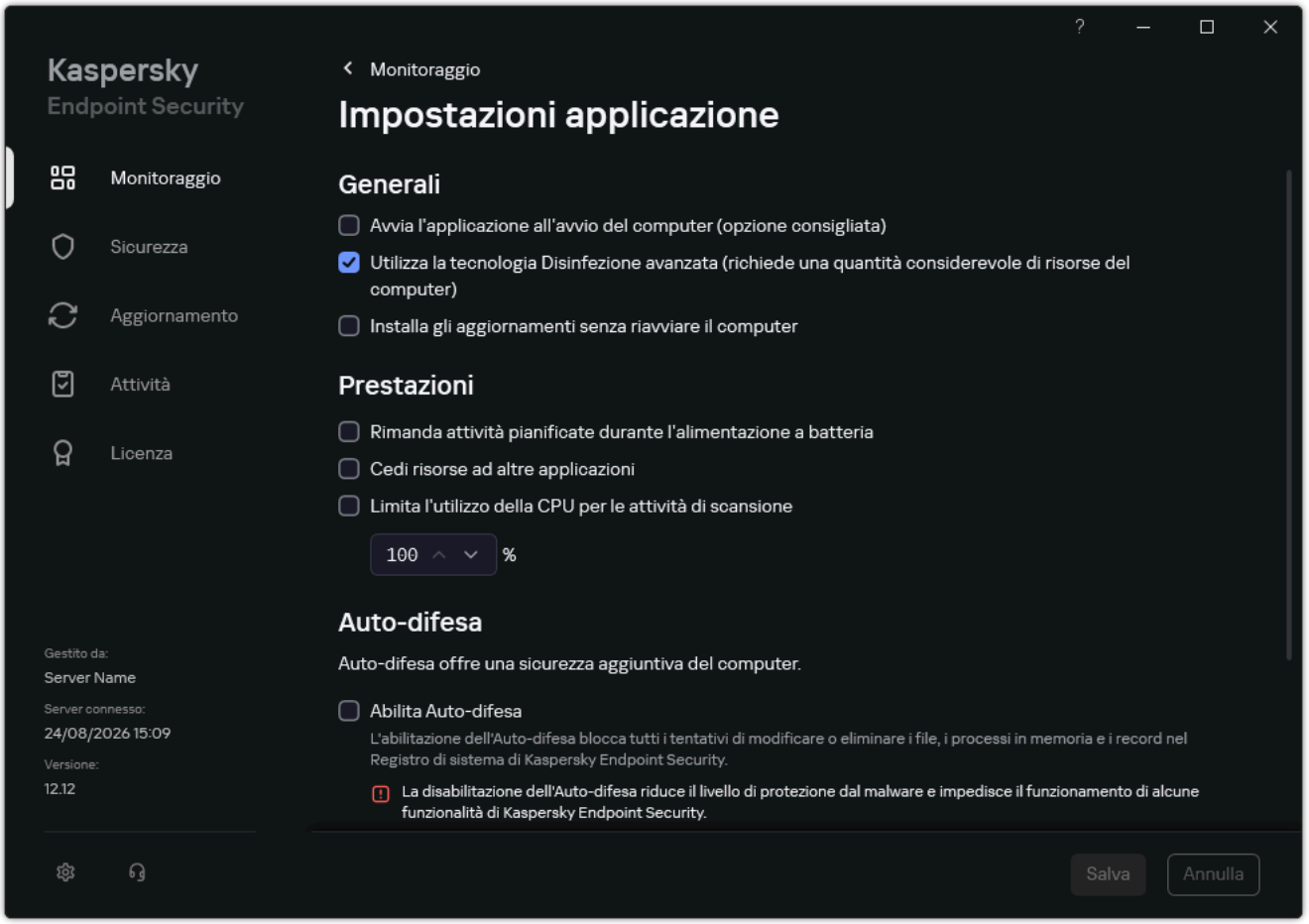
Come abilitare la protezione dei file di dump e dei file di traccia in Web Console e Cloud Console

1. Nella finestra principale di Web Console, fare clic su **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Verrà visualizzata la finestra delle proprietà del criterio.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali → Assistenza tecnica**.
5. Nella sezione **Informazioni di debug** utilizzare la casella di controllo **Protezione dei file di dump e traccia ABILITATA** per abilitare o disabilitare la protezione dei file.
6. Salvare le modifiche.

Come abilitare la protezione dei file di dump e dei file di traccia nell'interfaccia dell'applicazione

1. Nella finestra principale dell'applicazione, fare clic sul pulsante ⚙.
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.



Impostazioni di Kaspersky Endpoint Security for Windows

3. Nella sezione **Informazioni di debug** utilizzare la casella di controllo **Abilita protezione dei file di dump e di traccia** per abilitare o disabilitare la protezione dei file.
4. Salvare le modifiche.

I file di dump e di traccia di cui viene eseguita la scrittura mentre la protezione è attiva rimangono protetti anche dopo la disabilitazione di questa funzione.

Recupero dei dati del sistema operativo (Kaspersky Get System Info)

Dopo l'installazione dell'applicazione Kaspersky Endpoint Security, il sistema operativo o un'applicazione potrebbero non funzionare correttamente. È presente un conflitto tra l'applicazione e il software o i driver dei componenti del computer.

Per identificare la causa del problema, l'Assistenza tecnica Kaspersky richiede un rapporto dell'utilità Kaspersky Get System Info (di seguito denominata GSI). Per informazioni dettagliate sull'utilizzo dell'utilità, consultare la Knowledge Base di Kaspersky.

Limitazioni e avvisi

Kaspersky Endpoint Security presenta alcune limitazioni che non sono critiche per l'esecuzione dell'applicazione.

Installazione dell'applicazione

- Per informazioni dettagliate sul supporto per i sistemi operativi Microsoft Windows 10, Microsoft Windows Server 2016 e Microsoft Windows Server 2019, fare riferimento alla Knowledge Base dell'Assistenza tecnica.
- Per informazioni dettagliate sul supporto per i sistemi operativi Microsoft Windows 11 e Microsoft Windows Server 2022, consultare la Knowledge Base dell'Assistenza tecnica.
- Dopo essere stata installata in un computer infetto, l'applicazione non informa l'utente della necessità di eseguire una scansione del computer. Potrebbero verificarsi problemi durante l'attivazione dell'applicazione. Per risolvere questi problemi, avviare una Scansione delle aree critiche.
- Se vengono utilizzati caratteri non ASCII (ad esempio lettere russe) nei file setup.ini e setup.reg, è consigliabile modificare il file utilizzando notepad.exe e salvare il file con la codifica UTF-16LE. Non sono supportate altre codifiche.
- L'applicazione non supporta l'utilizzo di caratteri non ASCII quando si specifica il percorso di installazione dell'applicazione nelle impostazioni del pacchetto di installazione.
- Quando le impostazioni dell'applicazione vengono importate da un file CFG, il valore dell'impostazione che definisce la partecipazione a Kaspersky Security Network non viene applicato. Dopo l'importazione delle impostazioni, leggere il testo dell'Informativa di Kaspersky Security Network e confermare il proprio consenso a partecipare a Kaspersky Security Network. Il testo dell'Informativa è disponibile nell'interfaccia dell'applicazione o nel file ksn_*.txt che si trova nella cartella contenente il kit di distribuzione dell'applicazione.
- Se si desidera rimuovere e quindi reinstallare il criptaggio (FLE o FDE) o il componente Controllo dispositivi, è necessario riavviare il sistema prima della reinstallazione.
- Quando si utilizza il sistema operativo Microsoft Windows 10, è necessario riavviare il sistema dopo la rimozione del componente Criptaggio a livello di file (FLE, File Level Encryption).
- Quando si rimuovono componenti dell'applicazione singoli (ad esempio, utilizzando l'attività *Modifica i componenti dell'applicazione*), è possibile che sia necessario riavviare il computer.
- Nelle proprietà dell'attività *Modifica i componenti dell'applicazione*, quando si passa dalla modalità di installazione (**Modalità separata** / **Modalità combinata**), la sincronizzazione del set di componenti tra le modalità non è supportata. L'applicazione sincronizza il set di componenti tra le modalità dopo la riapertura delle proprietà dell'attività.
- L'installazione dell'applicazione potrebbe terminare con un errore in cui viene indicato che *Nel computer è installata un'applicazione il cui nome è mancante o illeggibile*. Ciò significa che nel computer rimangono applicazioni incompatibili o frammenti di esse. Per rimuovere elementi obsoleti di applicazioni incompatibili, inviare una richiesta con una descrizione dettagliata della situazione all'Assistenza tecnica di Kaspersky tramite Kaspersky CompanyAccount.
- Se è stata annullata la rimozione di Kaspersky Endpoint Security, avviare il ripristino dell'applicazione dopo aver riavviato il computer.

- L'applicazione richiede Microsoft .NET Framework 4.0 o versione successiva. Microsoft .NET Framework 4.6.1 presenta vulnerabilità. Se si utilizza Microsoft .NET Framework 4.6.1, è necessario installare gli aggiornamenti della protezione. Per i dettagli sugli aggiornamenti della protezione di Microsoft .NET Framework, fare riferimento al sito Web del servizio di assistenza tecnica di Microsoft.

- Se l'applicazione non viene installata correttamente con il componente Kaspersky Endpoint Agent selezionato in un sistema operativo del server e viene visualizzata la finestra *Errore di Windows Installer Coordinator*, fare riferimento alle istruzioni sul sito Web del supporto Microsoft.

- Se l'applicazione è stata installata localmente in modalità non interattiva, utilizzare il file setup.ini fornito per sostituire i componenti installati.

- Dopo l'installazione di Kaspersky Endpoint Security for Windows in alcune configurazioni di Windows 7, Windows Defender continua a funzionare. È consigliabile disabilitare manualmente Windows Defender per evitare di compromettere le prestazioni di sistema.

- Quando si installa Kaspersky Endpoint Security for Windows in un server su cui sono installate le applicazioni Kaspersky Security for Windows Server (KSWS) e Windows Defender, è necessario riavviare il sistema. È necessario riavviare il sistema anche se è stata abilitata l'installazione dell'applicazione senza il riavvio del sistema. Windows Defender per Windows Server è incluso nell'elenco del software non compatibile con Kaspersky Endpoint Security for Windows. Prima di installare l'applicazione, il programma di installazione rimuove Windows Defender per Windows Server. La rimozione del software incompatibile rende necessario il riavvio del sistema.

- Prima di installare Kaspersky Endpoint Security for Windows (KES) in un server su cui è installato Kaspersky Security for Windows Server (KSWS), è necessario disattivare KSWS Password Protection. Dopo la migrazione da KSWS a KES, abilitare la protezione tramite password nelle impostazioni dell'applicazione.

- Per installare l'applicazione su computer con Windows 7 o Windows Server 2008 R2 con il software Veeam Backup & Replication installato, potrebbe essere necessario riavviare il computer ed eseguire nuovamente l'installazione.

- La migrazione da Kaspersky Small Office Security (KSOS) a Kaspersky Endpoint Security (KES) con la funzionalità Protezione tramite password abilitata è disponibile a partire da KSOS build 21.16.*.*. Per eseguire la migrazione di versioni precedenti di KSOS, è necessario disabilitare Protezione tramite password o rimuovere manualmente KSOS. La migrazione da KSOS a KES con la funzionalità Protezione tramite password disabilitata viene eseguita correttamente.

- Non è possibile installare Kaspersky Endpoint Security in un'unità rimovibile di avvio. Durante l'installazione, Kaspersky Endpoint Security mostra un messaggio di errore: *È stata selezionata una cartella o un'unità non valida. L'applicazione deve essere installata in un'unità locale*. Se si riesce a installare l'applicazione in un'unità rimovibile utilizzando strumenti di terze parti, ciò potrebbe causare l'arresto anomalo del sistema operativo (BSOD) durante il processo di avvio. Questo significa che Kaspersky Endpoint Security non supporta Windows To Go e soluzioni simili. Per eseguire la scansione di un computer da un'unità rimovibile, è possibile utilizzare l'applicazione Kaspersky Rescue Disk in modo gratuito.

- L'installazione di Kaspersky Endpoint Security con i componenti di rete in un terminal server con sessioni RDP multiutente comporta alcune considerazioni particolari. I sistemi operativi forzano la terminazione di tutte le sessioni utente al termine della sessione Amministratore. Per connettersi al terminal server, è necessario riavviare il server o accedere al sistema in locale. Tale comportamento è dettato dalle peculiarità del funzionamento del sistema operativo Windows.

- Se i plug-in Web Kaspersky Endpoint Security for Windows (build 12.11.0.2004) e Kaspersky Endpoint Security for Linux (build 12.4.0.1354) sono installati in Kaspersky Security Center 16.0 o Kaspersky Security Center 16.1, l'aggiornamento del plug-in Web Kaspersky Endpoint Security for Windows alla versione 12.11.0.6004 potrebbe causare malfunzionamenti nei criteri di Kaspersky Endpoint Security for Linux.

  Possibile soluzione: passare alla finestra **Impostazioni** → **Plug-in Web** e rimuovere dall'elenco il plug-in Web Kaspersky Endpoint Security for Windows, il plug-in Web Kaspersky Endpoint Security for Linux e Unified Protection and Management Plug-in. Quindi installare prima il plug-in Web Kaspersky Endpoint Security for Linux, seguito dal plug-in Web Kaspersky Endpoint Security for Windows.

- In Web Console, l'elenco dei componenti viene visualizzato in modo errato nelle proprietà del pacchetto di installazione di Kaspersky Endpoint Security 12.11 for Windows. Un componente distinto, Anti-Cryptor, non è disponibile in questa versione dell'applicazione. La protezione delle cartelle condivise dalla funzionalità di criptaggio esterno è inclusa nel componente Rilevamento del Comportamento. In Kaspersky Endpoint Security 12.12 for Windows, questa funzionalità è un componente distinto. Allo stesso tempo, in Administration Console (MMC), l'elenco dei componenti viene visualizzato correttamente.

- Quando si utilizza il plug-in Web versione 7.0 o successiva, l'elenco dei componenti selezionati per l'installazione per impostazione predefinita viene visualizzato in modo errato nelle proprietà del pacchetto di installazione per Kaspersky Endpoint Security 14.1 e versioni precedenti. Se questo elenco non viene modificato durante la creazione del pacchetto di installazione, l'applicazione verrà installata con il set predefinito di componenti specificato per la versione corrispondente dell'applicazione.

Upgrade dell'applicazione

- A partire dalla versione dell'applicazione 11.0.0, è possibile installare il plug-in Kaspersky Endpoint Security for Windows MMC sulla versione precedente del plug-in. Per tornare a una versione precedente del plug-in, eliminare il plug-in corrente e installare una versione precedente del plug-in.

- Quando si esegue l'upgrade di Kaspersky Endpoint Security 11.0.0 o 11.0.1 for Windows, le impostazioni di pianificazione delle attività locali per le attività *Aggiornamento di database e moduli dell'applicazione*, *Scansione delle aree critiche*, *Scansione personalizzata* e *Controllo integrità applicazione* non vengono salvate.

- Nei computer che eseguono Windows 10 versione 1903 e 1909, gli upgrade da Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (build 10.3.3.275), Service Pack 2 Maintenance Release 4 (build 10.3.3.304), 11.0.0 e 11.0.1 con il componente Criptaggio a livello di file installato potrebbe terminare con un errore. Questo avviene perché il criptaggio dei file non è supportato per queste versioni di Kaspersky Endpoint Security for Windows in Windows 10 versione 1903 e 1909. Prima di installare questo upgrade, è consigliabile rimuovere il componente di criptaggio dei file.

- L'applicazione richiede Microsoft .NET Framework 4.0 o versione successiva. Microsoft .NET Framework 4.6.1 presenta vulnerabilità. Se si utilizza Microsoft .NET Framework 4.6.1, è necessario installare gli aggiornamenti della protezione. Per i dettagli sugli aggiornamenti della protezione di Microsoft .NET Framework, fare riferimento al sito Web del servizio di assistenza tecnica di Microsoft.

- Quando si esegue l'upgrade di Kaspersky Endpoint Security, l'applicazione disabilita l'uso di KSN finché non si accetta l'Informativa di Kaspersky Security Network. Inoltre, lo stato del computer può essere modificato in *Critico* in Kaspersky Security Center; a questo punto, si riceve l'evento *Server KSN non disponibili*. Se si utilizza Kaspersky Managed Detection and Response, si riceveranno eventi sulle violazioni nell'esecuzione della soluzione. L'uso di KSN è necessario per il funzionamento di Kaspersky Managed Detection and Response. Kaspersky Endpoint Security consente l'uso di KSN dopo aver applicato il criterio in cui l'amministratore accetta le condizioni per l'utilizzo di KSN. Una volta accettata l'Informativa di Kaspersky Security Network, l'esecuzione di Kaspersky Endpoint Security riprende.

- Dopo l'upgrade di Kaspersky Endpoint Security alla versione 11.10.0 o successiva senza un riavvio, nel computer verranno installate due applicazioni Kaspersky Endpoint Security. Non rimuovere manualmente la versione precedente dell'applicazione. La versione precedente verrà rimossa automaticamente al riavvio del computer.

- Dopo aver aggiornato Kaspersky Endpoint Security in un computer in cui viene eseguito Microsoft Windows 11, il menu contestuale del file potrebbe mostrare elementi sia per le versioni precedenti che per quelle nuove dell'applicazione. Riavviare il computer due volte per assicurare il corretto funzionamento del menu contestuale del file.

- Se la funzionalità Auto-difesa dell'applicazione è disattivata e tutte le schede di rete vengono arrestate, i componenti di rete dell'applicazione non funzioneranno tra la fine dell'aggiornamento dell'applicazione e il riavvio del computer. I componenti di rete dell'applicazione includono Protezione minacce Web, Protezione minacce di posta, Protezione minacce di rete, Firewall, Prevenzione Intrusioni Host e Controllo Web. Riavviare il computer affinché l'applicazione funzioni correttamente.

- Il componente Prevenzione Attacchi BadUSB non funziona tra la fine dell'aggiornamento dell'applicazione e il riavvio del computer. Riavviare il computer affinché l'applicazione funzioni correttamente.

- Non è possibile eseguire l'upgrade dell'applicazione se il processo di aggiornamento precedente non è stato completato. Riavviare il computer affinché l'applicazione funzioni correttamente.

- Dopo l'upgrade dell'applicazione dalle versioni precedenti a Kaspersky Endpoint Security 11 for Windows, il computer deve essere riavviato.

- Se si gestisce Kaspersky Endpoint Security con Kaspersky Security Center Cloud Console, l'aggiornamento dell'applicazione in locale non è consentito. Quando si aggiorna l'applicazione in locale, non è possibile accettare il Contratto per il trattamento dei dati di Kaspersky Security Center Cloud Console.

Supporto per l'architettura Arm

- L'installazione di Kaspersky Endpoint Security in modalità Light Agent in macchine virtuali basate su Arm non è supportata.

- Criptaggio disco Kaspersky non è supportato nei computer basati su Arm.

- Il criptaggio dei file non è supportato nei computer basati su Arm.

- Il criptaggio delle unità rimovibili non è supportato nei computer basati su Arm.

- Nei computer in cui viene eseguito Windows 11 for Arm64, EDR Agent non è compatibile con Bitdefender Endpoint Security Tools.

- La funzionalità di protezione del segnale audio e la funzionalità di protezione dell'accesso alla webcam non è supportata nei computer basati su Arm.

- Nei computer basati su Arm l'estensione Protezione minacce di posta supporta le versioni a 32 bit e a 64 bit di Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 per Arm64.

- Kaspersky Endpoint Security non invia oggetti destinati all'architettura Arm a Kaspersky Sandbox.

- Il controllo di stampa non è supportato nei computer basati su Arm.

- Nei computer basati su Arm, l'attività *Scansione IOC* supporta i file e-mail solo dai seguenti client di posta: versioni a 32 e 64 bit di Outlook 2016 e Outlook 2021, 2024 e 365 per Arm64.

- Nei computer con Windows 11 per Arm64, l'autenticazione basata su token potrebbe non essere disponibile perché il sistema operativo non è in grado di rilevare un certificato valido nel token. Questo comportamento è causato dal modo in cui il sistema operativo interagisce con il software del token. Ad esempio, il sistema operativo potrebbe non disporre dei driver necessari per il funzionamento del token. In questo caso, Kaspersky Endpoint Security non supporta neanche l'autenticazione basata su token (Protezione tramite password). È possibile utilizzare altri metodi di autenticazione, ad esempio le credenziali utente.

Supporto per le piattaforme server

- Nei server con *deduplicazione dei dati* abilitata, è necessario aggiungere il file fsdmhost.exe nell'elenco delle applicazioni attendibili. Questo aiuta a ottimizzare le prestazioni dell'applicazione e prevenire un carico eccessivo sulla CPU.

- Il file system ReFS è supportato con limitazioni:

  - Kaspersky Endpoint Security potrebbe elaborare gli eventi di disinfezione delle minacce in modo errato. Ad esempio, se l'applicazione ha eliminato un file dannoso, il rapporto potrebbe contenere una voce Oggetto non elaborato. Allo stesso tempo, Kaspersky Endpoint Security disinfetta le minacce in base alle impostazioni dell'applicazione. Kaspersky Endpoint Security può anche creare un duplicato dell'evento *Oggetto da disinfettare al riavvio* per lo stesso oggetto.

  - Protezione minacce file può ignorare alcune minacce. Allo stesso tempo, Scansione malware funziona correttamente.

  - Dopo l'avvio dell'attività *Scansione malware*, le esclusioni dalla scansione aggiunte con iChecker vengono reimpostate al riavvio del server.

  - La tecnologia iSwift non è supportata. Kaspersky Endpoint Security non considera le esclusioni dalla scansione aggiunte utilizzando la tecnologia iSwift.

  - Kaspersky Endpoint Security non rileva i file eicar.com e susp-eicar.com se nel computer era presente il file meicar.exe prima dell'installazione di Kaspersky Endpoint Security.

  - Kaspersky Endpoint Security potrebbe mostrare in modo errato le notifiche di disinfezione delle minacce. Ad esempio, l'applicazione può mostrare una notifica di minaccia per una minaccia precedentemente disinfettata.

- Le tecnologie Criptaggio a livello di file e Criptaggio disco Kaspersky non sono supportate nelle piattaforme server. Allo stesso tempo, Kaspersky Endpoint Security potrebbe elaborare in modo errato gli eventi di criptaggio dei dati.

- Nei sistemi operativi del server non viene visualizzato alcun avviso relativo alla necessità di una disinfezione avanzata.

- Microsoft Windows Server 2008 è stato escluso dal supporto. L'installazione dell'applicazione in un computer con sistema operativo Microsoft Windows Server 2008 non è supportata.

- Kaspersky Endpoint Security installato in un server con Microsoft Data Protection Manager (DPM) distribuito può causare il malfunzionamento di DPM. È correlato alle limitazioni nell'operazione DPM. Per eliminare i malfunzionamenti, è necessario aggiungere le unità del server locale alle esclusioni per il componente Protezione minacce file e le attività *Scansione malware*.

- La modalità Server Core è supportata con limitazioni:

  - L'interfaccia utente grafica locale non è disponibile, incluse le notifiche, le notifiche pop-up e altri comandi dell'interfaccia. L'applicazione non può mostrare le finestre delle richieste, incluse le seguenti finestre:

    - richiesta di conferma dell'upgrade dei moduli e versione dell'applicazione;

    - richiesta di riavvio del computer;

- richiesta delle credenziali di autenticazione sul server proxy;
- Richiesta di accesso a un dispositivo (Controllo dispositivi).

- I seguenti componenti non sono disponibili: Protezione minacce Web, Protezione minacce di posta, Controllo Web, Prevenzione Attacchi BadUSB.
- Anti-Bridging non è disponibile.
- È possibile accettare l'Informativa di Kaspersky Security Network solo nel criterio dell'applicazione in Kaspersky Security Center Console.
- Crittografia unità BitLocker è disponibile solo con un Trusted Platform Module (TPM). Non è possibile utilizzare un PIN/password per il criptaggio, poiché l'applicazione non è in grado di mostrare la finestra di richiesta della password per l'autenticazione di preavvio. Se nel sistema operativo è abilitata la modalità di compatibilità FIPS (Federal Information Processing Standard), collegare un'unità rimovibile per il salvataggio della chiave di crittografia prima di avviare il criptaggio dell'unità.

Supporto per le piattaforme virtuali

- Il Criptaggio dell'intero disco (FDE) sulle macchine virtuali Hyper-V non è supportato.
- Il Criptaggio dell'intero disco (FDE) sulle piattaforme virtuali Citrix non è supportato.
- I sistemi operativi Windows 10 Enterprise multisessione e Windows 11 Enterprise multisessione sono supportati con limitazioni:
  - Kaspersky Endpoint Security disinfetta le minacce attive senza avvisare l'utente, proprio come quando vengono disinfettate le minacce attive nei server. Poiché il sistema operativo continua a essere eseguito in modalità multisessione, altri utenti attivi potrebbero perdere i dati se la minaccia non viene risolta immediatamente.
  - Il Criptaggio dell'intero disco (FDE) non è supportato.
  - La gestione di BitLocker non è supportata.
  - L'utilizzo di Kaspersky Endpoint Security con unità rimovibili non è supportato. L'infrastruttura di Microsoft Azure definisce le unità rimovibili come unità di rete.
- L'installazione e l'utilizzo del Criptaggio a livello di file (FLE) sulle piattaforme virtuali Citrix non sono supportati.
- Per supportare la compatibilità di Kaspersky Endpoint Security for Windows con Citrix PVS, eseguire l'installazione con l'opzione **Garantisci la compatibilità con Citrix PVS** abilitata. Questa opzione può essere abilitata nell'Installazione guidata o utilizzando il parametro della riga di comando `/pCITRIXCOMPATIBILITY=1`. In caso di installazione remota, il file KUD deve essere modificato aggiungendo il seguente parametro: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Prima di iniziare la clonazione, è necessario disabilitare Auto-difesa per clonare le macchine virtuali che utilizzano vDisk.

- Quando si prepara una macchina modello per l'immagine master Citrix XenDesktop con Kaspersky Endpoint Security for Windows e Kaspersky Security Center Network Agent preinstallati, aggiungere i seguenti tipi di esclusioni al file di configurazione:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Per informazioni dettagliate su Citrix XenDesktop, visitare il sito Web del supporto Citrix.

- In alcuni casi, un tentativo di scollegare in modo sicuro un'unità rimovibile potrebbe non andare a buon fine su una macchina virtuale distribuita in un hypervisor VMware ESXi. Tentare di scollegare nuovamente il dispositivo in modo sicuro.

- Kaspersky Endpoint Security è compatibile con l'hypervisor VMware ESXi con le seguenti limitazioni:

  - Kaspersky Endpoint Security potrebbe essere incompatibile con i driver di Guest Introspection (vnetWFP.sys, vnetFLT.sys e altri). Per risolvere l'incompatibilità, aggiornare i driver alla versione più recente o disinstallare i driver.

  - In alcuni casi, il tentativo di rimuovere in modo sicuro un disco rimovibile in una macchina virtuale potrebbe non riuscire. Tentare di scollegare nuovamente il dispositivo in modo sicuro.

- L'installazione di Kaspersky Endpoint Security nelle macchine virtuali con l'agente Citrix VDA potrebbe interrompersi con un errore di compatibilità. Ciò accade perché Citrix Provisioning Services ha una compatibilità limitata con le soluzioni anti-virus. Per le best practice sull'utilizzo delle soluzioni anti-virus con Citrix Provisioning Services, fare riferimento al sito Web di assistenza di Citrix.

- Kaspersky Endpoint Security ignora la scansione di un'unità rimovibile se l'unità è connessa a una macchina virtuale nell'hypervisor Citrix (l'attività *Scansione unità rimovibili*). In tali dispositivi, il sistema operativo rileva l'unità rimovibile connessa come unità di rete. In questi casi, è possibile utilizzare l'attività *Scansione personalizzata*. Il comportamento dell'applicazione in modalità standard e in modalità Light Agent è lo stesso.

- Se Kaspersky Endpoint Security è installato in una macchina virtuale in un'infrastruttura che utilizza la tecnologia Citrix App Layering, i file rilevati dall'applicazione come infetti con lo stato *Oggetto da eliminare al riavvio* non verranno rimossi automaticamente quando la macchina virtuale viene riavviata.

  Per eliminare tali file, è necessario montare il file VHDX contenente User Layer nel computer dell'amministratore di Citrix App Layering ed eseguire una scansione malware sul disco montato.

- Prima di creare uno snapshot dell'Immagine gold di una macchina virtuale con Kaspersky Endpoint Security installato, è consigliabile arrestare la macchina virtuale e creare uno snapshot "a freddo". Se si crea uno snapshot mentre la macchina virtuale è in esecuzione (uno snapshot "a caldo"), il corretto funzionamento dell'applicazione non è garantito.

Compatibilità con Kaspersky Security Center

- In Kaspersky Security Center Web Console versione 14.1 e precedenti, i nomi delle aree funzionali per i componenti Log Inspection e Monitoraggio integrità file non sono visualizzati correttamente nella sezione delle impostazioni delle autorizzazioni di accesso utente delle proprietà dell'Administration Server.

- Dopo aver riparato l'applicazione, la protezione della connessione del computer ad Administration Server viene disattivata. Dopo aver riparato l'applicazione, eseguire di nuovo l'attività *Protezione della connessione ad Administration Server*.

- In Kaspersky Security Center Administration Console, la finestra **Selezionare un utente o un gruppo di utenti** mostra solo i primi 50.000 utenti dall'elenco di utenti di Kaspersky Security Center. Vedere la Guida di Kaspersky Security Center per maggiori dettagli.

- Durante la ricerca di dispositivi gestiti Kaspersky Security Center Administration Console, la scheda **Componenti dell'applicazione** può mostrare contemporaneamente più varianti del nome dello stesso componente dell'applicazione, inclusi i nomi corrispondenti a versioni precedenti di Kaspersky Endpoint Security. È inoltre possibile che i nomi di alcuni componenti siano duplicati.

  Per eseguire una ricerca per componente, è sufficiente selezionare una delle varianti visualizzate. Per ulteriori dettagli sul rilevamento dei dispositivi, consultare la Guida di Kaspersky Security Center.

- In Kaspersky Security Center Web Console 15.1 Update 2, con il plug-in Web di Kaspersky Endpoint Security for Windows versione 12.11 o successiva e Unified Protection and Management Plug-in installati, le condizioni di attivazione del profilo per il criterio non funzionano. Kaspersky Security Center non aggiunge alla console i nuovi dispositivi che soddisfano le condizioni di attivazione del profilo.

Gestione delle licenze

- Se viene visualizzato il messaggio di sistema *Errore durante la ricezione dei dati*, verificare che il computer nel quale si sta eseguendo l'attivazione disponga dell'accesso alla rete o configurare le impostazioni di attivazione tramite Kaspersky Security Center Activation Proxy.

- Nell'interfaccia dell'applicazione la data di scadenza della licenza viene visualizzata nell'ora locale del computer.

- L'installazione dell'applicazione con un file chiave integrato in un computer con accesso a Internet instabile può causare la visualizzazione temporanea di eventi che indicano che l'applicazione non è attivata o che la licenza non consente il funzionamento del componente. Ciò è causato dal fatto che durante il processo di installazione l'applicazione attiva prima la licenza di prova integrata. Richiede l'accesso a Internet.

- Durante il periodo di prova, l'installazione di qualsiasi upgrade o patch dell'applicazione in un computer con accesso a Internet instabile può causare la visualizzazione temporanea di eventi che indicano che l'applicazione non è attivata. Ciò è causato dal fatto che durante il processo di installazione dell'aggiornamento l'applicazione attiva prima la licenza di prova integrata. Richiede l'accesso a Internet.

- Se la licenza di prova è stata attivata automaticamente durante l'installazione dell'applicazione e quindi l'applicazione è stata rimossa senza salvare le informazioni sulla licenza, l'applicazione non verrà automaticamente attivata con la licenza di prova in caso di reinstallazione. In questo caso, attivare manualmente l'applicazione.

- Se si utilizza Kaspersky Security Center versione 11 e Kaspersky Endpoint Security versione 14.2, i rapporti sulle prestazioni dei componenti potrebbero non funzionare correttamente. Se sono stati installati componenti di Kaspersky Endpoint Security non inclusi nella licenza, Network Agent può inviare errori relativi allo stato dei componenti al registro eventi di Windows. Per evitare errori, rimuovere i componenti non inclusi nella licenza.

Protezione minacce di posta

- Quando si esegue la scansione delle e-mail con l'estensione Protezione minacce di posta per Microsoft Outlook, è consigliabile utilizzare la modalità cache di Exchange Server (Use Cached Exchange Mode).

- Kaspersky Endpoint Security non supporta la versione a 64 bit del client di posta Microsoft Outlook. Di conseguenza, Kaspersky Endpoint Security non esegue la scansione dei file Microsoft Outlook (file PST e OST) se nel computer è installata una versione a 64 bit di Microsoft Outlook, anche se la posta è inclusa nell'ambito della scansione.

- Kaspersky Endpoint Security non supporta il client di posta Microsoft Outlook New.

- Se è stata disabilitata la disinfezione delle minacce rilevate da Protezione minacce di posta ed è stata ricevuta un'e-mail infetta nella cassetta postale di Outlook, Protezione minacce Web potrebbe bloccare la comunicazione con il server Exchange tramite MAPI. Protezione minacce Web genera quindi un evento di rilevamento delle minacce e lo invia a Kaspersky Security Center. Per ripristinare la connessione tra il computer e il server Exchange, è necessario eliminare manualmente l'e-mail infetta dalla cassetta postale di Outlook.

  Quando si aggiorna la versione dell'applicazione senza riavviare il computer, il livello di protezione di Protezione minacce di posta si riduce temporaneamente (per un massimo di un minuto). Se si riceve un'e-mail infetta nella cassetta postale di Outlook durante l'aggiornamento dell'applicazione, Protezione minacce Web blocca anche la connessione al server Exchange tramite MAPI. Per ripristinare la connessione, eliminare l'e-mail infetta dalla cassetta postale di Outlook.

Motore di Remediation

- L'applicazione ripristina i file solo nei dispositivi con file system NTFS o FAT32.
- L'applicazione ripristina i file di dimensioni massime di 100 MB.
- L'applicazione può ripristinare i file con le seguenti estensioni: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Non è possibile ripristinare i file che risiedono nelle unità di rete o in dischi CD/DVD riscrivibili.
- Non è possibile ripristinare i file criptati con EFS (Encryption File System) Per ulteriori informazioni sul funzionamento di EFS, visitare il sito Web Microsoft.
- L'applicazione non monitora le modifiche dei file eseguite da processi al livello del kernel del sistema operativo.

Firewall

- Se una regola per i pacchetti di rete o una regola di rete dell'applicazione specifica nomi DNS, Kaspersky Endpoint Security può inviare richieste al server DNS per determinare gli indirizzi IP di queste risorse. Il firewall utilizza gli indirizzi IP per monitorare le attività di rete. Pertanto l'applicazione risolve i nomi DNS in indirizzi IP. Si consiglia di utilizzare i nomi DNS solo per computer LAN o servizi interni.
- Per specificare una regola per tutti gli indirizzi IPv6, aggiungere l'intervallo di indirizzi ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Firewall non supporta la maschera ::/0.
- Il filtro di pacchetti o connessioni per indirizzo locale, interfaccia fisica e TTL (Time-To-Live) del pacchetto è supportato nei seguenti casi:
  - I base all'indirizzo locale per le connessioni o i pacchetti in uscita nelle regole dell'applicazione per regole per i pacchetti, TCP e UDP.
  - In base all'indirizzo locale per le connessioni o i pacchetti in entrata (eccetto UDP) nelle regole di blocco dell'applicazione e nelle regole per i pacchetti.
  - In base al TTL dei pacchetti nelle regole per il blocco dei pacchetti per i pacchetti in entrata o in uscita.
  - Tramite l'interfaccia di rete per le connessioni o i pacchetti in entrata e in uscita nelle regole dei pacchetti.

- Se è stata eseguita la configurazione di una scheda di rete o di un Time to live (TTL) per i pacchetti per una regola di permesso per i pacchetti, la priorità di questa regola è inferiore rispetto a quella di una regola di blocco dell'applicazione. In altre parole, se l'attività di rete è bloccata per un'applicazione (ad esempio, l'applicazione si trova nel gruppo di attendibilità *Restrizione alta*), non è possibile consentire l'attività di rete dell'applicazione utilizzando una regola per i pacchetti con queste impostazioni. In tutti gli altri casi, la priorità di una regola per i pacchetti è superiore rispetto a quella di una regola di rete dell'applicazione.

- Quando si importano le regole per i pacchetti firewall, Kaspersky Endpoint Security può modificare i nomi delle regole. L'applicazione determina le regole con set identici di parametri generali: protocollo, direzione, porte remote e locali, TTL (Packet Time-to-Live). Se questo set di parametri generali è identico per più regole, l'applicazione assegna lo stesso nome a queste regole o aggiunge un tag del parametro al nome. In questo modo, Kaspersky Endpoint Security importa tutte le regole dei pacchetti, tuttavia il nome delle regole che hanno impostazioni generali identiche può essere modificato.

- Se è stata abilitata la generazione dei rapporti sugli eventi dell'applicazione in una regola di rete, lo spostamento dell'applicazione in un altro gruppo di attendibilità implica che le restrizioni di tale gruppo di attendibilità non verranno applicate. Pertanto, se l'applicazione è nel gruppo di attendibilità Attendibili, non sarà soggetta a restrizioni di rete. Successivamente è stata abilitata la generazione dei rapporti sugli eventi per questa applicazione ed è stata spostata nel gruppo di attendibilità *Non attendibili*. Il firewall non applicherà le restrizioni di rete per questa applicazione. Si consiglia di spostare prima l'applicazione nel gruppo di attendibilità appropriato e quindi di abilitare la generazione di rapporti sugli eventi. Se questo metodo non è applicabile, è possibile configurare manualmente le restrizioni per l'applicazione nelle impostazioni della regola di rete. La restrizione viene applicata solo all'interfaccia locale dell'applicazione. Lo spostamento dell'applicazione tra i gruppi di attendibilità nel criterio funziona correttamente.

- I componenti Firewall e Prevenzione Intrusioni condividono impostazioni comuni: diritti dell'applicazione e risorse protette. Se si modificano tali impostazioni per Firewall, Kaspersky Endpoint Security applica automaticamente le nuove impostazioni a Prevenzione Intrusioni. Se, ad esempio, sono state consentite le modifiche alle impostazioni generali del criterio Firewall (il lucchetto è aperto), sarà possibile modificare anche le impostazioni di Prevenzione Intrusioni.

- Quando si attiva una regola per i pacchetti di rete in Kaspersky Endpoint Security 11.6.0 o versioni precedenti, la colonna **Nome applicazione** nel rapporto Firewall mostrerà sempre il valore *Kaspersky Endpoint Security*. Inoltre, il Firewall bloccherà la connessione a livello di pacchetti per tutte le applicazioni. Questo comportamento è stato modificato per Kaspersky Endpoint Security 11.7.0 o versioni successive. Nel rapporto Firewall, è stata aggiunta la colonna **Tipo di regola**. Quando si attiva una regola per i pacchetti di rete, il valore nella colonna **Nome applicazione** resta vuoto.

- Se è stata vietata qualsiasi attività di rete tramite Firewall, il componente Protezione minacce di rete potrebbe rilevare un attacco di tipo Scansione porte. Questo può accadere perché l'applicazione avvia Protezione minacce di rete prima di Firewall per rilevare attività sospette nella rete.

Prevenzione Attacchi BadUSB

- Kaspersky Endpoint Security reimposta il timeout del blocco del dispositivo USB quando il computer è bloccato (ad esempio, quando è trascorso il timeout del blocco dello schermo). In altre parole, se si immette un codice di autorizzazione del dispositivo USB più volte e l'applicazione blocca il dispositivo USB, Kaspersky Endpoint Security consente di ripetere il tentativo di autorizzazione dopo aver sbloccato il computer. In questo caso, Kaspersky Endpoint Security non blocca il dispositivo USB per un periodo di tempo specificato nelle impostazioni del componente Prevenzione Attacchi BadUSB.

- Kaspersky Endpoint Security reimposta il timeout di blocco del dispositivo USB quando la protezione del computer è sospesa. In altre parole, se si immette un codice di autorizzazione del dispositivo USB più volte e l'applicazione blocca il dispositivo USB, Kaspersky Endpoint Security consente di ripetere il tentativo di autorizzazione dopo aver ripristinato la protezione del computer. In questo caso, Kaspersky Endpoint Security non blocca il dispositivo USB per un periodo di tempo specificato nelle impostazioni del componente Prevenzione Attacchi BadUSB.

Kaspersky Security Network

- Kaspersky Endpoint Security non supporta HTTPS durante la connessione al proxy KSN (casella di controllo **Usa HTTPS** selezionata nelle impostazioni di connessione del proxy KSN) se l'indirizzo del server include lettere non latine (simboli non ASCII).

- In Kaspersky Security Center, quando si passa dall'utilizzo di Kaspersky Security Network globale all'utilizzo di Kaspersky Security Network (KPSN) privato o viceversa, l'opzione per partecipare a Kaspersky Security Network è disabilitata nel criterio del prodotto specifico. Dopo il passaggio, leggere attentamente il testo dell'Informativa di Kaspersky Security Network e confermare il consenso a partecipare a KSN. È possibile leggere il testo dell'Informativa nell'interfaccia dell'applicazione o durante la modifica del criterio del prodotto.

- A partire da Kaspersky Endpoint Security 12.9 for Windows, quando si passa da KPSN a KSN globale, è necessario confermare nuovamente l'accettazione dell'Informativa di Kaspersky Security Network. A tale scopo, è necessario abilitare l'utilizzo di Kaspersky Security Network nelle proprietà del criterio o nell'interfaccia dell'applicazione e confermare l'accettazione dell'Informativa di Kaspersky Security Network. Se si è già utilizzato il KSN globale, è necessario prima disabilitare l'utilizzo di KSN, quindi riabilitarlo e confermare l'accettazione dell'Informativa di Kaspersky Security Network. Se non si accetta l'Informativa di Kaspersky Security Network, l'applicazione non sarà in grado di accedere ai dati di Kaspersky Security Network.

- Kaspersky Endpoint Security non invia file di testo (ad esempio, file TXT, CSV, LOG e DOCX senza macro) a Kaspersky Security Network per la scansione. L'applicazione invia i file che possono rappresentare una minaccia per KSN per la scansione. Questi file includono file eseguibili o file che possono contenere codice eseguibile (ad esempio le macro nei file DOCX). Altri componenti dell'applicazione sono responsabili della scansione dei file di testo. È inoltre possibile controllare manualmente la reputazione di un file di testo dal menu di scelta rapida del file. Se un file di testo ha una reputazione *Non attendibile (Kaspersky Security Network)*, l'applicazione ignora l'azione definita per le minacce rilevate.

Controllo applicazioni

- Quando si utilizzano le regole di Controllo applicazioni, non è consigliabile aggiungere più di 100.000 condizioni di inclusione ed esclusione totali per le applicazioni di diverse categorie, a condizione che Kaspersky Endpoint Security sia in esecuzione in un computer che soddisfa i requisiti hardware minimi e funzioni su Microsoft Windows 10.

- Sono supportati solo gli archivi in formato ZIP quando si utilizzano le regole di Controllo applicazioni in Kaspersky Security Center Web Console. Gli archivi in altri formati, come RAR o 7z, non sono supportati. Non esiste tale restrizione se si utilizzano le regole di Controllo applicazioni in Administration Console (MMC).

- Quando si utilizzano le regole di Controllo applicazioni in Kaspersky Security Center Web Console, la dimensione massima supportata di un file caricato è 104 MB. Non esiste tale restrizione se si utilizzano le regole di Controllo applicazioni in Administration Console (MMC).

- Quando si utilizza Microsoft Windows 10 nella modalità Lista vietati delle applicazioni, le regole di blocco potrebbero essere applicate in modo errato, il che potrebbe causare il blocco delle applicazioni non specificate nelle regole.

- Se sono state aggiunte nuove *regole di Controllo Applicazioni predefinite* durante l'upgrade di Kaspersky Endpoint Security, non è possibile applicare queste regole alle versioni precedenti dell'applicazione.

- Quando le app Web progressive (PWA, Progressive Web App) vengono bloccate dal componente Controllo applicazioni, appManifest.xml viene indicato come app bloccata nel rapporto.

- Quando si aggiunge l'applicazione Blocco note standard a una regola di Controllo applicazioni per Windows 11, si sconsiglia di specificare il percorso dell'applicazione. Nei computer in cui viene eseguito Windows 11, il sistema operativo utilizza Metro Notepad situato nella cartella `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. Nelle versioni precedenti del sistema operativo, Blocco note si trova nelle seguenti cartelle:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  Quando si aggiunge Blocco note a una regola di Controllo applicazioni, è possibile specificare il nome dell'applicazione e l'hash del file dalle proprietà dell'applicazione in esecuzione, ad esempio.

- Quando si migra il criterio KSWS al profilo criterio KES, la Conversione guidata di criteri e attività in batch (Migrazione guidata) rinomina le categorie di applicazioni se i nomi delle categorie contengono caratteri non consentiti: `'` `*` `<` `>` `?` `\` `:` `|`. La Migrazione guidata sostituisce questi caratteri con i caratteri `_`. Ad esempio, la categoria di applicazioni `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` viene rinominata in `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Controllo dispositivi

- Kaspersky Endpoint Security può registrare gli eventi di connessione e disconnessione dei dispositivi esterni. I servizi Windows utilizzano l'account utente di sistema per connettere o disconnettere i dispositivi. Questo rende impossibile sapere quale utente sta connettendo o disconnettendo il dispositivo. Kaspersky Endpoint Security specifica l'account utente SYSTEM nell'evento.

- L'accesso ai dispositivi Stampante aggiunti all'elenco dei dispositivi attendibili è bloccato dalle regole di blocco dei dispositivi e dei bus.

- Per i dispositivi MTP il controllo delle operazioni di Lettura, Scrittura e Connessione è supportato se si utilizzano i driver Microsoft integrati del sistema operativo. Se un utente installa un driver personalizzato per utilizzare un dispositivo (ad esempio nell'ambito di iTunes o Android Debug Bridge), il controllo delle operazioni di Lettura e Scrittura potrebbe non funzionare.

- Quando si utilizzano i dispositivi MTP, le regole di accesso vengono modificate dopo aver riconnesso il dispositivo.

- Il componente Controllo dispositivi registra gli eventi relativi ai dispositivi monitorati, come la connessione e la disconnessione di un dispositivo, la lettura di un file da un dispositivo, la scrittura di un file su un dispositivo e altri eventi. Kaspersky Endpoint Security registra gli eventi di disconnessione solo per i seguenti tipi di dispositivi: Dispositivi portatili (MTP), Unità rimovibili, Dischi floppy, Unità CD/DVD. Per gli altri tipi di dispositivi, l'applicazione non registra gli eventi di disconnessione. L'applicazione registra l'operazione di connessione di un dispositivo a un computer per tutti i tipi di dispositivi.

- Se si aggiunge un dispositivo all'elenco dei dispositivi attendibili in base a una maschera del modello e si utilizzano caratteri inclusi nell'ID ma non nel nome del modello, questi dispositivi non vengono aggiunti. In una workstation questi dispositivi verranno aggiunti all'elenco dei dispositivi attendibili in base a una maschera ID.

- Quando l'applicazione viene aggiornata senza riavviare il computer, Controllo dispositivi non applica le regole di accesso ai dispositivi che vengono ricollegati. Tuttavia, se il dispositivo era connesso prima dell'aggiornamento, Controllo dispositivi applica le regole correttamente. Riavviare il computer affinché l'applicazione funzioni correttamente con i dispositivi ricollegati.

- Nei computer in cui è installato Kaspersky Endpoint Security versione 12.0, la modalità di accesso alla stampante **Consenti e non registrare** per il tipo di dispositivo **Stampanti di rete** è definita **Dipende dal bus di connessione**, se il criterio di Kaspersky Endpoint Security versione 12.1 viene applicato al computer. In queste modalità, l'applicazione esegue le stesse azioni. In Kaspersky Endpoint Security versione 12.1, la modalità di accesso per le stampanti di rete è denominata correttamente **Consenti e non registrare**.

- A partire da Kaspersky Endpoint Security 12.0 for Windows, l'applicazione consente di configurare le regole di stampa per le stampanti (controllo della stampa). Dopo aver installato l'applicazione con controllo della stampa o aver eseguito l'upgrade dell'applicazione a una versione con controllo della stampa, è necessario riavviare il computer. Fino al riavvio del computer, Kaspersky Endpoint Security non applica le regole di stampa e può controllare solo l'accesso alle stampanti. Se il riavvio del computer influisce negativamente sui flussi di lavoro nell'organizzazione, è possibile riavviare solo il servizio spoolsv (Spooler di stampa). Il controllo di stampa non è supportato nei computer basati su Arm.

- A partire da Kaspersky Endpoint Security 12.0 for Windows, il protocollo WPA3 è supportato dall'applicazione per i dispositivi di tipo **Wi-Fi**. Se a un computer viene applicato un criterio di Kaspersky Endpoint Security versione 12.2, il protocollo WPA2 viene selezionato nei computer con Kaspersky Endpoint Security versione 11.11.0 e precedenti; WPA2/WPA3 viene selezionato per le versioni da 12.0 a 12.1; WPA3 viene selezionato per le versioni 12.2 e successive.

- I dispositivi Apple sono classificati come dispositivi portatili (MTP) e dispositivi iTunes. Il sistema operativo può identificare in modo errato la connessione del dispositivo Apple e non determinare il dispositivo Apple come dispositivo portatile (MTP). Pertanto, il dispositivo Apple non sarà disponibile nel file manager, ma accessibile nell'applicazione iTunes. Di conseguenza, Kaspersky Endpoint Security controllerà l'accesso al dispositivo Apple solo nell'applicazione iTunes. Per accedere al tuo dispositivo Apple come dispositivo portatile (MTP), è necessario passare Gestione dispositivi e rimuovere il driver USB del dispositivo mobile Apple dall'elenco dei controller USB. Dopo il riavvio del computer, il sistema operativo identificherà il dispositivo Apple come dispositivo portatile (MTP) e dispositivo iTunes. Kaspersky Endpoint Security controllerà l'accesso al dispositivo sia nell'applicazione iTunes che nel file manager.

- In Kaspersky Endpoint Security 12.3 for Windows, le impostazioni di accesso sono diverse per il tipo di dispositivo **Bluetooth**. Se è stato specificato il valore **Dipende dal bus di connessione** nella versione precedente dell'applicazione, dopo aver aggiornato l'applicazione alla versione 12.3, il valore configurato cambia in **Consenti e non registrare**. Ciò non altera il comportamento del dispositivo.

- Controllo dispositivi supporta i dispositivi Bluetooth solo tramite lo stack Bluetooth di Microsoft Windows. Controllo dispositivi potrebbe funzionare in modo non corretto con gli stack Bluetooth di terzi.

- Se il dispositivo Bluetooth nasconde o falsifica la sua classe del dispositivo (COD, Class of Device), Controllo dispositivi potrebbe funzionare in modo errato.

- Sui computer Windows 7 o Windows 8 con determinati driver del dongle Bluetooth Realtek, potrebbe non essere possibile consentire solo la connessione di dispositivi Bluetooth come dispositivi di input (classe HID). In altre parole, se si vieta l'accesso ai dispositivi Bluetooth nelle impostazioni dell'applicazione e si aggiungono dispositivi di input alle esclusioni, Controllo dispositivo potrebbe impedire l'accesso a tutti i dispositivi Bluetooth.

Controllo Web

- I formati OGV e WEBM non sono supportati.

- Il protocollo RTMP non è supportato.

- Controllo Web supporta solo WSL1. L'applicazione non controlla il traffico WSL2.

Controllo adattivo delle anomalie

- È consigliabile creare esclusioni automaticamente in base all'evento. Quando si aggiunge manualmente un'esclusione, aggiungere il carattere `*` all'inizio del percorso quando si specifica l'oggetto di destinazione.
- Il **Rapporto sulle regole attivate di Controllo adattivo delle anomalie** non può essere generato se il campione include anche un solo evento il cui nome contiene più di 260 caratteri.
- L'aggiunta di esclusioni dall'archivio Attivazione delle regole di Controllo adattivo delle anomalie non è supportata se le proprietà di un oggetto o di un processo hanno un valore costituito da più di 256 caratteri, ad esempio il percorso dell'oggetto di destinazione. È possibile aggiungere manualmente un'esclusione nelle impostazioni dei criteri. È inoltre possibile aggiungere un'esclusione nel Rapporto sulle regole attivate di Controllo adattivo delle anomalie.
- Kaspersky Security Center 15.1 non può generare un rapporto dettagliato **Rapporto sullo stato delle regole di Controllo adattivo delle anomalie** per una regola specifica.
- Le regole di Controllo adattivo delle anomalie sono disponibili solo nella lingua corrispondente a quella di installazione del plug-in Web. Se si modifica la lingua dell'interfaccia, Web Console visualizza un elenco vuoto di regole. Per accedere alle regole, ripristinare la lingua dell'interfaccia utilizzata per l'installazione del plug-in Web.

Crittografia unità (FDE)

- Criptaggio disco Kaspersky non è supportato nei computer basati su Arm.
- Crittografia unità BitLocker non è supportato nei computer in cui viene eseguito Windows Home.
- Con Crittografia unità BitLocker, l'utente può modificare manualmente la password di autenticazione utilizzando l'API di Windows. In questi casi, BitLocker ignora i requisiti per le password impostati nel criterio di Kaspersky Endpoint Security. In altre parole, l'utente può impostare qualsiasi password.
- Dopo avere installato l'applicazione, è necessario riavviare il sistema operativo affinché il criptaggio del disco rigido funzioni correttamente.
- L'Agente di Autenticazione non supporta i geroglifici o i caratteri speciali `|` e `\`.
- Per garantire prestazioni ottimali del computer dopo il criptaggio, è necessario che il processore supporti il set di istruzioni AES-NI (Intel Advanced Encryption Standard New Instructions). Se il processore non supporta AES-NI, le prestazioni del computer potrebbero essere ridotte.
- Quando sono presenti processi che tentano di accedere ai dispositivi criptati prima che l'applicazione abbia concesso l'accesso a tali dispositivi, l'applicazione mostra un avviso che indica che tali processi devono essere terminati. Se i processi non possono essere terminati, ricollegare i dispositivi criptati.
- Gli ID univoci dei dischi rigidi vengono visualizzati nelle statistiche di criptaggio dei dispositivi in formato invertito.
- Non è consigliabile formattare i dispositivi mentre vengono criptati.
- Quando più unità rimovibili vengono collegate contemporaneamente a un computer, il criterio di criptaggio può essere applicato a una sola unità rimovibile. Quando i dispositivi rimovibili vengono ricollegati, il criterio di criptaggio viene applicato correttamente.
- Il criptaggio potrebbe non avviarsi in un disco rigido molto frammentato. Deframmentare il disco rigido.

- Quando i dischi rigidi sono criptati, l'ibernazione viene bloccata dal momento in cui viene avviata l'attività di criptaggio fino al primo riavvio di un computer con Microsoft Windows 7/8/8.1/10 e dopo l'installazione del criptaggio del disco rigido fino al primo riavvio dei sistemi operativi Microsoft Windows 8/8.1/10. Quando i dischi rigidi vengono decriptati, l'ibernazione viene bloccata dal momento in cui l'unità di avvio viene completamente decriptata fino al primo riavvio del sistema operativo. Quando l'opzione Avvio rapido è abilitata in Microsoft Windows 8/8.1/10, il blocco dell'ibernazione impedisce l'arresto del sistema operativo.

- I computer Windows 7 non consentono di modificare la password durante il ripristino quando il disco è criptato con la tecnologia BitLocker. Dopo l'immissione della chiave di ripristino e il caricamento del sistema operativo, Kaspersky Endpoint Security non richiederà all'utente di modificare la password o il codice PIN. È pertanto impossibile impostare una nuova password o un codice PIN. Questo problema deriva dalle caratteristiche specifiche del sistema operativo. Per continuare, è necessario criptare nuovamente il disco rigido.

- Non è consigliabile utilizzare lo strumento xbootmgr.exe con provider aggiuntivi abilitati. Ad esempio Dispatcher, Rete o Driver.

- La formattazione di un'unità rimovibile criptata non è supportata in un computer in cui è installato Kaspersky Endpoint Security for Windows.

- La formattazione di un'unità rimovibile criptata con il file system FAT32 non è supportata (l'unità viene visualizzata come criptata). Per formattare un'unità, riformattala nel file system NTFS.

- In un computer criptato non possono coesistere più agenti di download.

- Nel tentativo di ripristinare l'immagine di un disco GPT di avvio in uno stato non criptato, il sistema operativo può rendere inutilizzabile il sistema operativo. Per evitare ciò, seguire i seguenti suggerimenti:

  - Decriptare completamente il disco prima di ripristinare l'immagine dal backup.

  - Utilizzare la copia settore per settore durante la creazione dell'immagine.

  - Eliminare i dati dai primi settori del disco criptato prima di ripristinare l'immagine e reinizializzare il disco.

- È impossibile accedere a un'unità rimovibile precedentemente criptata in un computer diverso quando vengono soddisfatte contemporaneamente tutte le seguenti condizioni:

  - Non è presente alcuna connessione al server di Kaspersky Security Center.

  - L'utente sta tentando l'autorizzazione con un nuovo token o una nuova password.

  Se si verifica una situazione simile, riavviare il computer. Dopo il riavvio del computer, verrà concesso l'accesso all'unità rimovibile criptata.

- Il rilevamento dei dispositivi USB da parte dell'Agente di Autenticazione potrebbe non essere supportato quando la modalità xHCI per USB è abilitata nelle impostazioni BIOS.

- Il criptaggio disco Kaspersky (FDE) per la parte SSD di un dispositivo utilizzato per la memorizzazione nella cache dei dati utilizzati più di frequente non è supportato per i dispositivi SSHD.

- Il criptaggio dei dischi rigidi nei sistemi operativi Microsoft Windows 8/8.1/10 a 32 bit in esecuzione in modalità UEFI non è supportato.

- Riavviare il computer prima di criptare nuovamente un disco rigido decriptato.

- Il criptaggio del disco rigido non è compatibile con Kaspersky Anti-Virus per UEFI. Non è consigliabile utilizzare il criptaggio del disco rigido nei computer in cui è installato Kaspersky Anti-Virus per UEFI.

- La creazione di account dell'Agente di Autenticazione basati sugli account Microsoft è supportata con le seguenti limitazioni:

  - La tecnologia Single Sign-On non è supportata.

  - La creazione automatica di account dell'Agente di Autenticazione non è supportata se è selezionata l'opzione per creare account per gli utenti che accedono al sistema negli ultimi N giorni.

- Se il nome di un account dell'Agente di Autenticazione ha il formato `<domain>/<Windows account name>`, dopo aver modificato il nome del computer è necessario modificare anche i nomi degli account creati per gli utenti locali di questo computer. Si provi a immaginare ad esempio che ci sia un utente locale `Ivanov` nel computer `Ivanov` e che sia stato creato un account dell'Agente di Autenticazione con il nome `Ivanov/Ivanov` per questo utente. Se il nome del computer `Ivanov` è stato modificato in `Ivanov-PC`, è necessario modificare il nome dell'account dell'Agente di Autenticazione per l'utente `Ivanov` da `Ivanov/Ivanov` a `Ivanov-PC/Ivanov`. È possibile modificare il nome dell'account utilizzando l'attività di gestione dell'account locale dell'Agente di Autenticazione. Prima che il nome dell'account venga modificato, l'autenticazione nell'ambiente di preavvio è possibile utilizzando il nome precedente (ad esempio `Ivanov/Ivanov`).

- Se un utente ha l'autorizzazione ad accedere a un computer criptato utilizzando la tecnologia Criptaggio disco Kaspersky solo utilizzando un token e questo utente deve completare la procedura di ripristino dell'accesso, assicurarsi che questo utente disponga dell'accesso basato su password per questo computer dopo il ripristino dell'accesso al computer criptato. La password impostata dall'utente durante il ripristino dell'accesso potrebbe non essere salvata. In questo caso l'utente dovrà completare nuovamente la procedura per ripristinare l'accesso al computer criptato al successivo riavvio del computer.

- Quando si decripta un disco rigido utilizzando lo strumento di ripristino FDE, il processo di decriptaggio potrebbe terminare con un errore se i dati sul dispositivo di origine vengono sovrascritti con i dati decriptati. Parte dei dati sul disco rigido rimarranno criptati. È consigliabile scegliere l'opzione per salvare i dati decriptati in un file nelle impostazioni di decriptaggio del dispositivo quando si utilizza lo strumento di ripristino FDE.

- Se la password dell'Agente di Autenticazione è stata modificata, viene visualizzato un messaggio contenente il testo *Password modificata.Viene visualizzato Fare clic su OK*, l'utente riavvia il computer e la nuova password non viene salvata. La password precedente deve essere utilizzata per la successiva autenticazione nell'ambiente di preavvio.

- Il criptaggio del disco non è compatibile con la tecnologia Intel Rapid Start.

- Il criptaggio del disco non è compatibile con la tecnologia ExpressCache.

- In alcuni casi, quando si tenta di decriptare un'unità criptata utilizzando lo strumento di ripristino FDE, lo strumento rileva erroneamente lo stato del dispositivo come "non criptato" dopo il completamento della procedura "Richiesta-Risposta". Il registro dello strumento mostra un evento che indica che il dispositivo è stato decriptato correttamente. In questo caso, è necessario riavviare la procedura di ripristino dei dati per decriptare il dispositivo.

- Dopo che il plug-in di Kaspersky Endpoint Security for Windows è stato aggiornato in Web Console, le proprietà del computer client non mostrano la chiave di ripristino di BitLocker fino al riavvio del servizio Web Console.

- Per visualizzare le altre limitazioni del supporto del Criptaggio dell'intero disco e un elenco dei dispositivi per i quali il criptaggio dei dischi rigidi è supportato con restrizioni, fare riferimento alla Knowledge Base dell'Assistenza tecnica.

Criptaggio a livello di file (FLE)

- Il criptaggio dei file non è supportato nei computer basati su Arm.
- Il criptaggio di file e cartelle non è supportato nei sistemi operativi Microsoft Windows Embedded.
- Dopo aver installato l'applicazione, è necessario riavviare il sistema operativo affinché il criptaggio di file e cartelle funzioni correttamente.
- L'applicazione supporta il criptaggio dei file solo nei dispositivi con file system NTFS e FAT32. Se un file criptato viene trasferito in un dispositivo con un file system non supportato (ad esempio exFAT), il file in tale dispositivo non verrà criptato e sarà disponibile per la modifica.
- Se un file criptato viene archiviato in un computer con funzionalità di criptaggio disponibili e si accede al file da un computer in cui il criptaggio non è disponibile, verrà fornito l'accesso diretto a questo file. Un file criptato archiviato in una cartella di rete in un computer con funzionalità di criptaggio disponibili viene copiato in formato decriptato in un computer che non dispone di funzionalità di criptaggio disponibili.
- È consigliabile decriptare i file che sono stati criptati con Encrypting File System prima di criptare i file con Kaspersky Endpoint Security for Windows.
- Dopo il criptaggio, le dimensioni di un file aumentano di 4 KB.
- Dopo il criptaggio, l'attributo *Archivio* viene impostato nelle proprietà del file.
- Quando si copia il file decriptato, ad esempio su un supporto rimovibile, il file potrebbe rimanere criptato. Questo può accadere perché quando il file manager (ad esempio, explorer.exe) tenta di ottenere l'accesso al file criptato, salva l'hash del file in un elenco speciale del processo. Dopo la decriptaggio del file, quando il file manager tenta di accedere al file, il processo cerca l'hash del file nell'elenco. Se l'hash viene trovato, Kaspersky Endpoint Security lascia il file criptato. Per evitare ciò, è necessario cancellare l'elenco del processo. Il sistema operativo cancella automaticamente l'elenco del processo mentre si riempie. È inoltre possibile cancellare manualmente l'elenco. A tale scopo, è possibile riavviare il computer, riavviare il processo utilizzato per ottenere l'accesso al file (ad esempio, explorer.exe) oppure è possibile utilizzare un file manager diverso non utilizzato per l'accesso al file criptato.
- Se un file decompresso da un archivio criptato ha lo stesso nome di un file già esistente nel computer, quest'ultimo verrà sovrascritto dal nuovo file decompresso da un archivio criptato. L'utente non riceve una notifica dell'operazione di sovrascrittura.
- Prima di decomprimere un archivio criptato, assicurarsi di disporre di spazio su disco sufficiente per contenere i file decompressi. Se non si dispone di spazio su disco sufficiente, la decompressione dell'archivio potrebbe essere completata, ma i file potrebbero essere danneggiati. In questo caso, è possibile che Kaspersky Endpoint Security non mostri alcun messaggio di errore.
- L'interfaccia di Portable File Manager non visualizza messaggi sugli errori che si verificano durante il funzionamento.
- Kaspersky Endpoint Security for Windows non avvia Portable File Manager in un computer in cui è installato il componente Criptaggio a livello di file.

- Non è possibile usare Portable File Manager per accedere a un'unità rimovibile se sussistono contemporaneamente le seguenti condizioni:
  - Non è presente alcuna connessione a Kaspersky Security Center;
  - Kaspersky Endpoint Security for Windows è installato nel computer.
  - Il criptaggio dei dati (FDE o FLE) non è stato eseguito nel computer.

  L'accesso è impossibile anche se si conosce la password di Portable File Manager.
- Quando viene utilizzato il criptaggio dei file, l'applicazione non è compatibile con il client di posta Sylpheed.
- Kaspersky Endpoint Security for Windows non supporta le regole di restrizione dell'accesso ai file criptati per alcune applicazioni. Ciò è dovuto al fatto che alcune operazioni sui file vengono eseguite da un'applicazione di terzi. Ad esempio, la copia dei file viene eseguita dal programma per la gestione dei file, non dall'applicazione stessa. In questo modo, se l'accesso ai file criptati viene negato al client di posta di Outlook, Kaspersky Endpoint Security consentirà al client di posta di accedere al file criptato, se l'utente ha copiato i file nel messaggio e-mail tramite gli appunti o la funzione di trascinamento e rilascio. L'operazione di copia è stata eseguita da un programma per la gestione dei file, per il quale non sono specificate le regole di restrizione dell'accesso ai file criptati, ovvero l'accesso è consentito.
- Quando le unità rimovibili sono criptate con il supporto della modalità portatile, il controllo della validità della password non può essere disabilitato.
- La modifica delle impostazioni del file di paging non è supportata. Il sistema operativo utilizza i valori predefiniti invece dei valori dei parametri specificati.
- Utilizzare la rimozione sicura quando si utilizzano unità rimovibili criptate. Non è possibile garantire l'integrità dei dati se l'unità rimovibile non viene rimossa in modo sicuro.
- Dopo il criptaggio dei file, gli originali non criptati vengono eliminati in modo sicuro.
- La sincronizzazione dei file offline utilizzando Client-Side Caching (CSC) non è supportata. Il criptaggio dei file offline o la tecnologia Branch Caching su SMB per i server non sono supportati. È consigliabile vietare la gestione offline delle risorse condivise a livello dei criteri di gruppo. I file che si trovano in modalità offline possono essere modificati. Dopo la sincronizzazione, le modifiche apportate a un file offline potrebbero andare perse.
- La creazione di un archivio criptato nella radice del disco rigido di sistema non è supportata.
- Potrebbero verificarsi problemi durante l'accesso ai file criptati nella rete. È consigliabile spostare i file in un'origine diversa o assicurarsi che il computer utilizzato come file server sia gestito dallo stesso Kaspersky Security Center Administration Server.
- La modifica del layout della tastiera potrebbe causare il blocco della finestra di immissione della password per un archivio criptato autoestraente. Per risolvere questo problema, chiudere la finestra di immissione della password, passare al layout di tastiera nel sistema operativo e immettere nuovamente la password per l'archivio criptato.
- Quando si utilizza il criptaggio dei file in sistemi che hanno più partizioni in un disco, è consigliabile utilizzare l'opzione che determina automaticamente la dimensione del file pagefile.sys. Dopo il riavvio del computer, il file pagefile.sys potrebbe spostarsi tra le partizioni del disco.

- Dopo aver applicato le regole di criptaggio dei file, inclusi i file nella cartella *Documenti*, assicurarsi che gli utenti per i quali è stato applicato il criptaggio possano accedere correttamente ai file criptati. A tale scopo, fare in modo che ogni utente acceda al sistema quando è disponibile una connessione a Kaspersky Security Center. Se un utente tenta di accedere a file criptati senza una connessione a Kaspersky Security Center, il sistema potrebbe bloccarsi.

- Se i file di sistema sono in qualche modo inclusi nell'ambito del criptaggio a livello di file, nei rapporti potrebbero essere visualizzati eventi relativi a errori durante il criptaggio di questi file. I file specificati in questi eventi non sono effettivamente criptati.

- I processi Pico non sono supportati.

- I percorsi con distinzione tra maiuscole e minuscole non sono supportati. Quando vengono applicate regole di criptaggio o regole di decriptaggio, i percorsi negli eventi del prodotto vengono visualizzati in minuscolo.

- Non è consigliabile criptare i file utilizzati dal sistema all'avvio. Se questi file sono criptati, un tentativo di accedere a file criptati senza una connessione a Kaspersky Security Center potrebbe causare il blocco del sistema o richiedere l'accesso a file non criptati.

- Se gli utenti utilizzano contemporaneamente un file nella rete in base alle regole FLE tramite applicazioni che utilizzano il metodo di mappatura file-memoria (come WordPad o FAR) e applicazioni progettate per l'impiego di file di grandi dimensioni (come Notepad ++), il file in formato non criptato può essere bloccato a tempo indeterminato senza la possibilità di accedervi dal computer in cui risiede.

- Kaspersky Endpoint Security non cripta i file che si trovano nell'archivio cloud di OneDrive o in altre cartelle con OneDrive come nome. Kaspersky Endpoint Security blocca inoltre la copia dei file criptati nelle cartelle OneDrive se tali file non vengono aggiunti alla regola di decriptaggio.

- Quando è installato il componente Criptaggio a livello di file, la gestione di utenti e gruppi non funziona in modalità WSL (Windows Subsystem for Linux).

- Quando è installato il componente Criptaggio a livello di file, POSIX (Portable Operating System Interface) per la ridenominazione e l'eliminazione dei file non è supportato.

- Non è consigliabile criptare i file temporanei, poiché può causare perdite di dati. Ad esempio, Microsoft Word crea file temporanei durante l'elaborazione di un documento. Se i file temporanei sono criptati, ma il file originale non lo è, l'utente potrebbe ricevere un errore *Accesso negato* durante il tentativo di salvataggio del documento. Inoltre, Microsoft Word potrebbe salvare il file, ma non sarà possibile aprire il documento la volta successiva, ovvero i dati andranno persi. Per prevenire la perdita di dati, è necessario escludere la cartella dei file temporanei dalle regole di criptaggio.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Non è possibile eseguire la scansione di un oggetto inserito in Quarantena a causa dell'attività *Sposta file in Quarantena*.

- Non è possibile spostare in Quarantena un Alternate Data Stream (ADS) di dimensioni superiori ai 4 MB. Kaspersky Endpoint Security ignora qualsiasi ADS di queste dimensioni senza avvisare l'utente.

- Kaspersky Endpoint Security non esegue le attività *Scansione IOC* nelle unità di rete se il percorso della cartella nelle proprietà dell'attività inizia con una lettera di unità. Kaspersky Endpoint Security supporta solo i percorsi in formato UNC per le attività *Scansione IOC* nelle unità di rete. Ad esempio, `\\server\shared_folder`.

- Per garantire che l'attività *Scansione IOC* che utilizza i termini di EmailItem funzioni correttamente, il plug-in Web Kaspersky Endpoint Security deve essere aggiornato alla versione più recente.

- Nei computer basati su Arm, l'attività *Scansione IOC* supporta i file e-mail solo dai seguenti client di posta: versioni a 32 e 64 bit di Outlook 2016 e Outlook 2021, 2024 e 365 per Arm64.

- L'importazione del file di configurazione di un'applicazione termina con un errore se l'impostazione Integrazione con Kaspersky Sandbox è abilitata nel file di configurazione. Prima di esportare le impostazioni dell'applicazione, disabilitare Kaspersky Sandbox. Quindi, eseguire la procedura di esportazione/importazione. Dopo aver importato il file di configurazione, abilitare Kaspersky Sandbox.

- Quando si importa un criterio da un file KLP, il valore del parametro che determina l'accettazione dei termini e delle condizioni del Contratto di Kaspersky Detection and Response Expert non viene applicato. Di conseguenza, dopo l'importazione del criterio, Kaspersky Endpoint Security non esegue le funzioni di EDR Agent. Affinché EDR Agent funzioni, aprire il criterio, modificare un parametro qualsiasi e salvare le impostazioni del criterio.

- Quando viene rilevato un indicatore di compromissione durante l'esecuzione dell'attività *Scansione IOC*, l'applicazione sposta in Quarantena un file solo per il termine FileItem. Lo spostamento in Quarantena di un file per altri termini non è supportata.

- Per la gestione dei dettagli degli avvisi, è necessario il plug-in Web Kaspersky Endpoint Security for Windows versione 11.7.0 o successiva. I dettagli degli avvisi sono necessari quando si utilizzano le soluzioni Endpoint Detection and Response (EDR Optimum ed EDR Expert). I dettagli degli avvisi sono disponibili solo in Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console.

- La migrazione della configurazione [KES+KEA] alla configurazione [KES+agente integrato] potrebbe essere completata con un errore di rimozione dell'applicazione Kaspersky Endpoint Agent. L'errore di rimozione dell'applicazione è stato risolto nella versione più recente di Kaspersky Endpoint Agent. Per rimuovere Kaspersky Endpoint Agent, riavviare il computer e creare un'attività di rimozione dell'applicazione.

- La configurazione [KES+KEA+agente integrato] non è supportata. Tale configurazione interrompe l'interazione tra le applicazioni e la soluzione Detection and Response distribuita nell'organizzazione. Inoltre, l'utilizzo di Kaspersky Endpoint Agent e dell'agente integrato nello stesso computer può causare la duplicazione dei dati di telemetria e un aumento del carico nel computer e nella rete. Dopo la migrazione alla configurazione [KES + agente integrato], assicurarsi che Kaspersky Endpoint Agent sia stato rimosso dal computer. Se Kaspersky Endpoint Agent continua a funzionare dopo la migrazione, disinstallare l'applicazione manualmente (ad esempio, utilizzando l'attività *Disinstalla l'applicazione in remoto*).

  Il programma di installazione consente di distribuire Kaspersky Endpoint Agent in un computer con Kaspersky Endpoint Security e l'agente integrato installato. Kaspersky Endpoint Agent e l'agente integrato possono anche essere installati in un computer grazie all'attività *Modifica i componenti dell'applicazione*. Il comportamento dipende dalle versioni di Kaspersky Endpoint Security e Kaspersky Endpoint Agent.

- Durante la generazione dei dettagli degli avvisi, l'applicazione fornisce informazioni sulla minaccia rilevata, inclusi gli hash dei file modificati. Kaspersky Endpoint Security calcola l'hash del file durante la generazione dei dettagli degli avvisi. Si noti che l'hash originale del file al momento della generazione dell'evento di modifica del file potrebbe non corrispondere all'hash calcolato quando sono stati generati i dettagli dell'avviso.

- L'agente integrato, EDR (KATA), riprende l'isolamento di rete di un computer dopo il riavvio di un computer, anche se il periodo di isolamento è scaduto. Per impedire il ripetuto isolamento del computer, è necessario disattivare l'isolamento della rete nella console di Kaspersky Anti Targeted Attack Platform.

- Si consiglia di effettuare l'upgrade dell'applicazione al termine dell'isolamento di rete. Dopo l'upgrade di Kaspersky Endpoint Security, l'isolamento di rete può essere interrotto.

- Gli agenti integrati per EDR (KATA), EDR Optimum ed EDR Expert non sono compatibili tra loro. Pertanto, l'attivazione dell'agente integrato EDR con una licenza autonoma del componente aggiuntivo Kaspersky Endpoint Detection and Response può essere ignorata se Kaspersky Endpoint Security è stato attivato con funzionalità EDR diverse. Ad esempio, l'attivazione dell'agente integrato EDR (KATA) con una licenza autonoma viene ignorata se Kaspersky Endpoint Security è stato attivato con la licenza di [KES EDR Optimum].

- In Kaspersky Endpoint Security versione 12.1, l'agente EDR (KATA) integrato non supporta i seguenti metafile per l'attività *Ottieni metafile NTFS*: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. A Kaspersky Endpoint Security versione 12.2 è stato aggiunto il supporto per questi metafile.

- Durante la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security per la soluzione Kaspersky Anti Targeted Attack Platform (EDR), è possibile che si verifichino errori durante la connessione del computer ai server di Central Node. Questa situazione è causata dalla migrazione guidata in Web Console, che ignora le seguenti impostazioni dei criteri e non le migra:

  - Divieto di modifica delle impostazioni **Impostazioni di connessione** ("lucchetto").

    Per impostazione predefinita, le impostazioni possono essere modificate (il "lucchetto" è aperto). Pertanto, le impostazioni non vengono applicate al computer. È necessario vietare la modifica delle impostazioni e chiudere il "lucchetto".

  - Contenitore crittografico.

    Se si utilizza l'autenticazione a due vie per la connessione ai server di Central Node, è necessario aggiungere di nuovo il contenitore crittografico. La migrazione guidata migra correttamente il certificato TLS del server.

  La Migrazione guidata dei criteri e delle attività in Administration Console (MMC) migra tutte le impostazioni per la soluzione Kaspersky Anti Targeted Attack Platform (EDR).

- Lo stato di attivazione dell'applicazione viene visualizzato erroneamente quando l'applicazione è installata in modalità Endpoint Detection and Response Agent per supportare la soluzione Kaspersky Managed Detection and Response senza connessione a Kaspersky Security Center. Dopo il download del file BLOB, l'area di notifica della barra delle applicazioni di Windows mostra uno stato errato: *L'applicazione non è stata attivata*. Tuttavia, l'interfaccia dell'applicazione mostra correttamente lo stato di attivazione. Riavviare il computer affinché l'applicazione funzioni correttamente.

- Kaspersky Endpoint Security consente l'integrazione con la soluzione Kaspersky Anti Targeted Attack Platform utilizzando il componente EDR (KATA) o Endpoint Sensor (non supportato). Si noti che è possibile utilizzare solo uno dei componenti per interagire con Kaspersky Anti Targeted Attack Platform. Per visualizzare lo stato del componente, aprire le proprietà del computer in Administration Console (MMC), nella sezione **Applicazioni**, aprire le proprietà di Kaspersky Endpoint Security for Windows e passare alla sezione **Componenti**. Le seguenti considerazioni speciali si applicano alla visualizzazione dello stato dei componenti per l'interazione con Kaspersky Anti Targeted Attack Platform:

  - Per il plug-in di gestione 12.0 e versioni precedenti, l'applicazione mostra lo stato corrente di **Endpoint Sensor**. In Kaspersky Endpoint Security 12.0 e versioni precedenti, il componente EDR (KATA) non è disponibile. Il componente EDR (KATA) è stato introdotto nella versione 12.1.

  - Per il plug-in di gestione 12.1 e versioni successive, l'applicazione mostra lo stato generale di **Endpoint Detection and Response (KATA)**, che può indicare lo stato di Sensore Endpoint o lo stato del componente EDR (KATA). Questo dipende dalla versione dell'applicazione installata nel computer dell'utente e dai componenti disponibili che è possibile utilizzare per interagire con Kaspersky Anti Targeted Attack Platform.

- A partire da Kaspersky Endpoint Security 12.6 e versioni successive, Kaspersky Security Center Web Console 14.2 e versioni precedenti non mostrano correttamente il nome del componente **Endpoint Detection and Response (KATA)** nelle proprietà del computer. Invece del componente **Endpoint Detection and Response (KATA)**, l'applicazione mostra il nome del componente **Endpoint Detection and Response Expert (KATA EDR)**. Per visualizzare l'elenco dei componenti, aprire le proprietà del computer in Web Console, nella sezione **Applicazioni**, aprire le proprietà di Kaspersky Endpoint Security for Windows e passare alla sezione **Componenti**. A partire da Kaspersky Security Center Web Console 15.1 e versioni successive, l'applicazione mostra correttamente il nome del componente.

- Quando si aggiorna il plug-in di gestione di Kaspersky Endpoint Detection and Response alla versione 15.3 installata nelle versioni di Console Web 14.0-14.2, i dettagli degli avvisi vengono visualizzati in modo errato. Per il corretto funzionamento dei dettagli degli avvisi, riavviare Kaspersky Security Center Administration Server.

- Il plug-in di gestione di Kaspersky Endpoint Detection and Response versione 15.4 e successive non supporta Kaspersky Security Center versione 14.0. Dopo l'aggiornamento del plug-in di gestione, i dettagli degli avvisi vengono visualizzati in modo errato.

- Le soluzioni di classe Kaspersky Extended Detection and Response (XDR) versione 1.4 non supportano il plug-in Web Kaspersky Endpoint Security for Windows versione 12.12 o successiva. È possibile lasciare la versione corrente del plug-in Web o aggiornare la soluzione XDR alla versione 2.0 o successiva.

- Kaspersky Endpoint Security non invia oggetti destinati all'architettura Arm a Kaspersky Sandbox.

- Kaspersky Endpoint Security supporta un massimo di 10.000 regole di filtro degli eventi di inclusione ed esclusione di EDR Expert (on-premises) in totale.

- Le regole di filtro degli eventi di EDR Expert (on-premises) non verranno passate dal criterio ai dispositivi gestiti in cui viene eseguito Kaspersky Endpoint Security versione 14.0 o precedenti se viene superato il limite supportato per le regole di filtro archiviate. L'applicazione mostrerà un avviso corrispondente.

- Le versioni 12.11–14.1 di Kaspersky Endpoint Security for Windows non supportano i seguenti eventi di telemetria di EDR Expert (on-premises):

  - LDAP Attribute Change
  - GPO Change
  - SCCM Local Config Mismatch
  - SCCM Config Change
  - SCCM Deployment Task
  - Smb Connection Open

  A partire dalla versione 14.2, Kaspersky Endpoint Security supporta tutti questi eventi di telemetria di EDR Expert (on-premises), ad eccezione di LDAP Attribute Change.

Altre limitazioni

- I sistemi operativi Windows, a partire dalla versione 11 24H2, supportano la tecnologia UDP Receive Segment Coalescing Offload (URO). La tecnologia è abilitata per impostazione predefinita se nel computer sono installati una scheda di rete e driver compatibili. La disabilitazione di URO nel computer di un utente può ridurre significativamente le prestazioni dell'applicazione.

- Kaspersky Endpoint Security supporta il sottosistema WSL (Windows Subsystem for Linux) con restrizioni:

  - WSL 1. L'applicazione monitora il traffico di rete e rileva le minacce tramite HTTP/HTTPS. Poiché Kaspersky Endpoint Security utilizza il proprio certificato per eseguire la scansione delle connessioni HTTPS protette, il funzionamento di alcune applicazioni di terze parti potrebbe essere interrotto.

  - WSL 2. L'applicazione non supporta WSL 2.

- Se l'applicazione restituisce errori o si blocca durante l'esecuzione, può essere riavviata automaticamente. Se si verificano errori ricorrenti che causano l'arresto anomalo dell'applicazione, vengono eseguite le seguenti operazioni:

  1. Vengono disabilitate le funzioni di controllo e di protezione (la funzionalità di criptaggio rimane abilitata).
  2. Viene notificato all'utente che le funzioni sono state disabilitate.
  3. Viene eseguito un tentativo di ripristinare l'applicazione a uno stato funzionante dopo avere aggiornato i database anti-virus o applicato gli aggiornamenti dei moduli dell'applicazione.

- Gli indirizzi Web aggiunti all'elenco degli indirizzi attendibili potrebbero essere elaborati in modo non corretto.

- Nella console di Kaspersky Security Center, non è possibile salvare un file su disco dalla cartella **Avanzate** → **Archivi** → **Minacce attive**. Per salvare il file, è necessario disinfettare il file infetto. Durante la disinfezione, l'applicazione salva una copia del file in Backup. Ora è possibile salvare il file su disco dalla cartella **Avanzate** → **Archivi** → **Backup**.

- L'ereditarietà delle impostazioni di trasferimento dei dati ad Administration Server (**Impostazioni generali** → **Rapporti e archivi** → **Trasferimento dei dati ad Administration Server**) differisce dall'ereditarietà di altre impostazioni. Se è stata consentita la modifica delle impostazioni di trasmissione dei dati nel criterio (il "lucchetto" è aperto), per tali impostazioni verranno reimpostati i valori predefiniti nelle proprietà del computer locale nella console, se non erano state definite in precedenza. Se queste impostazioni erano state definite in precedenza, i relativi valori verranno ripristinati. Quando si elimina un criterio, le impostazioni vengono ereditate allo stesso modo. In questi casi, le altre impostazioni nelle proprietà del computer locale vengono ereditate dal criterio.

- Kaspersky Endpoint Security monitora il traffico HTTP conforme agli standard RFC 2616, RFC 7540, RFC 7541, RFC 7301. Se Kaspersky Endpoint Security rileva un altro formato di scambio dei dati nel traffico HTTP, l'applicazione blocca questa connessione per impedire il download di file dannosi da Internet.

- Kaspersky Endpoint Security impedisce la comunicazione tramite il protocollo QUIC. I browser utilizzano il protocollo di trasporto standard (TLS o SSL) indipendentemente dal fatto che il supporto QUIC sia abilitato o meno nel browser.

- Possono verificarsi errori di connessione TLS quando il software di terzi funziona con la libreria Libcurl. Questi errori possono essere correlati al certificato Kaspersky utilizzato da Kaspersky Endpoint Security per esaminare le connessioni criptate. Per continuare a lavorare, è possibile disabilitare la convalida del certificato per il software di terzi (scelta non consigliata) o aggiungere un corpo del certificato Kaspersky all'archivio certificati cURL. Per informazioni dettagliate, consultare la Knowledge Base di Kaspersky.

- Quando Kaspersky Endpoint Security for Windows viene avviato per la prima volta, un'applicazione con firma digitale potrebbe essere temporaneamente inserita nel gruppo sbagliato. L'applicazione firmata digitalmente verrà poi inserita nel gruppo corretto.

- Durante una nuova scansione di un oggetto dannoso bloccato da un software di terzi, l'utente non viene informato quando la minaccia viene rilevata di nuovo. L'evento del nuovo rilevamento della minaccia viene visualizzato nel rapporto dell'applicazione e nel rapporto di Kaspersky Security Center.

- Il rapporto di Kaspersky Security Center sul criptaggio dei dispositivi non includerà le informazioni sui dispositivi criptati utilizzando Microsoft BitLocker in piattaforme server o in workstation in cui non è installato il componente Controllo dispositivi.

- Non è possibile abilitare la visualizzazione di tutte le voci dei rapporti in Kaspersky Security Center Web Console. In Web Console, è possibile modificare solo il numero di voci visualizzate nei rapporti. Per impostazione predefinita, Kaspersky Security Center Web Console mostra 1000 voci di rapporto. È possibile abilitare la visualizzazione di tutte le voci di rapporto in Administration Console (MMC).

- Non è possibile impostare la visualizzazione di più di 1000 voci dei rapporti in Kaspersky Security Center Web Console. Se si imposta una valore superiore a 1000, Kaspersky Security Center Console mostrerà solo le prime 1000 voci di rapporto.

- Quando si utilizza una gerarchia di criteri, le impostazioni della sezione Criptaggio unità rimovibili in un criterio figlio sono accessibili per la modifica se il criterio padre vieta la modifica di tali impostazioni.

- È necessario abilitare Controlla Accesso nelle impostazioni del sistema operativo per garantire il corretto funzionamento delle esclusioni per la protezione delle cartelle condivise dal criptaggio esterno.

- Se la protezione delle cartelle condivise è abilitata, Kaspersky Endpoint Security for Windows monitora i tentativi di criptaggio delle cartelle condivise per ciascuna sessione di accesso remoto avviata prima dell'avvio di Kaspersky Endpoint Security for Windows, incluso se il computer da cui è stata avviata la sessione di accesso remoto è stato aggiunto alle esclusioni. Se si desidera che Kaspersky Endpoint Security for Windows non monitori i tentativi di criptare le cartelle condivise per le sessioni di accesso remoto avviate da un computer aggiunto alle esclusioni e avviate prima dell'avvio di Kaspersky Endpoint Security for Windows, terminare e ristabilire la sessione di accesso remoto o riavviare il computer in cui è installato Kaspersky Endpoint Security for Windows.

- Se l'attività di aggiornamento viene eseguita con le autorizzazioni di un account utente specifico, le patch del prodotto non verranno scaricate durante l'aggiornamento da un'origine che richiede l'autorizzazione.

- L'applicazione potrebbe non avviarsi a causa di prestazioni di sistema insufficienti. Per risolvere questo problema, utilizzare l'opzione Ready Boot o aumentare il timeout del sistema operativo per l'avvio dei servizi.

- L'applicazione non può funzionare in Windows Safe Mode.

- Non è possibile garantire che Controllo audio funzioni fino al primo riavvio dopo l'installazione dell'applicazione.

- In Administration Console (MMC), nelle impostazioni di Prevenzione Intrusioni nella finestra di configurazione delle autorizzazioni dell'applicazione, il pulsante **Rimuovi** non è disponibile. È possibile rimuovere un'applicazione da un gruppo di attendibilità tramite il menu di scelta rapida dell'applicazione.

- Nell'interfaccia locale dell'applicazione, nelle impostazioni di Prevenzione Intrusioni, le risorse protette e le autorizzazioni dell'applicazione non sono disponibili per la visualizzazione se il computer è gestito da un criterio. Lo scorrimento, la ricerca, il filtraggio e altri comandi della finestra non sono disponibili. È possibile visualizzare le autorizzazioni dell'applicazione nelle proprietà del criterio in Kaspersky Security Center Console.

- Quando i file di traccia ruotati sono abilitati, non vengono create tracce per il componente AMSI e il plug-in di Outlook.

- Le tracce delle prestazioni non possono essere raccolte manualmente in Windows Server 2008.

- Le tracce delle prestazioni per il tipo di traccia "Riavvia" non sono supportate.

- La registrazione dump non è supportata per i processi pico.

- La disattivazione dell'opzione **Disabilita gestione esterna dei servizi di sistema** non consentirà di arrestare il servizio dell'applicazione installata con il parametro `AMPPL=1` (per impostazione predefinita, il valore del parametro è impostato su `1` a partire dalla versione del sistema operativo Windows 10RS2). Il parametro `AMPPL` con valore `1` abilita l'uso della tecnologia Processi di protezione per il servizio del prodotto.

- Per eseguire la scansione personalizzata di una cartella, l'utente che avvia la scansione personalizzata deve disporre delle autorizzazioni per leggere gli attributi di questa cartella. In caso contrario, la scansione delle cartelle personalizzate non sarà impossibile e terminerà con un errore.

- Quando una regola di scansione definita in un criterio include un percorso senza il carattere `\` alla fine, ad esempio `C:\folder1\folder2`, la scansione verrà eseguita per il percorso `C:\folder1\`.

- Se si utilizzano criteri restrizione software (SRP, Software Restriction Policies), il computer potrebbe avere difficoltà di caricamento (schermo nero). Per evitare malfunzionamenti, è necessario consentire l'uso delle librerie delle applicazioni nelle proprietà SRP. Nelle proprietà SRP, aggiungere la regola con il livello di sicurezza **Senza restrizioni** per il file khkum.dll (voce di menu **Nuova regola hash**). Il file si trova nella cartella `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.2\klhk\klhk_x64\`. Se è stato selezionato questo metodo, è inoltre necessario deselezionare la casella di controllo **Scarica aggiornamenti dei moduli dell'applicazione** nelle impostazioni dell'attività *Aggiornamento* per Kaspersky Endpoint Security. Per informazioni dettagliate sull'utilizzo di SRP, fare riferimento alla documentazione di Microsoft.

  È inoltre possibile disabilitare SRP e utilizzare il componente Controllo applicazioni di Kaspersky Endpoint Security per controllare l'uso delle applicazioni.

- Se il computer appartiene a un dominio nell'oggetto Criteri di gruppo (GPO, Group Policy Object) di Windows con il parametro DriverLoadPolicy impostato su 8 (Good only), il riavvio del computer con Kaspersky Endpoint Security installato causa un BSOD. Per evitare un errore, il parametro Early Launch Antimalware (ELAM) in Criteri di gruppo deve essere impostato su 1 (Good and unknown). Le impostazioni ELAM si trovano nel criterio in: **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.

- La gestione delle impostazioni del plug-in di Outlook tramite Rest API non è supportata.

- Le impostazioni di esecuzione dell'attività per un utente specifico non possono essere trasferite tra i dispositivi tramite un file di configurazione. Dopo aver applicato le impostazioni da un file di configurazione, specificare manualmente il nome utente e la password.

- Dopo l'installazione di un aggiornamento, l'attività di controllo dell'integrità non funziona finché il sistema non viene riavviato per applicare l'aggiornamento.

- Quando il livello di traccia ruotato viene modificato tramite l'utilità di diagnostica remota, Kaspersky Endpoint Security for Windows visualizza erroneamente un valore vuoto per il livello di traccia. Tuttavia, i file di traccia vengono scritti in base al livello di traccia corretto. Quando il livello di traccia ruotato viene modificato tramite l'interfaccia locale dell'applicazione, il livello di traccia viene modificato correttamente ma l'utilità di diagnostica remota visualizza in modo errato l'ultimo livello di traccia definito dall'utilità. Per questo motivo, l'amministratore potrebbe non disporre delle informazioni aggiornate sul livello di traccia corrente e le informazioni pertinenti potrebbero essere non disponibili nelle tracce se un utente modifica manualmente il livello di traccia nell'interfaccia locale dell'applicazione.

- Nell'interfaccia locale le impostazioni di Protezione tramite password non consentono di modificare il nome dell'account amministratore (KLAdmin per impostazione predefinita). Per modificare il nome dell'account amministratore, è necessario disabilitare Protezione tramite password, quindi abilitare Protezione tramite password e specificare un nuovo nome per l'account amministratore.

- Quando installata su un server Windows Server 2019, l'applicazione Kaspersky Endpoint Security non è compatibile con Docker. La distribuzione dei contenitori Docker in un computer con Kaspersky Endpoint Security causa un arresto anomalo (BSOD).

- Se Kaspersky Endpoint Security è installato in un server DBMS di SQL Server, l'applicazione invia le richieste all'istanza del server. Questo è necessario per eseguire la scansione dei lavori di SQL Server Agent e impedire l'esecuzione di processi dannosi. Kaspersky Endpoint Security utilizza l'account utente SQL Server per eseguire la scansione dei lavori. L'applicazione invia le richieste al server durante la scansione della memoria di sistema e dopo l'aggiornamento dei database anti-virus.

- La compatibilità del software Kaspersky Endpoint Security e Secret Net Studio è limitata:

  - L'applicazione Kaspersky Endpoint Security non è compatibile con il componente antivirus del software Secret Net Studio.

    L'applicazione non può essere installata in un computer in cui Secret Net Studio è distribuito con il componente Antivirus. Per rendere possibile l'interoperabilità, è necessario rimuovere il componente Antivirus da Secret Net Studio.

  - L'applicazione Kaspersky Endpoint Security non è compatibile con il componente Protezione dei dischi e criptaggio dei dati del software Secret Net Studio.

    L'applicazione non può essere installata in un computer in cui Secret Net Studio è distribuito con il componente Protezione dei dischi e criptaggio dei dati. Per rendere possibile l'interoperabilità, è necessario rimuovere il componente Protezione dei dischi e criptaggio dei dati da Secret Net Studio.

  - Secret Net Studio non è compatibile con il componente File Level Encryption (FLE) di Kaspersky Endpoint Security.

    Quando si installa Kaspersky Endpoint Security con il componente File Level Encryption (FLE), Secret Net Studio può funzionare con errori. Per garantire l'interoperabilità, è necessario rimuovere il componente File Level Encryption (FLE) da Kaspersky Endpoint Security.

- Durante l'importazione delle regole di Monitoraggio integrità di sistema, l'applicazione controlla l'ID e il nome della regola. Se gli ID delle regole coincidono, Kaspersky Endpoint Security sostituisce le regole esistenti con la nuova regola. Durante l'esportazione delle regole, l'applicazione assegna automaticamente gli ID. Può esistere una regola con ID identici, ad esempio se sono stati modificati manualmente i file XML delle regole esportati. Se gli ID delle regole sono univoci, ma i nomi delle regole sono gli stessi, aggiunge Kaspersky Endpoint Security `(1)` e così via fino al nome della regola.

- A partire dalla versione 12.11 di Kaspersky Endpoint Security for Windows, non è possibile visualizzare le impostazioni di un criterio principale aperto in un gruppo secondario in Web Console. Web Console mostra inoltre un avviso: *Questo criterio è ereditato. È possibile modificare le impostazioni del criterio solo nel gruppo di amministrazione in cui è stato creato*.

- Le notifiche pop-up di lunghezza superiore a 256 caratteri non vengono visualizzate in Administration Console (MMC).

- I nomi dei componenti nel criterio e nel pacchetto di installazione potrebbero essere diversi. Ad esempio, Endpoint Detection and Response Expert (on-premises) può essere denominato Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises) e Kaspersky Anti Targeted Attack Platform Integration. I nomi dei componenti possono inoltre variare a seconda della versione dell'applicazione.

Glossario

Agente di Autenticazione

Interfaccia che consente di completare l'autenticazione per l'accesso ai dischi rigidi criptati e il caricamento del sistema operativo dopo il criptaggio del disco rigido di avvio.

Ambito della protezione

Oggetti per i quali viene eseguita costantemente la scansione da parte del componente Protezione Minacce Essenziale quando il componente è in esecuzione. Gli ambiti di protezione dei vari componenti dispongono di differenti proprietà.

Ambito della scansione

Oggetti per i quali Kaspersky Endpoint Security esegue la scansione durante l'esecuzione di un'attività di scansione.

Archivio

Uno o più file compressi in un singolo file. Per comprimere e decomprimere i dati è richiesta un'applicazione specifica chiamata archiver.

Attività

Funzioni eseguite dall'applicazione Kaspersky come attività, ad esempio: protezione dei file in tempo reale, scansione completa del dispositivo, aggiornamento del database.

Autenticazione Kerberos

Meccanismo di autenticazione reciproca da parte del client e del server prima di stabilire una connessione tra loro, che consente la comunicazione su reti non sicure. Il meccanismo si basa su un ticket, che l'utente ottiene da un centro di autenticazione attendibile.

Autorità di emissione del certificato

Centro di certificazione che ha emesso il certificato.

Certificato di licenza

Documento che Kaspersky trasferisce all'utente insieme al file chiave o al codice di attivazione. Contiene informazioni sulla licenza concessa all'utente.

Chiave attiva

Chiave attualmente utilizzata dall'applicazione.

Cloud Discovery

Cloud Discovery gestisce l'accesso degli utenti ai servizi cloud. I servizi cloud includono, ad esempio, Microsoft Teams, Salesforce e Microsoft Office 365. I servizi cloud sono raggruppati in categorie, ad esempio *Condivisione file*, *Messenger*, *E-mail*.

Database anti-virus

Database che contengono informazioni sulle minacce per la protezione del computer note a Kaspersky al momento del rilascio dei database anti-virus. Le firme dei database anti-virus consentono di rilevare il codice dannoso negli oggetti esaminati. I database anti-virus sono creati dagli specialisti di Kaspersky e vengono aggiornati ogni ora.

Database di indirizzi Web dannosi

Elenco di indirizzi Web il cui contenuto può essere considerato pericoloso. L'elenco viene creato dagli specialisti di Kaspersky. È regolarmente aggiornato e incluso nel kit di distribuzione dell'applicazione Kaspersky.

Database di indirizzi Web di phishing

Elenco di indirizzi Web identificati dagli specialisti di Kaspersky come correlati ad attività di phishing. Il database viene aggiornato regolarmente e fa parte del kit di distribuzione dell'applicazione Kaspersky.

Disinfezione

Metodo di elaborazione degli oggetti infetti che determina un ripristino parziale o completo dei dati. Non tutti gli oggetti infetti possono essere disinfettati.

Falso allarme

Un falso allarme si verifica quando un'applicazione Kaspersky segnala un file non infetto come infetto perché la firma del file è simile a quella di un virus.

File infettabile

File che, a causa della sua struttura o del suo formato, può essere utilizzato da utenti malintenzionati come "contenitore" per memorizzare e distribuire codice dannoso. In genere si tratta di file eseguibili, con estensioni come .com, .exe e .dll. Questi file presentano un rischio piuttosto alto di intrusione di codice dannoso.

File infetto

Un file che contiene codice dannoso (è stato rilevato codice di un malware noto durante la scansione del file). Kaspersky consiglia di evitare di utilizzare tali file, dal momento che possono infettare il computer.

File IOC

Un file che contiene una serie di indicatori di compromissione (IOC) che l'applicazione tenta di abbinare per eseguire un rilevamento. La probabilità di rilevamento può essere maggiore se vengono trovate corrispondenze esatte con più file IOC per l'oggetto come risultato della scansione.

Forma normalizzata dell'indirizzo di una risorsa Web

La forma normalizzata dell'indirizzo di una risorsa Web è una rappresentazione testuale dell'indirizzo di una risorsa Web ottenuta tramite la normalizzazione. La *normalizzazione* è un processo tramite il quale la rappresentazione testuale dell'indirizzo di una risorsa Web viene modificata in base a specifiche regole, ad esempio escludendo dalla rappresentazione testuale dell'indirizzo della risorsa Web il nome di accesso dell'utente, la password e la porta di connessione. L'indirizzo della risorsa Web viene inoltre modificato in caratteri minuscoli.

Rispetto al funzionamento dei componenti della protezione, lo scopo della normalizzazione degli indirizzi delle risorse Web è evitare di eseguire più di una volta la scansione di indirizzi di siti Web che possono presentare differenze a livello di sintassi pur essendo fisicamente equivalenti.

Esempio:

Forma non normalizzata di un indirizzo: www.example.com\.

Forma normalizzata di un indirizzo: www.example.com.

Gruppo di amministrazione

Un set di dispositivi che condividono funzioni comuni e un set di applicazioni Kaspersky installate. I dispositivi vengono raggruppati in modo da poterli gestire facilmente come una singola unità. Un gruppo può includere altri gruppi. È possibile creare criteri di gruppo e attività di gruppo per ogni applicazione installata nel gruppo.

IOC

Indicatore di compromissione. Una serie di dati su un oggetto o un'attività dannosi.

Light Agent

Componente Kaspersky Endpoint Security for Virtualization Light Agent. Viene installato in ogni macchina virtuale da proteggere.

Maschera

Rappresentazione di un nome file e di un'estensione tramite caratteri jolly.

Le maschere di file possono contenere qualsiasi carattere consentito nei nomi dei file, inclusi caratteri speciali:

- Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.

- Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida. La maschera ** è disponibile solo per la creazione delle esclusioni dalla scansione.

- Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

Network Agent

Componente di Kaspersky Security Center che consente l'interazione tra l'Administration Server e le applicazioni Kaspersky installate in uno specifico nodo di rete (workstation o server). Questo componente è comune a tutte le applicazioni Kaspersky con sistema operativo Windows. Le versioni dedicate di Network Agent sono destinate alle applicazioni con altri sistemi operativi.

Oggetto OLE

Un file allegato o un file incorporato in un altro file. Le applicazioni Kaspersky consentono di esaminare gli oggetti OLE per verificare la presenza di eventuali virus. Se ad esempio si inserisce una tabella di Microsoft Office Excel® in un documento di Microsoft Office Word, tale tabella viene esaminata come oggetto OLE.

OpenIOC

Standard aperto di descrizioni degli indicatori di compromissione (IOC) basato su XML e che include oltre 500 diversi indicatori di compromissione.

Portable File Manager

Questa applicazione fornisce un'interfaccia per l'utilizzo dei file criptati nelle unità rimovibili quando non è disponibile alcuna funzionalità di criptaggio nel computer.

Server di integrazione

Componente Kaspersky Endpoint Security for Virtualization Light Agent. Interagisce tra i componenti di Kaspersky Endpoint Security e l'infrastruttura virtuale.

SVM

Macchina virtuale protetta: una macchina virtuale speciale in cui è installato il servizio scanserver (server di protezione, un componente di Kaspersky Endpoint Security for Virtualization Light Agent).

Trusted Platform Module

Un microchip sviluppato per fornire funzioni di sicurezza di base (ad esempio, per l'archiviazione di chiavi di criptaggio). Un Trusted Platform Module in genere è installato nella scheda madre del computer e interagisce con tutti gli altri componenti del sistema tramite il bus hardware.

Appendici

Questa sezione contiene informazioni integrative rispetto al corpo del documento.

Appendice 1. Impostazioni applicazione

È possibile utilizzare un criterio, attività o l'interfaccia dell'applicazione per configurare Kaspersky Endpoint Security. Informazioni dettagliate sui componenti dell'applicazione sono disponibili nelle sezioni corrispondenti.

Protezione minacce file

Il componente Protezione minacce file consente di impedire l'infezione del file system del computer. Per impostazione predefinita, il componente Protezione minacce file risiede permanentemente nella RAM del computer ed esegue la scansione di tutti i file aperti, salvati e avviati in tempo reale. Questo componente esegue la scansione dei file in tutte le unità del computer, incluse le unità collegate. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica.

Il componente esegue la scansione dei file a cui l'utente o l'applicazione ha eseguito l'accesso. Se viene rilevato un file dannoso, Kaspersky Endpoint Security blocca l'esecuzione del file. L'applicazione quindi disinfetta o elimina il file dannoso, a seconda delle impostazioni del componente Protezione minacce file.

Quando si tenta di accedere a un file i cui contenuti risiedono nell'archivio cloud OneDrive, Kaspersky Endpoint Security scarica ed esamina i contenuti dei file.

Impostazioni del componente Protezione minacce file

Parametro	Descrizione
Livello di sicurezza *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Per Protezione minacce file, Kaspersky Endpoint Security può applicare diversi gruppi di impostazioni. I gruppi di impostazioni archiviate nell'applicazione sono denominati *livelli di protezione*: • **Alto**. Quando si seleziona questo livello di sicurezza dei file, il componente Protezione minacce file esegue il controllo più approfondito di tutti i file aperti, salvati e avviati. Il componente Protezione minacce file esamina tutti i tipi di file in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer. Vengono inoltre esaminati archivi, pacchetti di installazione e oggetti OLE incorporati. • **Consigliato**. Questo livello di sicurezza dei file è consigliato dagli esperti di Kaspersky Lab. Il componente Protezione minacce file esamina solo i formati di file specificati in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer, oltre agli oggetti OLE incorporati. Il componente Protezione minacce file non esamina gli archivi o i pacchetti di installazione. • **Basso**. Le impostazioni di questo livello di sicurezza dei file garantiscono la massima velocità di scansione. Il componente Protezione minacce file esamina solo i file con determinate estensioni in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer. Il componente Protezione minacce file non esamina i file compositi.
Tipi di file *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	**Tutti i file**. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina tutti i file senza eccezioni (tutti i formati e le estensioni). **File esaminati per formato**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Prima di esaminare un file alla ricerca di codice dannoso, viene analizzata l'intestazione interna del file per determinarne il formato (ad esempio, .txt, .doc o .exe). La scansione cerca inoltre i file con estensioni file particolari. **File esaminati per estensione**. Se questa impostazione è abilitata, l'applicazione esamina solo i file infettabili. Il formato del file viene quindi determinato in base all'estensione.
Ambito della scansione	Contiene gli oggetti che sono esaminati dal componente Protezione minacce file. Un oggetto da esaminare può essere un disco rigido, un'unità rimovibile, un'unità di rete, una cartella, un file o più file definiti da una maschera. Per impostazione predefinita, il componente Protezione minacce file esamina i file avviati in tutti i dischi rigidi, le unità rimovibili o le unità di rete. L'ambito di protezione per questi oggetti non può essere modificato o eliminato. È possibile escludere solo un oggetto (ad esempio unità rimovibili) dalle scansioni.

Parametro	Descrizione
Machine Learning e analisi delle firme *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Il metodo Machine Learning e analisi delle firme utilizza i database di Kaspersky Endpoint Security, che contengono le descrizioni delle minacce conosciute, nonché i metodi per neutralizzarle. La protezione che utilizza questo metodo fornisce il livello di sicurezza minimo accettabile. In base ai suggerimenti degli esperti Kaspersky, il metodo Machine Learning e analisi delle firme è sempre abilitato.
Analisi euristica *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto. Durante la scansione dei file alla ricerca di codice dannoso, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.
Azione se viene rilevata una minaccia	**Disinfetta (se non è possibile, elimina)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato. **Disinfetta (se non è possibile, blocca)**. Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, l'applicazione blocca questo file. **Blocca**. Se questa opzione è selezionata, l'applicazione blocca automaticamente il file infetto senza tentare di disinfettarlo o eliminarlo. Prima di tentare di disinfettare o eliminare un file infetto, l'applicazione crea una copia di backup del file nel caso in cui sia necessario ripristinare il file o se può essere disinfettato in futuro.
Esamina solo i file nuovi e modificati	Esamina solo i nuovi file e i file che sono stati modificati dopo l'ultima scansione. Questo consente di ridurre la durata di una scansione. Questa modalità si applica sia ai file semplici che compositi.
Esamina gli archivi	Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio).
Esamina i pacchetti di distribuzione	Scansione dei pacchetti di distribuzione delle applicazioni di terze parti.
Esamina i file nei formati Microsoft Office	Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE. L'applicazione analizza i file in formato Office di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Esamina i file in formato e-mail	Scansiona i file in formato e-mail. L'applicazione esegue la scansione dei file MSG ed EML. I file in formato e-mail includono anche gli oggetti OLE e i file MHT. Kaspersky Endpoint Security analizza i file in formato e-mail di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Non decomprimere i file compositi di grandi dimensioni	Se la casella di controllo è selezionata, l'applicazione non esegue la scansione dei file compositi se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, l'applicazione esamina i file compositi di qualsiasi dimensione. L'applicazione esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.

Parametro	Descrizione
Decomprimi file compositi in background	Se la casella di controllo è selezionata, l'applicazione consente di accedere ai file compositi di dimensioni superiori al valore specificato prima della scansione dei file. In questo caso, Kaspersky Endpoint Security decomprime ed esamina i file compositi in background. L'applicazione consente di accedere ai file compositi di dimensioni inferiori a questo valore solo dopo la decompressione e la scansione dei file. Se la casella di controllo non è selezionata, l'applicazione consente di accedere ai file compositi solo dopo la decompressione e la scansione di file di qualsiasi dimensione.
Modalità di scansione *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Kaspersky Endpoint Security esegue la scansione dei file a cui accede l'utente, il sistema operativo o un'applicazione in esecuzione con l'account dell'utente. **Modalità Smart**. In questa modalità Protezione minacce file esamina un oggetto in base a un'analisi delle azioni eseguite sull'oggetto. Ad esempio, quando si utilizza un documento di Microsoft Office, Kaspersky Endpoint Security esegue la scansione del file quando viene aperto per la prima volta e chiuso per l'ultima volta. Le operazioni intermedie di sovrascrittura del file non ne determinano la scansione. **In fase di accesso e modifica**. In questa modalità Protezione minacce file esamina gli oggetti in caso di tentativo di apertura o modifica. **In fase di accesso**. In questa modalità Protezione minacce file esamina gli oggetti solo in caso di tentativo di apertura. **In fase di esecuzione**. In questa modalità Protezione minacce file esamina gli oggetti solo in caso di tentativo di esecuzione.
Usa Tecnologia iSwift *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iSwift è un miglioramento della tecnologia iChecker per il file system NTFS.
Usa Tecnologia iChecker *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalle scansioni utilizzando uno speciale algoritmo che tiene conto della data di rilascio dei database di Kaspersky Endpoint Security, della data dell'ultima scansione del file e di eventuali modifiche delle impostazioni di scansione. La tecnologia iChecker presenta tuttavia alcune limitazioni: non risulta efficace con i file di grandi dimensioni e si applica solo ai file con una struttura riconosciuta dall'applicazione (ad esempio, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP e RAR).
Sospendi Protezione minacce file *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Il funzionamento di Protezione minacce file viene temporaneamente e automaticamente sospeso all'ora specificata o quando si utilizzano le applicazioni specificate.
Scansione delle operazioni sui file eseguite nei contenitori Windows	Se viene rilevata una minaccia all'interno di un contenitore, l'applicazione applica l'azione selezionata per il componente Protezione minacce file. **Arresta il contenitore se la disinfezione non riesce**. L'applicazione potrebbe non disporre di diritti di lettura e scrittura sufficienti per l'oggetto rilevato. In tal caso, la disinfezione o l'eliminazione dell'oggetto rilevato non è possibile. Se questa casella di controllo è selezionata, l'applicazione blocca l'oggetto rilevato e arresta il contenitore. Se questa casella di controllo è deselezionata, l'applicazione blocca solo l'oggetto rilevato. **Non eseguire la scansione delle operazioni sui file eseguiti nei contenitori Windows**. Se la casella di controllo è selezionata, l'applicazione esegue la scansione del contenitore solo all'avvio del contenitore. Se la casella di controllo è deselezionata, l'applicazione esegue la scansione del contenitore costantemente in tempo reale.

Protezione minacce Web

Il componente Protezione minacce Web impedisce il download di file dannosi da Internet e blocca inoltre la connessione a siti Web dannosi e di phishing. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica.

Kaspersky Endpoint Security esamina il traffico HTTP, HTTPS e FTP. Kaspersky Endpoint Security esamina URL e indirizzi IP.

Per utilizzare Protezione minacce Web, è necessario completare la configurazione iniziale dell'applicazione:

- Per il monitoraggio del traffico HTTPS, abilitare la scansione delle connessioni criptate (abilitata per impostazione predefinita).
- Selezionare le porte che Kaspersky Endpoint Security deve monitorare (per impostazione predefinita, l'applicazione monitora tutte le porte).
- Selezionare le applicazioni il cui traffico si desidera venga monitorato da Kaspersky Endpoint Security. La maggior parte dei browser è già presente nell'elenco delle applicazioni consigliate da Kaspersky. Se il browser non è presente nell'elenco, aggiungerlo manualmente.
- Si consiglia di inoculare lo script per l'interazione con le pagine Web nel traffico Web (per impostazione predefinita, l'inserimento dello script è disabilitato). Questo script consente la registrazione degli eventi di Protezione minacce Web per il registro eventi dell'applicazione, il registro eventi del sistema operativo e i rapporti.

Quando un utente tenta di aprire un sito Web dannoso o di phishing, Kaspersky Endpoint Security bloccherà l'accesso e mostrerà un avviso.

Impostazioni del componente Protezione minacce Web

Parametro	Descrizione
Livello di sicurezza *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Per Protezione minacce Web, l'applicazione può applicare diversi gruppi di impostazioni. I gruppi di impostazioni archiviate nell'applicazione sono denominati *livelli di protezione*: • **Alto**. Il livello di sicurezza in cui il componente Protezione minacce Web esegue la massima scansione del traffico Web ricevuto dal computer tramite i HTTP e FTP. Protezione minacce Web esegue la scansione dettagliata di tutti gli oggetti del traffico Web, utilizzando l'intero set di database dell'applicazione, ed esegue l'analisi euristica più approfondita possibile. • **Consigliato**. Questo livello di sicurezza assicura l'equilibrio ottimale tra le prestazioni dell'applicazione e la sicurezza del traffico Web. Il componente Protezione minacce Web esegue l'analisi euristica al livello di scansione Media. Questo livello di sicurezza del traffico Web è consigliato dagli specialisti di Kaspersky. • **Basso**. Le impostazioni di questo livello di sicurezza assicurano la massima velocità di scansione del traffico Web. Il componente Protezione minacce Web esegue l'analisi euristica al livello di scansione superficiale.
Azione se viene rilevata una minaccia	**Blocca**. Se questa opzione è selezionata e viene rilevato un oggetto infetto nel traffico Web, il componente Protezione minacce Web blocca l'accesso all'oggetto e visualizza un messaggio nel browser. **Informa**. Se questa opzione è selezionata e un oggetto infetto viene rilevato nel traffico Web, Kaspersky Endpoint Security consente il download di questo oggetto nel computer ma aggiunge informazioni sull'oggetto infetto all'elenco delle minacce attive.
Verifica l'indirizzo Web a fronte del database degli indirizzi Web dannosi *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	La scansione dei collegamenti per determinare se sono inclusi nel database degli indirizzi Web dannosi consente di tenere traccia dei siti Web che sono stati aggiunti alla lista vietati. Il database degli indirizzi Web dannosi è gestito da Kaspersky è incluso nel pacchetto di installazione dell'applicazione e viene aggiornato durante gli aggiornamenti del database di Kaspersky Endpoint Security.
Usa l'analisi euristica *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto. Quando il traffico Web viene esaminato alla ricerca di virus e altre applicazioni che costituiscono una minaccia, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.

Parametro	Descrizione
Verifica l'indirizzo Web a fronte del database degli indirizzi Web di phishing *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Il database degli indirizzi Web di phishing include gli indirizzi Web dei siti Web attualmente noti utilizzati per generare attacchi di phishing. Kaspersky integra questo database dei collegamenti di phishing con gli indirizzi ottenuti dall'organizzazione internazionale nota come Anti-Phishing Working Group. Il database degli indirizzi di phishing è incluso nel pacchetto di installazione dell'applicazione e viene integrato dagli aggiornamenti del database di Kaspersky Endpoint Security.
Non esaminare il traffico Web per gli indirizzi Web attendibili	Se questa opzione di controllo è selezionata, il componente Protezione minacce Web non esegue la scansione del contenuto delle pagine Web o dei siti Web i cui indirizzi sono inclusi nell'elenco degli indirizzi Web attendibili. È possibile aggiungere sia l'indirizzo specifico che una maschera di indirizzi di una pagina Web o un sito Web all'elenco degli indirizzi Web attendibili. È inoltre possibile creare un elenco generale di esclusioni per le connessioni criptate. In questo caso, Kaspersky Endpoint Security non esamina il traffico HTTPS degli indirizzi Web attendibili quando i componenti Protezione minacce Web, Protezione minacce di posta e Controllo Web sono in esecuzione.

Protezione minacce di posta

Il componente Protezione minacce di posta esamina gli allegati dei messaggi e-mail in entrata e in uscita alla ricerca di virus e altre minacce. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica.

Protezione minacce di posta può eseguire la scansione sia dei messaggi in entrata che di quelli in uscita. L'applicazione supporta POP3, SMTP, IMAP e NNTP nei seguenti client di posta:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Per eseguire la scansione del traffico nei client di posta Thunderbird, MyOffice Mail e R7-Office Organizer, è necessario aggiungere il certificato Kaspersky all'archivio certificati e selezionare il proprio archivio certificati.

Protezione minacce di posta non supporta altri protocolli e client di posta.

Protezione minacce di posta potrebbe non essere sempre in grado di ottenere l'accesso a *livello di protocollo* ai messaggi (ad esempio, quando si utilizza la soluzione Microsoft Exchange). Per questo motivo, Protezione minacce di posta include un'estensione per Microsoft Office Outlook. L'estensione consente la scansione dei messaggi al *livello del client di posta*. L'estensione Protezione minacce di posta supporta le versioni a 32 bit e a 64 bit di Outlook 2010, 2013, 2016, 2019, 2021, 2024 e 365. Nei computer basati su Arm l'estensione Protezione minacce di posta supporta le versioni a 32 bit e a 64 bit di Outlook 2016, Outlook 2021, Outlook 2024 e Outlook 365 per Arm64.

Il componente Protezione minacce di posta non esegue la scansione dei messaggi se il client di posta è aperto in un browser.

Quando viene rilevato un file dannoso in un allegato, Kaspersky Endpoint Security aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*.

Parametro	Descrizione
Livello di sicurezza *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Per Protezione minacce di posta, l'applicazione può applicare diversi gruppi di impostazioni. I gruppi di impostazioni archiviate nell'applicazione sono denominati *livelli di protezione*: • **Alto**. Quando questo livello di sicurezza dei messaggi e-mail è selezionato, il componente Protezione minacce di posta esamina i messaggi e-mail in modo più approfondito. Il componente Protezione minacce di posta esamina i messaggi e-mail in entrata e in uscita ed esegue l'analisi euristica in modo approfondito. Il livello di sicurezza di posta Alto è consigliato per gli ambienti ad alto rischio. Un esempio di ambiente di questo tipo è rappresentato da una connessione a un servizio di posta elettronica gratuito da una rete domestica priva di protezione centralizzata della posta elettronica. • **Consigliato**. Il livello di sicurezza e-mail che assicura un equilibrio ottimale tra le prestazioni dell'applicazione e la sicurezza della posta elettronica. Il componente Protezione minacce di posta esamina i messaggi e-mail in entrata e in uscita ed esegue l'analisi euristica di livello medio. Questo livello di sicurezza del traffico e-mail è consigliato dagli specialisti di Kaspersky. • **Basso**. Quando si seleziona questo livello di sicurezza, il componente Protezione minacce di posta esamina solo i messaggi e-mail in entrata, esegue l'analisi euristica in modo superficiale e non esamina gli archivi allegati ai messaggi e-mail. A questo livello di sicurezza e-mail, Protezione minacce di posta esamina i messaggi e-mail con la massima velocità e con il minimo utilizzo di risorse del sistema operativo. Il livello di sicurezza Basso è consigliato quando si lavora in un ambiente protetto in modo affidabile. Un esempio di ambiente di questo tipo è rappresentato da una rete LAN aziendale con protezione centralizzata della posta elettronica.
Azione se viene rilevata una minaccia	**Disinfetta (se non è possibile, elimina)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata o in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione elimina l'oggetto infetto. L'applicazione aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*. **Disinfetta (se non è possibile, blocca)**. Quando un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Quando un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. Se l'oggetto non può essere disinfettato, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore. **Blocca**. Se un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Se un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.
Ambito della protezione *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	L'*ambito della protezione* include gli oggetti che il componente controlla durante l'esecuzione: Messaggi in entrata e in uscita o Solo messaggi in entrata. Per proteggere i computer, è sufficiente esaminare i messaggi in entrata. È possibile attivare la scansione dei messaggi in uscita per impedire l'invio dei file infetti negli archivi. È inoltre possibile attivare la scansione dei messaggi in uscita se si desidera impedire l'invio di file di determinati formati, ad esempio file audio e video.
Esegui scansione traffico POP3, SMTP, NNTP e IMAP	Scansione da parte del componente Protezione minacce di posta del traffico trasferito tramite i protocolli POP3, SMTP, NNTP e IMAP.
Connetti estensione Microsoft Outlook	Se la casella di controllo è selezionata, la scansione dei messaggi e-mail trasmessi tramite i protocolli POP3, SMTP, NNTP, IMAP è abilitata per l'estensione integrata in Microsoft Outlook. Se viene eseguita la scansione dei messaggi tramite l'estensione per Microsoft Outlook, è consigliabile utilizzare Cached Exchange Mode. Per informazioni più dettagliate sulla Modalità cache e per raccomandazioni sul relativo utilizzo, fare riferimento alla Microsoft Knowledge Base.
Analisi euristica *(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)*	Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto. Durante la scansione dei file alla ricerca di codice dannoso, l'analizzatore euristico esegue le istruzioni nei file eseguibili. Il numero di istruzioni eseguite dall'analizzatore euristico dipende dal livello specificato per l'analizzatore euristico. Il livello di analisi euristica garantisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e la durata dell'analisi euristica.

Parametro	Descrizione
Esamina gli archivi allegati	Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio). Se durante la scansione l'applicazione rileva una password per un archivio nel testo del messaggio, tale password verrà utilizzata per analizzare il contenuto dell'archivio alla ricerca di applicazioni dannose. In questo caso, la password non viene salvata. Un archivio viene decompresso durante la scansione. Se si verifica un errore dell'applicazione durante il processo di decompressione, è possibile eliminare manualmente i file decompressi che vengono salvati nel percorso seguente: %systemroot%\temp. I file hanno il prefisso PR.
Esamina i file allegati nei formati Microsoft Office	Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE. L'applicazione analizza i file in formato Office di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Non esaminare archivi superiori a N MB	Se la casella di controllo è selezionata, il componente Protezione minacce di posta esclude dalla scansione gli archivi allegati ai messaggi e-mail se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, il componente Protezione minacce di posta esamina gli archivi allegati ai messaggi e-mail di qualsiasi dimensione.
Limita il tempo per il controllo degli archivi a N sec	Se la casella di controllo è selezionata, il tempo allocato per la scansione degli archivi allegati ai messaggi e-mail è limitato al periodo specificato.
Filtro allegati	Il filtro allegati non viene applicato ai messaggi e-mail in uscita. **Disabilita il filtro**. Se questa opzione è selezionata, il componente Protezione minacce di posta non filtra i file allegati ai messaggi e-mail. **Rinomina allegati dei tipi selezionati**. Se questa opzione è selezionata, il componente Protezione minacce di posta sostituirà l'ultimo carattere dell'estensione rilevato nei file allegati dei tipi specificati con il carattere di sottolineatura (ad esempio allegato.doc_). Per aprire il file l'utente deve quindi rinominare il file. **Elimina allegati dei tipi selezionati**. Se questa opzione è selezionata, il componente Protezione minacce di posta elimina i file allegati dei tipi specificati dai messaggi e-mail. Nell'elenco delle maschere di file è possibile specificare i tipi di file allegati da rinominare o eliminare dai messaggi e-mail.

Protezione minacce di rete

Il componente *Protezione minacce di rete* (chiamato anche Intrusion Detection System, IDS) monitora il traffico di rete in entrata per verifiche le caratteristiche delle attività degli attacchi di rete. Quando l'applicazione rileva un tentativo di attacco di rete nel computer dell'utente, blocca la connessione di rete con il computer che ha originato l'attacco. Nei database dell'applicazione è inclusa una descrizione degli attacchi di rete attualmente conosciuti, nonché dei metodi utilizzati per contrastarli. L'elenco degli attacchi di rete che il componente Protezione minacce di Rete è in grado di rilevare viene aggiornato durante gli aggiornamenti dei database e dei moduli dell'applicazione.

Parametro	Descrizione
Considera la scansione delle porte e il flooding di rete come attacchi	Il *flooding di rete* è un attacco alle risorse di rete di un'organizzazione (come i server Web). Questo attacco consiste nell'invio di un gran numero di richieste per sovraccaricare la larghezza di banda delle risorse di rete. Quando ciò accade, gli utenti non sono in grado di accedere alle risorse di rete dell'organizzazione. Un attacco di *scansione delle porte* consiste nella scansione di porte UDP, TCP e servizi di rete nel computer. Questo attacco consente all'autore dell'attacco di identificare il grado di vulnerabilità del computer prima di eseguire tipi più pericolosi di attacchi di rete. La scansione delle porte consente inoltre all'autore dell'attacco di identificare il sistema operativo nel computer e selezionare gli attacchi di rete appropriati per tale sistema operativo. Se questa casella di controllo è selezionata, Kaspersky Endpoint Security monitora il traffico di rete per rilevare tali attacchi. Se viene rilevato un attacco, l'applicazione avvisa l'utente e invia l'evento corrispondente a Kaspersky Security Center. L'applicazione fornisce informazioni sul computer che ha originato l'attacco, necessarie per azioni tempestive di risposta alle minacce. È possibile disabilitare il rilevamento di questi tipi di attacchi nel caso in cui alcune delle applicazioni consentite eseguano operazioni tipiche di queste tipologie di attacchi. Ciò contribuirà a evitare falsi allarmi.
Blocca dispositivi che hanno originato l'attacco per N min	Se l'opzione è abilitata, il componente Protezione minacce di rete aggiunge il computer che ha originato l'attacco all'elenco di computer bloccati. In altre parole, il componente Protezione minacce di rete blocca la connessione di rete con il computer che ha originato l'attacco dopo il primo tentativo di un attacco di rete per il periodo di tempo specificato. Questo blocco protegge automaticamente il computer dell'utente da ulteriori possibili attacchi di rete dallo stesso indirizzo. Il tempo minimo che un computer che ha originato l'attacco deve trascorrere nell'elenco dei blocchi è di un minuto. Il tempo massimo è 999 minuti. È possibile visualizzare l'elenco dei blocchi nella finestra dello strumento Monitor di rete. Kaspersky Endpoint Security cancella l'elenco dei blocchi al riavvio dell'applicazione e quando le impostazioni di Protezione minacce di rete vengono modificate.
Esclusioni	L'elenco contiene gli indirizzi IP da cui Protezione minacce di rete non blocca gli attacchi di rete. È possibile aggiungere un indirizzo IP con porta e protocollo specificati. L'applicazione non registra le informazioni sugli attacchi di rete dagli indirizzi IP che fanno parte dell'elenco delle esclusioni.
Protezione dallo spoofing MAC	Un *attacco di spoofing MAC* consiste nella modifica dell'indirizzo MAC di un dispositivo di rete (scheda di rete). L'autore di un attacco può quindi reindirizzare i dati inviati a un dispositivo a un altro dispositivo e ottenere l'accesso a questi dati. Kaspersky Endpoint Security consente di bloccare gli attacchi di spoofing MAC e di ricevere notifiche sugli attacchi.

Firewall

Il componente Firewall blocca le connessioni non autorizzate al computer in Internet o sulla rete locale. Firewall controlla anche l'attività di rete delle applicazioni nel computer. Questo consente di proteggere la LAN aziendale dal furto di identità e da altri attacchi. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e *regole di rete* predefinite.

Network Agent viene utilizzato per l'interazione con Kaspersky Security Center. Firewall crea automaticamente le regole di rete necessarie per il funzionamento dell'applicazione e di Network Agent. Successivamente Firewall apre diverse porte nel computer. Le porte aperte dipendono dal ruolo del computer (ad esempio il ruolo di punto di distribuzione). Per ulteriori informazioni sulle porte che verranno aperte nel computer, consultare la Guida di Kaspersky Security Center.

Regole di rete

È possibile configurare le regole di rete ai seguenti livelli:

- *Regole per i pacchetti di rete*. Le regole per i pacchetti di rete applicano restrizioni ai pacchetti di rete, indipendentemente dall'applicazione. Le regole di questo tipo limitano il traffico di rete in entrata e in uscita tramite specifiche porte del protocollo dati selezionato. Kaspersky Endpoint Security ha regole predefinite per i pacchetti di rete con autorizzazioni consigliate dagli esperti di Kaspersky.

- *Regole di rete dell'applicazione*. Le regole di rete dell'applicazione applicano restrizioni all'attività di rete per una specifica applicazione. Tengono conto non solo delle caratteristiche del pacchetto di rete, ma anche della specifica applicazione a cui il pacchetto di rete è indirizzato o da cui è stato generato.

L'accesso controllato delle applicazioni alle risorse del sistema operativo, ai processi e ai dati personali viene garantito dal componente Prevenzione Intrusioni Host utilizzando *i diritti delle applicazioni*.

Durante il primo avvio dell'applicazione, Firewall esegue le seguenti azioni:

1. Verifica la sicurezza dell'applicazione utilizzando i database anti-virus scaricati.

2. Verifica la sicurezza dell'applicazione in Kaspersky Security Network.

   È consigliabile partecipare a Kaspersky Security Network per un miglior funzionamento di Firewall.

3. Colloca l'applicazione in uno dei gruppi di attendibilità: *Attendibili*, *Restrizione bassa*, *Restrizione alta*, *Non attendibili*.

   Un gruppo di attendibilità definisce i diritti a cui Kaspersky Endpoint Security fa riferimento durante il controllo delle attività delle applicazioni. Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità in base al livello di pericolosità che l'applicazione può rappresentare per il computer.

   Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità per i componenti Firewall e Prevenzione Intrusioni Host. Non è possibile modificare il gruppo di attendibilità solo per Firewall o Prevenzione Intrusioni Host.

   Se si rifiuta di partecipare a KSN o non è disponibile alcuna rete, Kaspersky Endpoint Security inserisce l'applicazione in un gruppo di attendibilità in base alle impostazioni del componente Prevenzione Intrusioni Host. Dopo la ricezione della reputazione dell'applicazione da KSN, il gruppo di attendibilità può essere modificato automaticamente.

4. Blocca l'attività di rete dell'applicazione in base al gruppo di attendibilità. Ad esempio, alle applicazioni nel gruppo di attendibilità *Restrizione alta* non è consentito l'utilizzo di nessuna connessione di rete.

Al successivo avvio dell'applicazione, Kaspersky Endpoint Security verifica l'integrità dell'applicazione. Se l'applicazione non è stata modificata, il componente utilizza le regole di rete correnti. Se l'applicazione è stata modificata, Kaspersky Endpoint Security la analizza come se si trattasse del primo avvio.

Priorità delle regole di rete

Ogni regola ha una priorità. Più alta è la posizione di una regola nell'elenco, maggiore è la priorità. Se l'attività di rete viene aggiunta a diverse regole, Firewall regola l'attività di rete in base alla regola con la priorità più elevata.

Le regole per i pacchetti di rete hanno una priorità superiore rispetto alle regole di rete per le applicazioni. Se per lo stesso tipo di attività di rete sono specificate sia regole per i pacchetti di rete che regole di rete per le applicazioni, l'attività viene gestita in base alle regole per i pacchetti di rete.

Le regole di rete per le applicazioni funzionano in un modo particolare. La regola di rete per le applicazioni include regole di accesso basate sullo stato della rete: *Rete pubblica*, *Rete locale*, *Rete attendibile*. Ad esempio, per impostazione predefinita per le applicazioni nel gruppo di attendibilità *Restrizione alta* non è autorizzata alcuna attività di rete nelle reti con qualsiasi stato. Se viene specificata una regola di rete per una singola applicazione (applicazione padre), i processi figlio delle altre applicazioni verranno eseguiti in base alla regola di rete dell'applicazione padre. Se non esiste una regola di rete per l'applicazione, i processi figlio verranno eseguiti in base alla regola di accesso alla rete del gruppo di attendibilità dell'applicazione.

Se ad esempio hai vietato qualsiasi attività di rete nelle reti con qualsiasi stato per tutte le applicazioni, ad eccezione del browser X e avvii l'installazione del browser Y (processo figlio) dal browser X (applicazione padre), il programma di installazione del browser Y accederà alla rete e scaricherà i file necessari. Dopo l'installazione, al browser Y verrà negata qualsiasi connessione di rete in base alle impostazioni del firewall. Per vietare l'attività di rete del programma di installazione del browser Y come processo figlio, è necessario aggiungere una regola di rete per il programma di installazione del browser Y.

Tipi di connessioni di rete

Firewall consente di controllare l'attività di rete in base al tipo di connessione di rete. Kaspersky Endpoint Security riceve il tipo di connessione di rete dal sistema operativo del computer. Il tipo di connessione di rete nel sistema operativo viene impostato dall'utente durante la configurazione della connessione. È possibile modificare il tipo di connessione di rete nelle impostazioni di Kaspersky Endpoint Security. Firewall monitorerà l'attività di rete in base al tipo di rete specificato nelle impostazioni di Kaspersky Endpoint Security e non nel sistema operativo.

Sono disponibili i seguenti tipi di connessioni di rete:

- **Rete pubblica**. La rete non è protetta da applicazioni anti-virus, firewall o filtri (ad esempio la rete Wi-Fi di un bar). Quando l'utente utilizza un computer connesso a una rete di questo tipo, Firewall blocca l'accesso ai file e alle stampanti del computer in uso. Anche gli utenti esterni non sono in grado di accedere ai dati tramite cartelle condivise e di accedere in remoto al desktop del computer in uso. Firewall filtra l'attività di rete di ogni applicazione in base alle regole di rete impostate per l'applicazione.

  Per impostazione predefinita, Firewall assegna a Internet il tipo *Rete pubblica*. Non è possibile modificare il tipo di Internet.

- **Rete locale**. Rete per utenti con accesso limitato a file e stampanti in questo computer (ad esempio una rete LAN aziendale o una rete domestica).

- **Rete attendibile**. Rete sicura in cui il computer non è esposto ad attacchi o a tentativi di accesso non autorizzato ai dati. Per le reti di questa categoria, Firewall consente qualsiasi attività di rete.

Impostazioni del componente Firewall

Parametro	Descrizione
Regole per i pacchetti	Tabella con un elenco delle regole per i pacchetti di rete. Le regole per i pacchetti di rete vengono utilizzate per applicare restrizioni ai pacchetti di rete, indipendentemente dall'applicazione. Le regole di questo tipo limitano il traffico di rete in entrata e in uscita tramite specifiche porte del protocollo dati selezionato. Nella tabella sono elencate le regole per i pacchetti di rete preconfigurate, consigliate da Kaspersky per una protezione ottimale del traffico di rete dei computer con sistema operativo Microsoft Windows. Firewall imposta la priorità di esecuzione per ogni regola per i pacchetti di rete. Firewall elabora le regole per i pacchetti di rete nell'ordine in cui compaiono nell'elenco delle regole per i pacchetti di rete, dalla prima all'ultima. Firewall individua la regola per i pacchetti di rete più adatta alla connessione di rete e la applica, consentendo o bloccando l'attività di rete. Firewall ignora quindi tutte le successive regole per i pacchetti di rete per la connessione di rete specifica. Le regole per i pacchetti di rete hanno una priorità superiore rispetto alle regole di rete per le applicazioni.
Reti disponibili	Questa tabella contiene informazioni sulle connessioni di rete rilevate da Firewall sul computer. La categoria *Rete pubblica* viene assegnata a Internet per impostazione predefinita. Non è possibile modificare la categoria di Internet.
Regole per le applicazioni	**Applicazione**. Tabella delle applicazioni controllate dal componente Firewall. Le applicazioni sono assegnate ai gruppi di attendibilità. Un gruppo di attendibilità definisce i diritti utilizzati da Kaspersky Endpoint Security durante il controllo dell'attività di rete delle applicazioni. È possibile selezionare un'applicazione da un singolo elenco di tutte le applicazioni installate nei computer sotto l'influenza di un criterio e aggiungere l'applicazione a un gruppo di attendibilità. **Regole di rete**. Tabella delle regole di rete per le applicazioni che fanno parte di un gruppo di attendibilità. Firewall gestisce le attività di rete delle applicazioni in base a queste regole. La tabella visualizza le regole di rete predefinite consigliate dagli esperti di Kaspersky. Queste regole di rete sono state aggiunte per proteggere in modo ottimale il traffico di rete dei computer che eseguono sistemi operativi Windows. Non è possibile eliminare le regole di rete predefinite.

Prevenzione Attacchi BadUSB

Alcuni virus modificano il firmware dei dispositivi USB per indurre il sistema operativo a rilevare il dispositivo USB come una tastiera. Di conseguenza, il virus potrebbe eseguire comandi con l'account dell'utente per scaricare malware, ad esempio.

Il componente Prevenzione Attacchi BadUSB impedisce la connessione al computer di dispositivi USB infetti che emulano una tastiera.

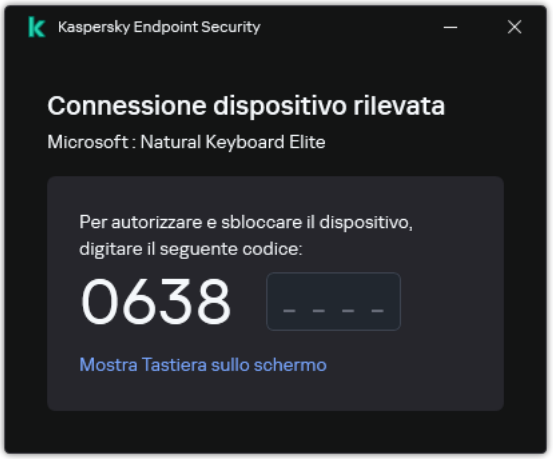
Quando un dispositivo USB viene connesso al computer e identificato dal sistema operativo come una tastiera, l'applicazione richiede all'utente di immettere un codice numerico generato dall'applicazione da questa tastiera o utilizzando Tastiera sullo schermo (vedere la figura di seguito). Questa procedura è denominata autorizzazione della tastiera.

Se il codice è stato immesso correttamente, l'applicazione salva i parametri di identificazione (VID/PID della tastiera e numero della porta a cui è stata connessa) nell'elenco delle tastiere autorizzate. L'autorizzazione delle tastiera non deve essere ripetuta quando la tastiera viene connessa di nuovo o dopo il riavvio del sistema operativo.

Quando la tastiera autorizzata viene connessa a una diversa porta USB del computer, l'applicazione visualizza nuovamente una richiesta di autorizzazione della tastiera.

Se il codice numerico è stato immesso in modo errato, l'applicazione genera un nuovo codice. È possibile configurare il numero di tentativi di immissione del codice numerico. Se il codice numerico viene immesso più volte in modo errato o la finestra dell'autorizzazione della tastiera viene chiusa (vedere la figura riportata di seguito), l'applicazione blocca l'input dalla tastiera. Quando la durata di blocco del dispositivo USB termina o il sistema operativo viene riavviato, l'applicazione richiede all'utente di eseguire nuovamente l'autorizzazione della tastiera.

L'applicazione consente l'utilizzo di una tastiera autorizzata e blocca una tastiera che non è stata autorizzata.



Autorizzazione tastiera

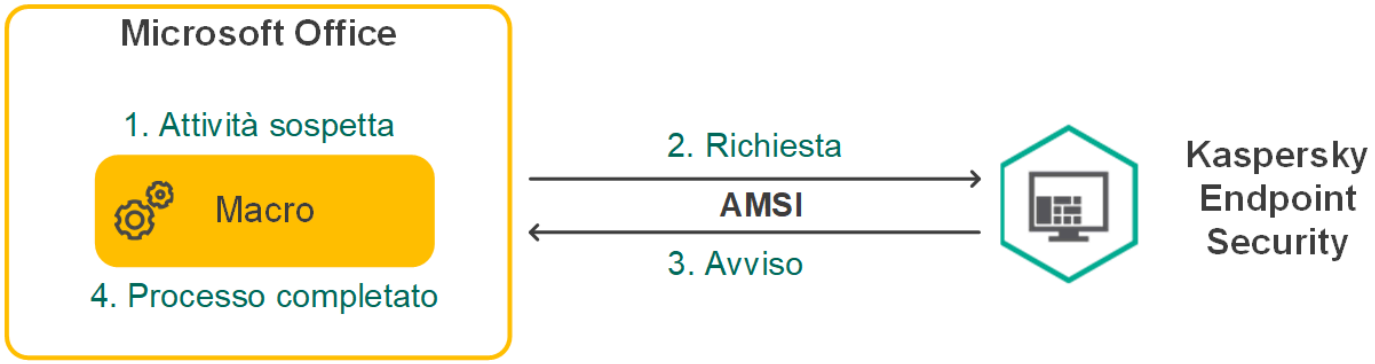
Impostazioni del componente Prevenzione Attacchi BadUSB

Parametro	Descrizione
Impedisci l'utilizzo di Tastiera sullo schermo per l'autorizzazione di dispositivi USB	Se l'interruttore è attivato, l'applicazione impedisce di utilizzare la Tastiera sullo schermo per l'autorizzazione di un dispositivo USB da cui non è possibile immettere un codice di autorizzazione.
Impedisci l'utilizzo di un codice a barre per l'autorizzazione di dispositivi USB	Se l'interruttore è abilitato, l'applicazione non mostra il codice a barre nella notifica di autenticazione dello scanner di codici a barre.
Numero massimo di tentativi di autorizzazione del dispositivo USB	Blocco automatico del dispositivo USB se il codice di autorizzazione viene immesso in modo errato per il numero di volte specificato. I valori validi sono compresi tra 1 e 10. Ad esempio, se si consentono cinque tentativi di immissione del codice di autorizzazione, l'applicazione blocca il dispositivo USB dopo il quinto tentativo non riuscito. Kaspersky Endpoint Security mostra la durata del blocco per il dispositivo USB. Trascorso questo tempo, sono di nuovo disponibili cinque tentativi di immissione del codice di autorizzazione.
Timeout al raggiungimento del numero massimo di tentativi	Durata del blocco del dispositivo USB dopo il numero specificato di tentativi non riusciti di immissione del codice di autorizzazione. I valori validi sono compresi tra 1 e 180 (minuti).

Protezione AMSI

Il componente Protezione AMSI è progettato per il supporto dell'interfaccia AMSI (Antimalware Scan Interface) di Microsoft. *AMSI (Antimalware Scan Interface)* consente ad applicazioni di terzi con il supporto AMSI di inviare oggetti (ad esempio script di PowerShell) a Kaspersky Endpoint Security per un'ulteriore analisi e quindi di ricevere i risultati della scansione di questi oggetti. Tra le applicazioni di terzi possono essere incluse, ad esempio, le applicazioni Microsoft Office (vedere la figura di seguito). Per informazioni dettagliate su AMSI, consultare la documentazione di Microsoft.

Protezione AMSI è solo in grado di rilevare una minaccia e di informare un'applicazione di terzi della minaccia rilevata. Dopo la ricezione di una notifica di minaccia, un'applicazione di terzi non consente azioni dannose (ad esempio arresti).



Esempio di funzionamento del Provider di protezione AMSI

Il componente Protezione AMSI può rifiutare una richiesta da un'applicazione di terzi, ad esempio se questa applicazione supera il numero massimo di richieste all'interno di un intervallo di tempo specificato. Kaspersky Endpoint Security invia le informazioni su una richiesta rifiutata da un'applicazione di terzi ad Administration Server. Il componente Protezione AMSI non nega le richieste provenienti dalle applicazioni di terzi per cui è abilitata l'integrazione continua con il componente Protezione AMSI.

Protezione AMSI è disponibile per i seguenti sistemi operativi per workstation e server:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessione;
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-sessione;
- Windows Server 2016 Essentials / Standard / Datacenter (inclusa la modalità Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (inclusa la modalità Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (inclusa la modalità Server Core);
- Windows Server 2025 Standard / Datacenter.

Impostazioni di protezione AMSI

Parametro	Descrizione
Esamina gli archivi	Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio).
Esamina i pacchetti di distribuzione	Scansione dei pacchetti di distribuzione delle applicazioni di terze parti.
Esamina i file nei formati Microsoft Office	Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE. L'applicazione analizza i file in formato Office di dimensioni inferiori a 1 MB, indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Non decomprimere i file compositi di grandi dimensioni	Se la casella di controllo è selezionata, l'applicazione non esegue la scansione dei file compositi se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, l'applicazione esamina i file compositi di qualsiasi dimensione. L'applicazione esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.

Prevenzione Exploit

Il componente Prevenzione Exploit rileva il codice del programma che sfrutta le vulnerabilità del computer per sfruttare i privilegi di amministratore o eseguire attività dannose. Gli exploit possono ad esempio utilizzare un attacco di overflow del buffer. A tale scopo, l'exploit invia una grande quantità di dati a un'applicazione vulnerabile. Durante l'elaborazione di questi dati, l'applicazione vulnerabile esegue un codice dannoso. In seguito a questo attacco, l'exploit può avviare un'installazione non autorizzata di malware. In caso di tentativo di esecuzione di un file eseguibile da un'applicazione vulnerabile non eseguito dall'utente, Kaspersky Endpoint Security blocca l'esecuzione di questo file o invia una notifica all'utente.

Il componente Prevenzione Exploit consente inoltre di monitorare le porte di rete alla ricerca di processi delle applicazioni che possono minacciare la sicurezza del computer. L'applicazione ottiene informazioni su tali processi con i database anti-virus.

Impostazioni del componente Prevenzione Exploit

Parametro	Descrizione
Al rilevamento di exploit	**Blocca**. Se questo elemento è selezionato, quando viene rilevato un exploit Kaspersky Endpoint Security blocca le operazioni di questo exploit e crea una voce del registro con informazioni sull'exploit. **Informa**. Se questo elemento è selezionato, quando Kaspersky Endpoint Security rileva un exploit registra una voce contenente le informazioni sull'exploit e aggiunge informazioni sull'exploit all'elenco delle minacce attive.
Abilita protezione della memoria dei processi di sistema	Se questo interruttore è attivato, Kaspersky Endpoint Security blocca i processi esterni che tentano di accedere alla memoria dei processi di sistema.

Rilevamento del Comportamento

Il componente Rilevamento del Comportamento riceve dati sulle azioni delle applicazioni nel computer e fornisce tali informazioni ad altri componenti della protezione per migliorarne le prestazioni. Il componente Rilevamento del Comportamento utilizza le firme Behavior Stream Signatures (BSS) per le applicazioni. Se l'attività di un'applicazione corrisponde a uno schema BSS, Kaspersky Endpoint Security esegue l'azione di risposta selezionata. La funzionalità di Kaspersky Endpoint Security basata sugli schemi Behavior Stream Signatures e assicura una difesa proattiva del computer.

Il componente Rilevamento del Comportamento consente inoltre di monitorare le porte di rete alla ricerca di processi delle applicazioni che possono minacciare la sicurezza del computer. L'applicazione ottiene informazioni su tali processi con i database anti-virus.

Impostazioni del componente Rilevamento del Comportamento

Parametro	Descrizione
Azione se viene rilevata un'attività malware	**Elimina**. Se questa opzione è selezionata, al rilevamento di attività dannose Kaspersky Endpoint Security elimina il file eseguibile dell'applicazione dannosa e crea una copia di backup del file in Backup. **Blocca**. Se si seleziona questa opzione, Kaspersky Endpoint Security termina l'applicazione al momento del rilevamento dell'attività dannosa. **Informa**. Se questa opzione è selezionata e vengono rilevate attività dannose di un'applicazione, Kaspersky Endpoint Security non termina questa applicazione ma aggiunge informazioni sulle attività dannose dell'applicazione all'elenco delle minacce attive.

Prevenzione Intrusioni Host

Il componente Prevenzione Intrusioni Host impedisce alle applicazioni di eseguire azioni che possono essere pericolose per il sistema operativo, assicurando il controllo dell'accesso alle risorse del sistema operativo e ai dati personali. Il componente garantisce la protezione del computer mediante database anti-virus e il servizio cloud Kaspersky Security Network.

Il componente controlla l'esecuzione delle applicazioni utilizzando *i diritti delle applicazioni*. I diritti delle applicazioni includono i seguenti parametri di accesso:

- Accesso alle risorse del sistema operativo (ad esempio opzioni di avvio automatico, chiavi di registro)
- Accesso ai dati personali (ad esempio file e applicazioni)

L'attività di rete delle applicazioni è controllata dal componente Firewall mediante le *regole di rete*.

Durante il primo avvio dell'applicazione, il componente Prevenzione Intrusioni Host esegue le seguenti azioni:

1. Verifica la sicurezza dell'applicazione utilizzando i database anti-virus scaricati.
2. Verifica la sicurezza dell'applicazione in Kaspersky Security Network.

   È consigliabile partecipare a Kaspersky Security Network per un miglior funzionamento del componente Prevenzione Intrusioni Host.

3. Colloca l'applicazione in uno dei gruppi di attendibilità: *Attendibili*, *Restrizione bassa*, *Restrizione alta*, *Non attendibili*.

   Un gruppo di attendibilità definisce i diritti a cui Kaspersky Endpoint Security fa riferimento durante il controllo delle attività delle applicazioni. Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità in base al livello di pericolosità che l'applicazione può rappresentare per il computer.

   Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità per i componenti Firewall e Prevenzione Intrusioni Host. Non è possibile modificare il gruppo di attendibilità solo per Firewall o Prevenzione Intrusioni Host.

   Se si rifiuta di partecipare a KSN o non è disponibile alcuna rete, Kaspersky Endpoint Security inserisce l'applicazione in un gruppo di attendibilità in base alle impostazioni del componente Prevenzione Intrusioni Host. Dopo la ricezione della reputazione dell'applicazione da KSN, il gruppo di attendibilità può essere modificato automaticamente.

4. Blocca le azioni dell'applicazione in base al gruppo di attendibilità. Ad esempio, alle applicazioni del gruppo di attendibilità *Restrizione alta* viene negato l'accesso ai moduli del sistema operativo.

Al successivo avvio dell'applicazione, Kaspersky Endpoint Security verifica l'integrità dell'applicazione. Se l'applicazione non è stata modificata, il componente utilizza i diritti delle applicazioni correnti. Se l'applicazione è stata modificata, Kaspersky Endpoint Security la analizza come se si trattasse del primo avvio.

Parametro	Descrizione
Diritti applicazione	Tabella delle applicazioni monitorate dal componente Prevenzione Intrusioni Host. Le applicazioni sono assegnate ai gruppi di attendibilità. Un gruppo di attendibilità definisce i diritti a cui Kaspersky Endpoint Security fa riferimento durante il controllo delle attività delle applicazioni. È possibile selezionare un'applicazione da un singolo elenco di tutte le applicazioni installate nei computer sotto l'influenza di un criterio e aggiungere l'applicazione a un gruppo di attendibilità. I diritti di accesso alle applicazioni sono riportati nelle seguenti tabelle: • **File e Registro di sistema**. Tabella dei diritti di accesso per le risorse del sistema operativo e dei dati personali per le applicazioni appartenenti al gruppo di attendibilità. • **Diritti**. Tabella dei diritti di accesso per i processi e le risorse del sistema operativo per le applicazioni appartenenti al gruppo di attendibilità. • **Regole di rete**. Tabella delle regole di rete per le applicazioni che fanno parte di un gruppo di attendibilità. Firewall gestisce le attività di rete delle applicazioni in base a queste regole. La tabella visualizza le regole di rete predefinite consigliate dagli esperti di Kaspersky. Queste regole di rete sono state aggiunte per proteggere in modo ottimale il traffico di rete dei computer che eseguono sistemi operativi Windows. Non è possibile eliminare le regole di rete predefinite.
Risorse protette	La tabella contiene le risorse del computer suddivise per categoria. Il componente Prevenzione Intrusioni Host monitora i tentativi delle altre applicazioni di accedere alle risorse nella tabella. Le risorse possono essere rappresentate da categorie di registro, file, cartelle o chiavi di registro.
Gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security	Un gruppo di attendibilità in cui Kaspersky Endpoint Security inserirà le applicazioni avviate prima di Kaspersky Endpoint Security.
Aggiorna le regole per le applicazioni precedentemente sconosciute da KSN	Se la casella di controllo è selezionata, il componente Prevenzione Intrusioni Host aggiorna i diritti per le applicazioni precedentemente sconosciute utilizzando il database di Kaspersky Security Network.
Considera attendibili le applicazioni con firma digitale	Se la casella di controllo è selezionata, il componente Prevenzione Intrusioni Host posiziona le applicazioni con la firma digitale di produttori attendibili nel gruppo *Attendibili*. I *produttori attendibili* sono i produttori di software considerati attendibili da Kaspersky. È inoltre possibile aggiungere manualmente il certificato del produttore all'archivio certificati attendibili. Se la casella di controllo è deselezionata, il componente Prevenzione Intrusioni Host non considera attendibili tali applicazioni e utilizza altri parametri per determinarne il gruppo di attendibilità.
Elimina le regole per le applicazioni non avviate per più di N giorni (da 1 a 90)	Se la casella di controllo è selezionata, Kaspersky Endpoint Security elimina automaticamente le informazioni sull'applicazione (gruppo di attendibilità e diritti di accesso) se vengono soddisfatte le seguenti condizioni: • L'utente ha manualmente inserito l'applicazione in un gruppo di attendibilità o ne ha configurato i diritti di accesso. • L'applicazione non si è avviata entro il periodo di tempo definito. Se il gruppo di attendibilità e i diritti di un'applicazione sono stati determinati automaticamente, Kaspersky Endpoint Security elimina le informazioni sull'applicazione dopo 30 giorni. Non è possibile modificare il periodo di archiviazione per le informazioni dell'applicazione o disattivare l'eliminazione automatica. Al successivo avvio dell'applicazione, Kaspersky Endpoint Security analizza l'applicazione come se si trattasse del primo avvio.
Gruppo di attendibilità per le applicazioni non incluse in altri gruppi	Gli elementi in questo elenco a discesa determinano a quale gruppo di attendibilità Kaspersky Endpoint Security assegnerà un'applicazione sconosciuta. È possibile selezionare uno dei seguenti elementi: • **Restrizione bassa**. • **Restrizione alta**. • **Non attendibili**.

Motore di Remediation

Il componente Motore di Remediation consente a Kaspersky Endpoint Security di eseguire il rollback delle azioni eseguite dal malware nel sistema operativo.

Durante il rollback dell'attività del malware nel sistema operativo, Kaspersky Endpoint Security gestisce i seguenti tipi di attività del malware:

- **Attività sui file**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Elimina i file eseguibili creati dal malware (in tutti i supporti eccetto le unità di rete).
  - Elimina i file eseguibili creati da programmi in cui si è verificata un'infiltrazione di malware.
  - Ripristina i file modificati o eliminati dal malware.

  La funzionalità di ripristino dei file prevede diverse limitazioni.

- **Attività sul registro di sistema**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Elimina le chiavi del registro di sistema create dal malware.
  - Non ripristina le chiavi del registro di sistema modificate o eliminate dal malware.

- **Attività sul sistema**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Termina i processi avviati dal malware.
  - Termina i processi in cui è penetrata un'applicazione dannosa.
  - Non riprende i processi che sono stati arrestati dal malware.

- **Attività di rete**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Blocca l'attività di rete del malware.
  - Blocca l'attività di rete dei processi in cui si è verificata un'infiltrazione di malware.

Il rollback delle azioni del malware può essere avviato dal componente Protezione minacce file o Rilevamento del Comportamento o nel corso di una scansione malware.

La procedura di rollback delle operazioni del malware influisce su un set di dati ben definito. Il rollback non ha alcun effetto indesiderato sul sistema operativo o sull'integrità dei dati del computer.

Kaspersky Security Network



Per proteggere il computer in modo più efficace, Kaspersky Endpoint Security utilizza dati ricevuti dagli utenti di tutto il mondo. L'acquisizione di questi dati viene eseguita tramite Kaspersky Security Network.

La funzionalità KSN potrebbe non essere disponibile nell'applicazione negli Stati Uniti.

Kaspersky Security Network (KSN) è un'infrastruttura di servizi cloud che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce risposte più rapide da parte di Kaspersky Endpoint Security alle nuove minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi positivi. Se si partecipa a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla reputazione degli indirizzi Web scansionati, nonché informazioni sulla categoria e sulla reputazione dei file scansionati. Per ulteriori dettagli sulla configurazione dell'accesso a KSN, consultare la Guida di Kaspersky Security Center.

L'utilizzo di Kaspersky Security Network è facoltativo. L'applicazione richiede di utilizzare KSN durante la configurazione iniziale dell'applicazione. Gli utenti possono aderire al servizio o interrompere la partecipazione a KSN in qualsiasi momento.

Per informazioni più dettagliate sull'invio a Kaspersky delle informazioni statistiche generate durante la partecipazione a KSN, nonché sull'archiviazione e l'eliminazione di tali informazioni, fare riferimento all'Informativa di Kaspersky Security Network e al sito Web di Kaspersky. Il file ksn_<ID lingua>.txt con il testo dell'Informativa di Kaspersky Security Network è incluso nel kit di distribuzione dell'applicazione.

L'infrastruttura dei database di reputazione di Kaspersky

Kaspersky Endpoint Security supporta le seguenti soluzioni di infrastruttura per l'utilizzo dei database di reputazione di Kaspersky:

- *Kaspersky Security Network (KSN)* è la soluzione utilizzata dalla maggior parte delle applicazioni Kaspersky. I partecipanti KSN ricevono le informazioni da Kaspersky e inviano a Kaspersky le informazioni sugli oggetti rilevati nel computer dell'utente per un'analisi aggiuntiva da parte degli analisti di Kaspersky e per essere incluse nei database statistici e della reputazione.

- *Kaspersky Private Security Network (KPSN)* è una soluzione che consente agli utenti di computer che ospitano Kaspersky Endpoint Security o altre applicazioni Kaspersky di ottenere l'accesso ai database di reputazione di Kaspersky e ad altri dati statistici senza inviare dati a Kaspersky dai propri computer. KPSN è progettato per i clienti aziendali che non sono in grado di partecipare a Kaspersky Security Network per uno dei seguenti motivi:

  - Le workstation locali non sono connesse a Internet.

La trasmissione dei dati al di fuori del paese o al di fuori della LAN aziendale è vietato dalla legge o sottoposto a restrizioni in base ai criteri di protezione aziendali.

Parametro	Descrizione
Abilita modalità KSN estesa	*Modalità KSN estesa* è una modalità in cui Kaspersky Endpoint Security invia dati aggiuntivi a Kaspersky. Kaspersky Endpoint Security utilizza KSN per rilevare le minacce indipendentemente dalla posizione di attivazione/disattivazione.
Abilita modalità cloud	La *Modalità cloud* fa riferimento alla modalità operativa dell'applicazione in cui Kaspersky Endpoint Security utilizza una versione leggera dei database anti-virus. Kaspersky Security Network supporta il funzionamento dell'applicazione con l'utilizzato dei database anti-virus leggeri. La versione leggera dei database anti-virus consente di utilizzare circa la metà della RAM del computer che altrimenti verrebbe utilizzata con i database standard. Se non si partecipa a Kaspersky Security Network o se la modalità cloud è disabilitata, Kaspersky Endpoint Security scarica la versione completa dei database anti-virus dai server di Kaspersky. Se l'interruttore è attivato, Kaspersky Endpoint Security utilizza la versione leggera dei database anti-virus, riducendo così il carico sulle risorse del sistema operativo. Kaspersky Endpoint Security scarica la versione leggera dei database anti-virus durante il successivo aggiornamento dopo la selezione della casella di controllo. Se l'interruttore è disattivato, Kaspersky Endpoint Security utilizza la versione completa dei database anti-virus. Kaspersky Endpoint Security scarica la versione completa dei database anti-virus durante il successivo aggiornamento dopo la deselezione della casella di controllo.
Stato del computer quando i server KSN non sono disponibili *(disponibile solo in Kaspersky Security Center Console)*	Gli elementi presenti in questo elenco a discesa determinano lo stato di un computer in Kaspersky Security Center quando i server KSN non sono disponibili.
Usa Administration Server come server proxy KSN *(disponibile solo in Kaspersky Security Center Console)*	Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza il servizio proxy KSN. È possibile configurare le impostazioni del servizio proxy KSN nelle proprietà di Administration Server.
Usa i server di Kaspersky Security Network se il server proxy KSN non è disponibile *(disponibile solo in Kaspersky Security Center Console)*	Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza i server KSN quando il servizio KSN Proxy non è disponibile. I server KSN possono essere gestiti sia da Kaspersky che da terzi (quando si utilizza Kaspersky Private Security Network).

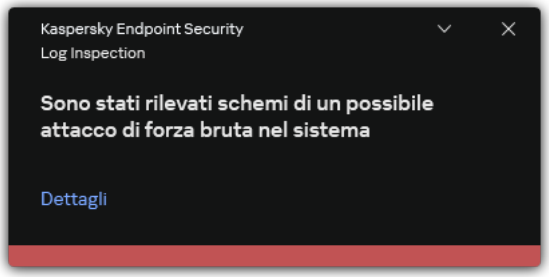
Log Inspection

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation.

Log Inspection monitora l'integrità dell'ambiente protetto in base all'analisi del Registro eventi di Windows. Quando l'applicazione rileva segnali di comportamento atipico nel sistema, ne informa l'amministratore, poiché questo comportamento potrebbe indicare un tentativo di attacco informatico.

Kaspersky Endpoint Security analizza i registri eventi di Windows e rileva le violazioni in base alle regole. Il componente include regole predefinite. Le regole predefinite sono basate sull'analisi euristica. È inoltre possibile aggiungere le proprie regole (regole personalizzate). Quando si attiva una regola, l'applicazione crea un evento con lo stato *Critico* (vedere la figura riportata di seguito).

Se si desidera utilizzare Log Inspection, verificare che le impostazioni di sicurezza del criterio di controllo siano configurate e che il sistema stia registrando gli eventi pertinenti (per ulteriori dettagli, visitare il sito Web dell'Assistenza tecnica Microsoft).



Notifica di Log Inspection

Impostazioni di Log Inspection

Parametro	Descrizione
Regole predefinite	Elenco delle regole di Log Inspection. Le regole predefinite includono modelli di attività anomale nel computer protetto. Le attività anomale possono indicare un tentativo di attacco.
Regole personalizzate	Elenco delle regole di Log Inspection aggiunte dall'utente. È possibile impostare i propri criteri di attivazione della regola di Log Inspection. A tal fine, è necessario immettere un ID evento e selezionare un'origine evento. È possibile selezionare un'origine evento tra i registri standard: *Application*, *Security* o *System*. È inoltre possibile specificare il registro di un'applicazione di terzi.

Anti-Cryptor

Il componente Anti-Cryptor analizza le attività nelle cartelle condivise. Se questa attività corrisponde a una firma BSS tipica del criptaggio esterno, Kaspersky Endpoint Security esegue l'azione selezionata.

Kaspersky Endpoint Security impedisce il criptaggio esterno solo dei file che si trovano in supporti che dispongono del file system NTFS e non sono criptati dal sistema EFS.

Parametro	Descrizione
Esclusioni in base al nome o all'indirizzo IP	**Esclusioni in base al nome o all'indirizzo IP**. Elenco di computer da cui i tentativi di criptaggio delle cartelle condivise non verranno monitorati. Per applicare l'elenco delle esclusioni dei computer dalla protezione delle cartelle condivise dal criptaggio esterno, è necessario abilitare Controlla Accesso nel criterio di controllo di sicurezza Windows. Controlla Accesso è disabilitato per impostazione predefinita. Per ulteriori informazioni su un criterio di controllo di sicurezza Windows, visitare il sito Web Microsoft. **Esclusioni in base alla maschera**. Esclusioni dell'ambito di protezione. L'esclusione di una cartella dall'ambito di protezione può ridurre la quantità di falsi positivi se l'organizzazione utilizza il criptaggio dei dati durante lo scambio di file tramite cartelle condivise. Ad esempio, Rilevamento del Comportamento può generare falsi positivi quando l'utente utilizza file con estensione ENC in una cartella condivisa. Tale attività corrisponde a uno schema comportamentale tipico del criptaggio esterno. Se sono presenti file criptati in una cartella condivisa per proteggere i dati, aggiungere tale cartella alle esclusioni. Utilizzare le maschere: • Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle. • Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida. • Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.
Azione se viene rilevata una minaccia	• **Informa**. Se questa opzione è selezionata, al rilevamento di un tentativo di modifica dei file nelle cartelle condivise, Kaspersky Endpoint Security aggiunge le informazioni su questo tentativo di modifica nell'elenco delle minacce attive, aggiunge una voce ai rapporti dell'interfaccia dell'applicazione locale e invia le informazioni sull'attività dannosa rilevata a Kaspersky Security Center. • **Blocca connessione per (min) N min**. Se questa opzione è selezionata, quando Kaspersky Endpoint Security rileva un tentativo di modifica dei file nelle cartelle condivise, blocca l'accesso alla modifica dei file per la sessione che ha avviato l'attività dannosa e crea copie di backup dei file modificati. Se il componente Motore di Remediation è abilitato e l'opzione **Blocca connessione per (min) N min** è selezionata, i file modificati vengono ripristinati dalle copie di backup.
Ambito della protezione	L'*ambito di protezione* è un elenco di percorsi delle cartelle condivise in cui Kaspersky Endpoint Security monitora le attività sui file. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera. Per impostazione predefinita, l'applicazione identifica automaticamente le cartelle condivise e monitora le attività sui file in tutte le cartelle.

Controllo Web

Controllo Web gestisce l'accesso degli utenti alle risorse Web. Questo consente di ridurre il traffico e l'utilizzo inappropriato dell'orario di lavoro. Quando un utente tenta di aprire un sito Web sottoposto a restrizioni da Controllo Web, Kaspersky Endpoint Security bloccherà l'accesso o mostrerà un avviso (vedere la figura seguente).

Per utilizzare Controllo Web, è necessario completare la configurazione iniziale dell'applicazione:

- Per il monitoraggio del traffico HTTPS, abilitare la scansione delle connessioni criptate (abilitata per impostazione predefinita).
- Selezionare le porte che Kaspersky Endpoint Security deve monitorare (per impostazione predefinita, l'applicazione monitora tutte le porte).

- Selezionare le applicazioni il cui traffico si desidera venga monitorato da Kaspersky Endpoint Security. La maggior parte dei browser è già presente nell'elenco delle applicazioni consigliate da Kaspersky. Se il browser non è presente nell'elenco, aggiungerlo manualmente.

- Si consiglia di inoculare lo script per l'interazione con le pagine Web nel traffico Web (per impostazione predefinita, l'inserimento dello script è disabilitato). Questo script consente la registrazione degli eventi di Controllo Web per il registro eventi dell'applicazione, il registro eventi del sistema operativo e i rapporti.

Metodi per la gestione dell'accesso ai siti Web

Controllo Web consente di configurare l'accesso ai siti Web utilizzando i seguenti metodi:

- **Categoria di siti Web**. I siti Web vengono suddivisi in categorie in base al servizio cloud di Kaspersky Security Network, all'analisi euristica e al database dei siti Web noti (inclusi nei database delle applicazioni). È ad esempio possibile limitare l'accesso degli utenti alla categoria *Social network* o ad altre categorie.

- **Tipo di dati**. È ad esempio possibile limitare l'accesso degli utenti ai dati di un sito Web e nascondere le immagini. Kaspersky Endpoint Security determina il tipo di dati in base al formato di file e non in base alla relativa estensione.

  Kaspersky Endpoint Security non esegue la scansione dei file all'interno degli archivi. Se ad esempio i file di immagini sono stati inseriti in un archivio, Kaspersky Endpoint Security identifica il tipo di dati *Archivi* e non *Grafica*.

- **A singoli indirizzi**. È possibile inserire un indirizzo Web o usare le maschere.

È possibile utilizzare diversi metodi contemporaneamente per regolare l'accesso ai siti Web. È ad esempio possibile limitare l'accesso al tipo di dati *Applicazioni Office* solo per la categoria di siti Web *E-mail basata sul Web*.

Regole di accesso ai siti Web

Controllo Web gestisce l'accesso dell'utente ai siti Web utilizzando le *regole di accesso*. È possibile configurare le seguenti impostazioni avanzate per una regola di accesso ai siti Web:

- Utenti ai quali si applica la regola.

  È ad esempio possibile limitare l'accesso a Internet tramite un browser per tutti gli utenti dell'azienda ad eccezione del dipartimento IT.

- Pianificazione regola.

  È ad esempio possibile limitare l'accesso a Internet tramite un browser solo durante l'orario di lavoro.

Priorità delle regole di accesso

Ogni regola ha una priorità. Più alta è la posizione di una regola nell'elenco, maggiore è la priorità. Se un sito Web è stato aggiunto a più regole, Controllo Web regola l'accesso al sito Web in base alla regola con la massima priorità. Ad esempio, Kaspersky Endpoint Security potrebbe identificare un portale aziendale come social network. Per limitare l'accesso ai social network e fornire l'accesso al portale Web aziendale, creare due regole: una regola di blocco per la categoria di siti Web *Social network* e una regola di permesso per il portale Web aziendale. La regola di accesso per il portale Web aziendale deve avere una priorità più elevata rispetto alla regola di accesso per i social network.



Messaggi di Controllo Web

Parametro	Descrizione
Regola di accesso alle risorse Web	Elenco contenente le regole di accesso alle risorse Web. Ogni regola ha una priorità. Più alta è la posizione di una regola nell'elenco, maggiore è la priorità. Se un sito Web è stato aggiunto a più regole, Controllo Web regola l'accesso al sito Web in base alla regola con la massima priorità.
Regola predefinita	La *regola predefinita* è una regola di accesso alle risorse Web a cui non si applica nessun'altra regola. Sono disponibili le seguenti opzioni: • **Consenti tutto tranne l'elenco di regole**, nota anche come modalità Lista vietati per i siti Web vietati. • **Vieta tutto tranne l'elenco di regole**, nota anche come modalità Lista consentiti per i siti Web consentiti.
Termina le sessioni browser attive dopo l'applicazione della regola	Se la casella di controllo è selezionata, Controllo Web interrompe la connessione alle risorse Web bloccate subito dopo l'applicazione del criterio. Il browser interrompe immediatamente il download dei dati dalla pagina Web. Quando si aggiorna la pagina Web o si passa a un'altra pagina Web vietata, l'applicazione mostra un avviso. Controllo Web consente di disconnettere immediatamente le risorse Web solo nei browser Web. Per le altre applicazioni, Controllo Web limita solo le nuove connessioni. Se la casella di controllo è deselezionata, Controllo Web limita solo le nuove connessioni alle risorse Web vietate. Controllo Web non termina le connessioni attive.
Modelli	**Avviso**. Il campo di immissione contiene un modello del messaggio visualizzato se viene attivata una regola per la segnalazione dei tentativi di accesso a una risorsa Web indesiderata. **Messaggio relativo al blocco**. Il campo di immissione contiene il modello del messaggio visualizzato se viene attivata una regola che blocca l'accesso a una risorsa Web. **Messaggio all'amministratore**. Modello del messaggio da inviare all'amministratore della rete LAN se l'utente ritiene che il blocco sia stato applicato per errore. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'accesso a una pagina Web**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato. Sono disponibili variabili speciali per la gestione del modello di messaggio (ad esempio `%USER_NAME%`). Le variabili consentono di utilizzare un unico modello di messaggio per computer diversi.
Registra l'apertura delle pagine consentite	Kaspersky Endpoint Security registra i dati sulle visite a tutti i siti Web, inclusi i siti Web consentiti. Kaspersky Endpoint Security invia gli eventi a Kaspersky Security Center, al registro locale di Kaspersky Endpoint Security e al registro eventi di Windows. Per monitorare l'attività Internet degli utenti è necessario configurare le impostazioni per il salvataggio degli eventi. Browser che supportano la funzione di monitoraggio: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Il monitoraggio delle attività degli utenti non funziona in altri browser. Il monitoraggio dell'attività Internet degli utenti può richiedere più risorse del computer quando si decripta il traffico HTTPS.

Controllo dispositivi

Controllo dispositivi consente di gestire l'accesso dell'utente ai dispositivi installati nel computer o connessi al computer (ad esempio dischi rigidi, fotocamere o moduli Wi-Fi). In questo modo è possibile proteggere il computer dalle infezioni quando tali dispositivi sono connessi e prevenire perdite o fughe di dati.

Se Controllo dispositivi è abilitato, l'applicazione inoltra le informazioni sui dispositivi connessi a Kaspersky Security Center. È possibile visualizzare l'elenco dei dispositivi connessi in Kaspersky Security Center nella cartella **Avanzate** → **Archivi** → **Hardware**.

Livelli di accesso ai dispositivi

Controllo dispositivi controlla l'accesso ai seguenti livelli:

- **Tipo di dispositivo**. Ad esempio stampanti, unità rimovibili e unità CD/DVD.

  È possibile configurare l'accesso ai dispositivi nel modo seguente:

  - Consenti – .
  - Blocca – .
  - In base alle regole (solo stampanti e dispositivi portatili) - .
  - Dipende dal bus di connessione (eccetto Wi-Fi) - .
  - Blocca con eccezioni (Solo Wi-Fi) - .

- **Bus di connessione**. Un *bus di connessione* è un'interfaccia utilizzata per la connessione dei dispositivi al computer (ad esempio, USB o FireWire). Se la modalità **Dipende dal bus di connessione** è selezionata per il tipo di dispositivo, l'applicazione consente o nega l'accesso al dispositivo a seconda dell'interfaccia di connessione (ad esempio, USB).

  È possibile configurare l'accesso ai dispositivi nel modo seguente:

  - Consenti – .
  - Blocca – .

- **Dispositivi attendibili**. I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile.

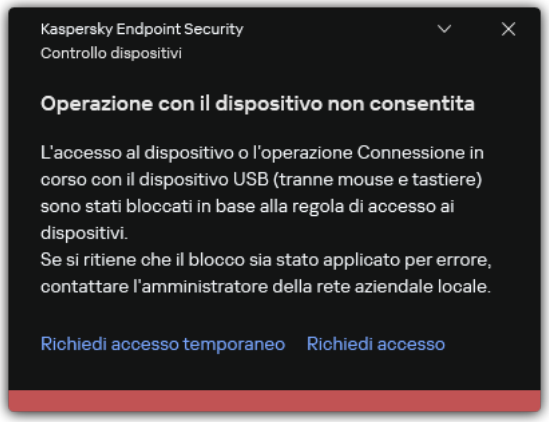
  È possibile aggiungere dispositivi attendibili in base ai seguenti dati:

  - **Dispositivi per ID**. Ogni dispositivo ha un identificatore univoco (Hardware ID o HWID). È possibile visualizzare l'ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. Esempio di ID dispositivo: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. L'aggiunta di dispositivi in base all'ID è utile se si desidera aggiungere più dispositivi specifici.
  - **Dispositivi per modello**. Ogni dispositivo ha un Vendor ID (VID) e un Product ID (PID). È possibile visualizzare gli ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. Modello per l'immissione di VID e PID: `VID_1234&PID_5678`. L'aggiunta di dispositivi in base al modello è utile se si utilizzano dispositivi di un determinato modello nell'organizzazione. In tal modo è possibile aggiungere tutti i dispositivi di questo modello.
  - **Dispositivi per maschera ID**. Se si utilizzano più dispositivi con ID simili, è possibile aggiungere dispositivi all'elenco dei dispositivi attendibili utilizzando le maschere. Il carattere `*` sostituisce qualsiasi set di caratteri. Kaspersky Endpoint Security non supporta il carattere `?` quando si immette una maschera. Ad esempio, `WDC_C*`.
  - **Dispositivi per maschera del modello**. Se si utilizzano più dispositivi con VID o PID simili, ad esempio dispositivi dello stesso produttore, è possibile aggiungere dispositivi all'elenco dei dispositivi attendibili utilizzando le maschere. Il carattere `*` sostituisce qualsiasi set di caratteri. Kaspersky Endpoint Security non supporta il carattere `?` quando si immette una maschera. Ad esempio, `VID_05AC&PID_*`.

Controllo dispositivi regola l'accesso dell'utente ai dispositivi utilizzando le *regole di accesso*. Controllo dispositivi consente inoltre di salvare gli eventi di connessione/disconnessione dei dispositivi. Per salvare gli eventi, è necessario configurare la registrazione degli eventi in un criterio.

Se l'accesso a un dispositivo dipende dal bus di connessione (stato), Kaspersky Endpoint Security non salva gli eventi di connessione/disconnessione del dispositivo. Per consentire a Kaspersky Endpoint Security di salvare gli eventi di connessione/disconnessione del dispositivo, consentire l'accesso al tipo di dispositivo corrispondente (stato) o aggiungere il dispositivo all'elenco degli oggetti attendibili.

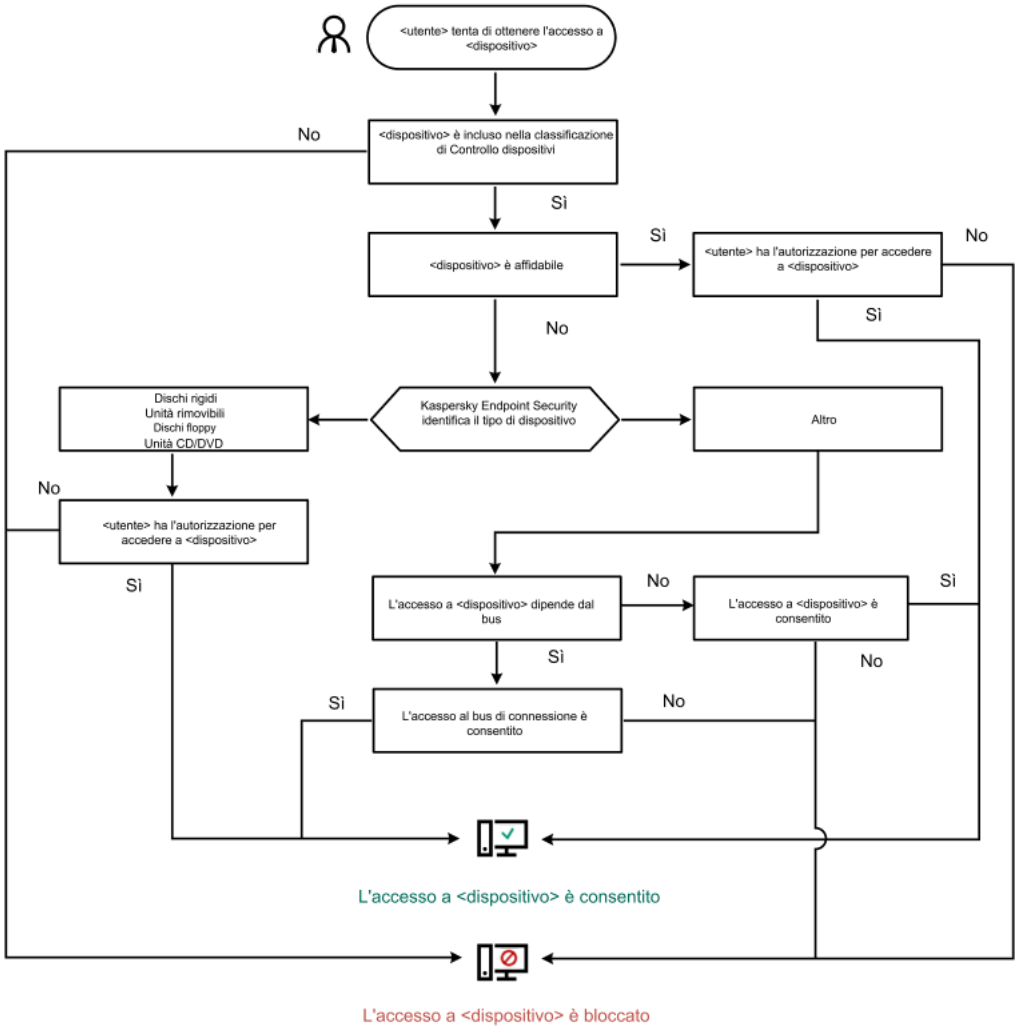
Quando un dispositivo bloccato da Controllo dispositivi viene connesso al computer, Kaspersky Endpoint Security bloccherà l'accesso e mostrerà una notifica (vedere la figura seguente).



Notifica Controllo dispositivi

Algoritmo operativo di Controllo dispositivi

Kaspersky Endpoint Security stabilisce se consentire l'accesso a un dispositivo dopo che l'utente connette il dispositivo al computer (vedere la figura di seguito).



Algoritmo operativo di Controllo dispositivi

Se un dispositivo è connesso e l'accesso è consentito, è possibile modificare la regola di accesso e bloccare l'accesso. In tal caso, la volta successiva che qualcuno tenta di accedere al dispositivo (ad esempio per visualizzare la struttura delle cartelle o eseguire operazioni di lettura o scrittura), Kaspersky Endpoint Security blocca l'accesso. Un dispositivo privo di file system viene bloccato solo alla connessione successiva.

Se un utente del computer in cui è installato Kaspersky Endpoint Security deve richiedere l'accesso a un dispositivo che ritiene sia stato bloccato per errore, inviare all'utente le istruzioni per la richiesta di accesso.

Parametro	Descrizione
Consenti richieste di accesso temporaneo *(disponibile solo in Kaspersky Security Center Console)*	Se la casella di controllo è selezionata, il pulsante **Richiedi accesso** è disponibile nell'interfaccia locale di Kaspersky Endpoint Security. Utilizzando questo pulsante, l'utente può richiedere l'accesso temporaneo a un dispositivo bloccato.
Dispositivi e reti Wi-Fi	Questa tabella contiene tutti i possibili tipi di dispositivi in base alla classificazione del componente Controllo dispositivi, con i relativi stati di accesso.
Bus di connessione	Un elenco di tutti i bus di connessione disponibili in base alla classificazione del componente Controllo dispositivi, con i relativi stati di accesso. Kaspersky Endpoint Security consente o nega l'accesso ai dispositivi a seconda del tipo di bus di connessione, se la modalità **Dipende dal bus di connessione** è selezionata.
Dispositivi attendibili	Elenco di dispositivi attendibili e di utenti ai quali è stato concesso l'accesso a questi dispositivi.
Unisci i valori quando vengono ereditati *(disponibile solo in Kaspersky Security Center Console)*	In questo modo viene unito l'elenco dei dispositivi attendibili nei criteri padre e figlio di Kaspersky Security Center. Per unire gli elenchi, il criterio figlio deve essere configurato per ereditare le impostazioni del criterio padre di Kaspersky Security Center. Se la casella di controllo è selezionata, gli elementi dell'elenco del criterio padre di Kaspersky Security Center vengono visualizzati nei criteri figlio. In questo modo è possibile creare ad esempio un elenco consolidato di dispositivi attendibili per l'intera organizzazione. Gli elementi dell'elenco ereditati in un criterio figlio non possono essere eliminati o modificati. Gli elementi nell'elenco dei dispositivi attendibili uniti durante l'ereditarietà possono essere eliminati e modificati solo nel criterio padre. È possibile aggiungere, modificare o eliminare elementi dell'elenco nei criteri di livello inferiore. Se gli elementi negli elenchi del criterio padre e figlio corrispondono, questi elementi vengono visualizzati come lo stesso elemento del criterio padre. Se la casella di controllo non è selezionata, gli elementi degli elenchi non vengono uniti quando ereditano le impostazioni dei criteri di Kaspersky Security Center. Questa funzionalità consente inoltre di unire gli elenchi nei profili dei criteri. Per unire gli elenchi, nel profilo con priorità più alta abilitare l'ereditarietà delle impostazioni da un profilo con priorità più bassa. Per ulteriori dettagli sulle priorità dei profili dei criteri, consultare la Guida di Kaspersky Security Center .
Anti-Bridging	Anti-Bridging inibisce la creazione di bridge di rete impedendo la creazione simultanea di più connessioni di rete per un computer. Questo consente di proteggere una rete aziendale dagli attacchi su reti non protette e non autorizzate. Anti-Bridging blocca la creazione di connessioni multiple in base alle priorità dei dispositivi. Più alta è la posizione di un dispositivo nell'elenco, maggiore è la priorità. Se una connessione attiva e una nuova connessione sono entrambe dello stesso tipo (ad esempio, Wi-Fi), Kaspersky Endpoint Security blocca la connessione attiva e consente la creazione della nuova connessione. Se una connessione attiva e una nuova connessione appartengono a tipologie diverse (ad esempio una scheda di rete e Wi-Fi), Kaspersky Endpoint Security blocca la connessione con la priorità più bassa e consente la connessione con la priorità più alta. Anti-Bridging supporta il funzionamento con i seguenti tipi di dispositivi: scheda di rete, Wi-Fi e modem.
Modelli di messaggi	**Messaggio relativo al blocco**. Modello del messaggio visualizzato quando un utente tenta di accedere a un dispositivo bloccato. Questo messaggio viene visualizzato anche quando un utente tenta di eseguire un'operazione sui contenuti del dispositivo bloccata per questo utente. **Messaggio all'amministratore**. Un modello del messaggio inviato all'amministratore della rete LAN quando l'utente ritiene che l'accesso al dispositivo sia stato bloccato o che un'operazione relativa ai contenuti del dispositivo sia stata vietata per errore. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'accesso a un dispositivo**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato.

Controllo applicazioni

Controllo applicazioni gestisce l'avvio delle applicazioni nei computer degli utenti. Ciò consente di implementare un criterio di sicurezza aziendale quando si utilizzano le applicazioni. Controllo applicazioni riduce anche il rischio di infezione del computer limitando l'accesso alle applicazioni.

La configurazione di Controllo applicazioni prevede i seguenti passaggi:

1. Creazione delle categorie di applicazioni.

   L'amministratore crea categorie di applicazioni che l'amministratore desidera gestire. Le categorie di applicazioni sono destinate a tutti i computer della rete aziendale, indipendentemente dai gruppi di amministrazione. Per creare una categoria, è possibile utilizzare i seguenti criteri: Categoria KL (ad esempio, *Browser* o un'altra categoria), hash del file, fornitore dell'applicazione e altri criteri.

2. Creazione delle regole di Controllo applicazioni.

   L'amministratore crea le regole di Controllo applicazioni nel criterio per il gruppo di amministrazione. La regola include le categorie di applicazioni e lo stato di avvio delle applicazioni di queste categorie: bloccate o consentite. L'amministratore può creare molte regole. Una sola applicazione può soddisfare i criteri di più regole. La priorità di una regola di blocco è superiore a quella di una regola di autorizzazione. Kaspersky Endpoint Security controlla se un'applicazione soddisfa una regola ogni volta che viene avviata. Kaspersky Endpoint Security abbina in sequenza l'applicazione a tutte le regole di Controllo applicazioni.

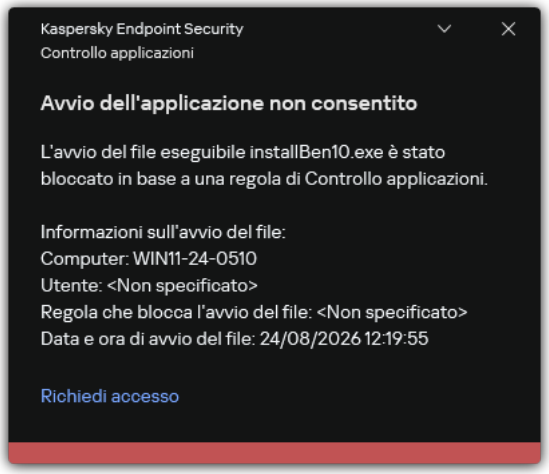
3. Selezione della modalità di Controllo applicazioni.

   L'amministratore sceglie la modalità per l'utilizzo delle applicazioni che non sono incluse in nessuna delle regole: (lista vietati e lista consentiti delle applicazioni).

Quando un utente tenta di avviare un'applicazione vietata, Kaspersky Endpoint Security blocca l'avvio dell'applicazione e visualizza una notifica (vedere la figura seguente).

È disponibile una *modalità test* per verificare la configurazione di Controllo applicazioni. In questa modalità, Kaspersky Endpoint Security procede come segue:

- Consente l'avvio delle applicazioni, comprese quelle vietate.
- Mostra una notifica sull'avvio di un'applicazione vietata e aggiunge informazioni al rapporto sul computer dell'utente.
- Invia i dati sull'avvio delle applicazioni vietate a Kaspersky Security Center.



Notifica di Controllo applicazioni

Modalità di esecuzione di Controllo applicazioni

Il componente Controllo applicazioni funziona in due modalità:

- **Lista vietati**. In questa modalità, Controllo applicazioni consente agli utenti di avviare tutte le applicazioni ad eccezione di quelle vietate nelle regole di Controllo applicazioni.

  Questa modalità di Controllo applicazioni è abilitata per impostazione predefinita.

- **Lista consentiti**. In questa modalità, Controllo applicazioni impedisce agli utenti di avviare qualsiasi applicazione ad eccezione di quelle consentite e non vietate nelle regole di Controllo applicazioni.

  Se le regole di permesso di Controllo applicazioni sono completamente configurate, il componente blocca l'avvio di tutte le nuove applicazioni che non sono state verificate dall'amministratore della LAN, consentendo al contempo il funzionamento del sistema operativo e delle applicazioni attendibili alle quali gli utenti si affidano per le proprie attività.

  Sono disponibili suggerimenti sulla configurazione delle regole di Controllo applicazioni nella modalità Lista consentiti.

Controllo Applicazioni può essere configurato per il funzionamento in queste modalità sia utilizzando l'interfaccia locale di Kaspersky Endpoint Security che utilizzando Kaspersky Security Center.

Tuttavia, Kaspersky Security Center offre strumenti che non sono disponibili nell'interfaccia locale di Kaspersky Endpoint Security, come gli strumenti necessari per le seguenti attività:

- Creazione delle categorie di applicazioni.

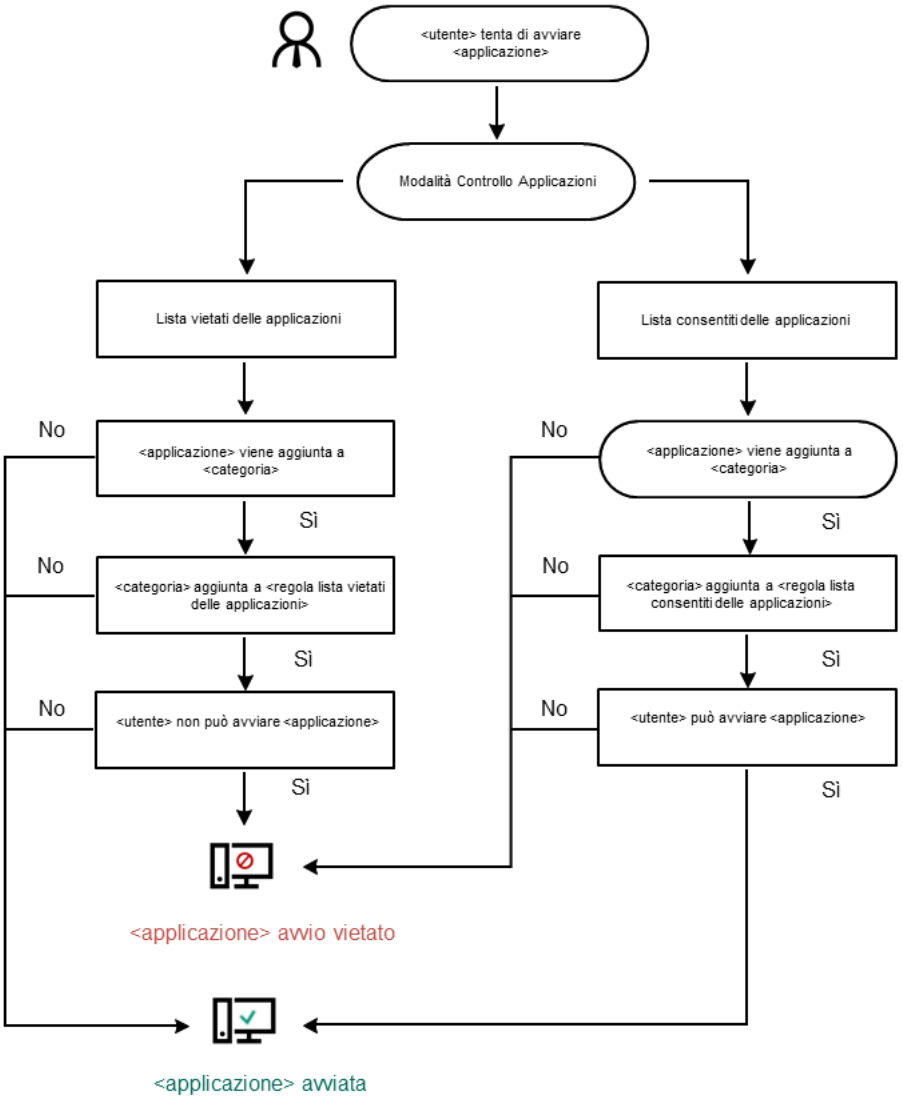
  Le regole di Controllo applicazioni create in Kaspersky Security Center Administration Console si basano sulle categorie di applicazioni personalizzate e non sulle condizioni di inclusione ed esclusione, come nel caso dell'interfaccia locale di Kaspersky Endpoint Security.

- Ricezione delle informazioni sulle applicazioni installate nei computer della LAN aziendale.

Questo è il motivo per cui si consiglia di utilizzare Kaspersky Security Center per configurare il funzionamento del componente Controllo applicazioni.

Algoritmo operativo di Controllo applicazioni

Kaspersky Endpoint Security utilizza un algoritmo per prendere una decisione in merito all'avvio di un'applicazione (vedere la figura seguente).



Algoritmo operativo di Controllo applicazioni

Parametro	Descrizione
Azione all'avvio delle applicazioni bloccate dalle regole	**Applica regole**. Kaspersky Endpoint Security gestisce l'avvio delle applicazioni in base alla modalità selezionata. **Testa regole**. Kaspersky Endpoint Security consente l'avvio di un'applicazione bloccata nella modalità corrente di Controllo applicazioni, ma registra le informazioni sull'avvio dell'applicazione nel rapporto.
Modalità Controllo avvio applicazioni	È possibile selezionare una delle seguenti opzioni: • **Lista vietati**. Se è selezionata questa opzione, Controllo applicazioni consente a tutti gli utenti di avviare qualsiasi applicazione, fatta eccezione per i casi in cui vengono soddisfatte le condizioni delle regole di blocco di Controllo applicazioni. • **Lista consentiti**. Se è selezionata questa opzione, Controllo applicazioni impedisce a tutti gli utenti di avviare qualsiasi applicazione, fatta eccezione per i casi in cui vengono soddisfatte le condizioni delle regole di permesso di Controllo applicazioni. Quando la modalità **Lista consentiti** è selezionata, vengono automaticamente create due regole di Controllo applicazioni: • **Immagine gold**. • **Programmi di aggiornamento attendibili**. Non è possibile modificare le impostazioni di o eliminare le regole create automaticamente. È possibile abilitare o disabilitare queste regole.
Monitora caricamento dei moduli DLL	Se la casella di controllo è selezionata, Kaspersky Endpoint Security controlla il caricamento dei moduli DLL quando gli utenti tentano di avviare le applicazioni. Le informazioni sul modulo DLL e sull'applicazione che lo ha caricato vengono registrate nel rapporto. Quando si abilita il controllo del caricamento dei moduli DLL e dei driver, verificare che nelle impostazioni di Controllo applicazioni sia abilitata una delle seguenti regole: la regola **Immagine gold** predefinita o un'altra regola che contiene la categoria KL "**Immagine gold\Certificati attendibili**" e garantisce che i moduli DLL e i driver attendibili siano caricati prima dell'avvio di Kaspersky Endpoint Security. Abilitare il controllo del caricamento dei moduli DLL e dei driver quando la regola **Immagine gold** è disabilitata può generare instabilità nel sistema operativo. Kaspersky Endpoint Security monitora solo i moduli DLL e i driver caricati dal momento che è stata selezionata la casella di controllo. Dopo aver selezionato la casella di controllo, è consigliabile riavviare il computer per assicurarsi che l'applicazione monitori tutti i moduli DLL e i driver, inclusi quelli caricati prima dell'avvio di Kaspersky Endpoint Security.
Usa una rigorosa verifica della firma digitale	È possibile selezionare un certificato come condizione di attivazione per una regola di Controllo applicazioni. Se questa casella di controllo è selezionata, Kaspersky Endpoint Security applica le regole alle applicazioni firmate con i certificati solo dall'archivio dei certificati di sistema attendibili. Le applicazioni firmate con tale certificato sono considerate attendibili anche dai componenti della protezione, ad esempio l'attività *Scansione malware*. Tuttavia, se si specifica un certificato da un archivio diverso in una regola di Controllo applicazioni, Kaspersky Endpoint Security non applica tale regola. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security applica le regole alle applicazioni firmate da un certificato dell'archivio dei certificati radice attendibili di Windows. Tali applicazioni non fanno parte dell'area attendibile. I componenti della protezione monitorano le attività di tali applicazioni.
Modelli di messaggi sul blocco delle applicazioni	**Messaggio relativo al blocco**. Modello del messaggio visualizzato quando viene attivata una regola di Controllo applicazioni che blocca l'avvio di un'applicazione. **Messaggio all'amministratore**. Modello del messaggio che un utente può inviare all'amministratore della LAN aziendale se l'utente ritiene che un'applicazione sia stata bloccata per errore. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'avvio di un'applicazione**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato.

Controllo adattivo delle anomalie

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server.

Il componente Controllo adattivo delle anomalie monitora e blocca le azioni non tipiche dei computer in una rete aziendale. Controllo adattivo delle anomalie utilizza un set di regole per monitorare i comportamenti non tipici (ad esempio, la regola *Avvio di Microsoft PowerShell dall'applicazione Office*). Le regole vengono create dagli esperti di Kaspersky in base agli scenari tipici delle attività dannose. È possibile configurare la modalità di gestione di ogni regola da parte di Controllo adattivo delle anomalie e, ad esempio, consentire l'esecuzione degli script PowerShell per l'automazione di determinate attività del flusso di lavoro. Kaspersky Endpoint Security aggiorna il set di regole insieme ai database dell'applicazione. Gli aggiornamenti dei set di regole devono essere confermati manualmente.

Impostazioni di Controllo adattivo delle anomalie

La configurazione di Controllo adattivo delle anomalie prevede i seguenti passaggi:

1. Addestramento di Controllo adattivo delle anomalie.

   In seguito all'attivazione di Controllo adattivo delle anomalie, le relative regole vengono eseguite in *modalità addestramento*. Durante l'addestramento, Controllo adattivo delle anomalie monitora l'attivazione delle regole e invia gli eventi di attivazione a Kaspersky Security Center. Ogni regola ha una durata specifica per la modalità di addestramento. La durata della modalità di addestramento è impostata dagli esperti di Kaspersky. In genere, la modalità di addestramento è attiva per due settimane.

   Se una regola non è attivata durante l'addestramento, Controllo adattivo delle anomalie considererà non tipiche le azioni associate a tale regola. Kaspersky Endpoint Security bloccherà tutte le azioni associate alla regola.

   Se è stata attivata una regola durante l'addestramento, Kaspersky Endpoint Security registra gli eventi nel rapporto sull'attivazione delle regole e nell'archivio **Attivazioni di regole nello stato Smart Training**.

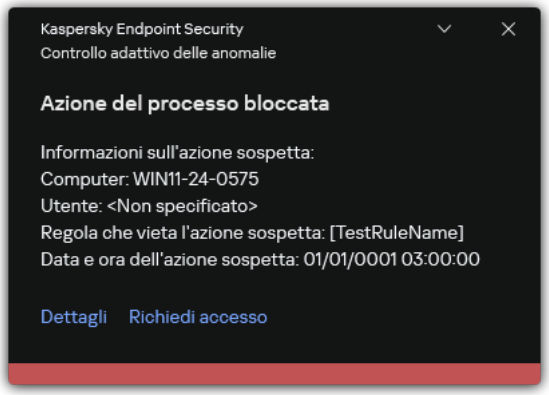
2. Analisi del rapporto sull'attivazione delle regole.

   L'amministratore analizza il rapporto sull'attivazione delle regole o i contenuti dell'archivio **Attivazioni di regole nello stato Smart Training**. L'amministratore può quindi selezionare il comportamento di Controllo adattivo delle anomalie quando viene attivata la regola, scegliendo se bloccarla o consentirla. L'amministratore può inoltre continuare a monitorare la modalità di esecuzione della regola e prolungare la durata della modalità addestramento. Se l'amministratore non esegue alcuna azione, anche l'applicazione continuerà a funzionare in modalità addestramento. Il periodo della modalità addestramento viene riavviato.

Controllo adattivo delle anomalie viene configurato in tempo reale tramite i seguenti canali:

- Controllo adattivo delle anomalie inizia automaticamente a bloccare le azioni associate alle regole che non sono mai state attivate in modalità addestramento.
- Kaspersky Endpoint Security aggiunge nuove regole oppure rimuove quelle obsolete.
- L'amministratore configura l'esecuzione di Controllo adattivo delle anomalie dopo l'analisi del rapporto sull'attivazione delle regole e dei contenuti dell'archivio **Attivazioni di regole nello stato Smart Training**. È consigliabile controllare il rapporto sull'attivazione delle regole e i contenuti dell'archivio **Attivazioni di regole nello stato Smart Training**.

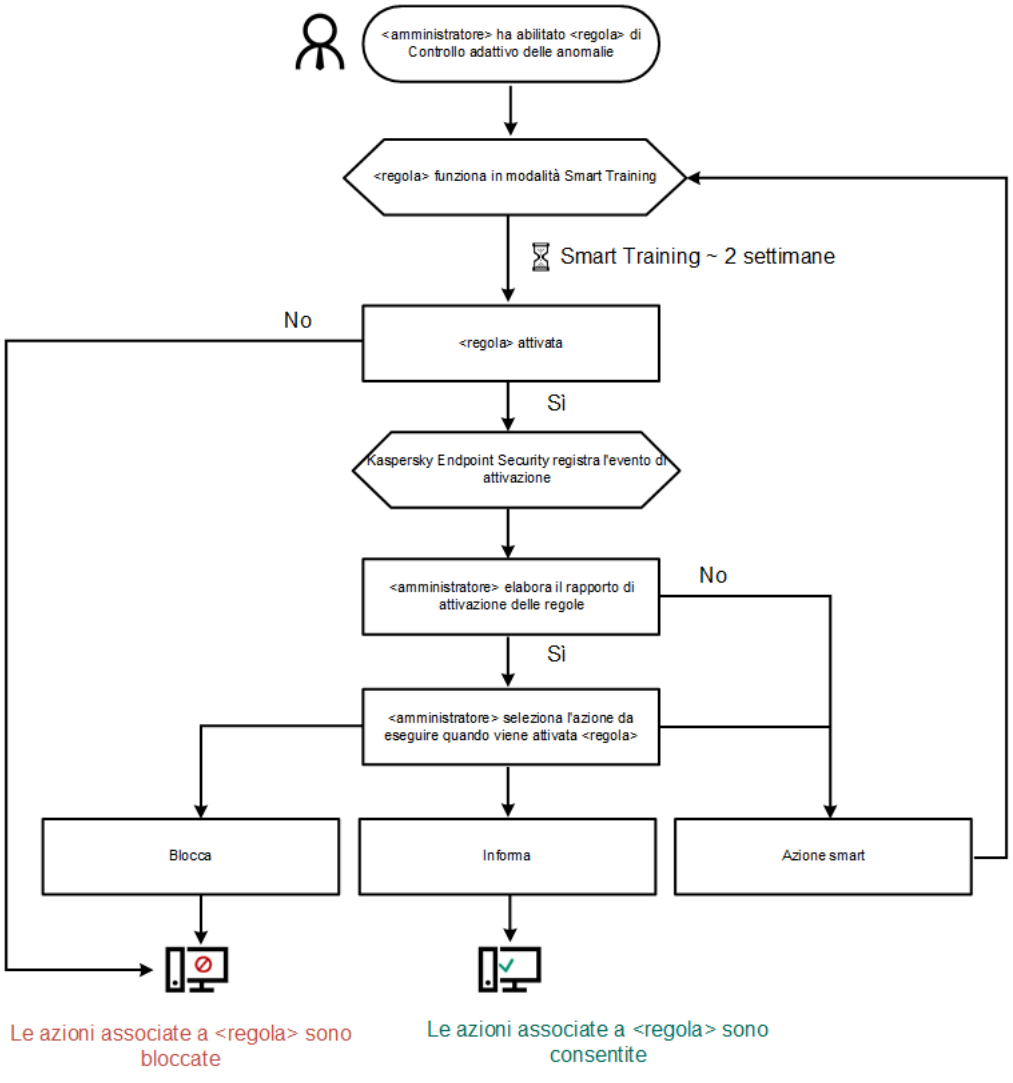
Quando un'applicazione dannosa tenta di eseguire un'azione, Kaspersky Endpoint Security blocca l'azione e visualizza una notifica (vedere la figura seguente).



Notifica di Controllo adattivo delle anomalie

Algoritmo operativo di Controllo adattivo delle anomalie

Kaspersky Endpoint Security decide se consentire o bloccare un'azione associata a una regola in base al seguente algoritmo (vedere la figura seguente).



Algoritmo operativo di Controllo adattivo delle anomalie

Parametro	Descrizione
Rapporto sullo stato delle regole di Controllo adattivo delle anomalie *(disponibile solo in Kaspersky Security Center Console)*	Questo rapporto contiene informazioni sullo stato delle regole di rilevamento di Controllo adattivo delle anomalie (ad esempio *Disabilitato* o *Blocca*). Il rapporto viene generato per tutti i gruppi di amministrazione.
Rapporto sulle regole attivate di Controllo adattivo delle anomalie *(disponibile solo in Kaspersky Security Center Console)*	Questo rapporto contiene informazioni sulle azioni non tipiche rilevate da Controllo adattivo delle anomalie. Il rapporto viene generato per tutti i gruppi di amministrazione.
Regole	Tabella delle regole di Controllo adattivo delle anomalie. Le regole vengono create dagli esperti di Kaspersky in base agli scenari tipici delle attività dannose.
Modelli	**Messaggio relativo al blocco**. Modello del messaggio visualizzato a un utente quando viene attivata una regola di Controllo adattivo delle anomalie che blocca un'azione non tipica. **Messaggio all'amministratore**. Modello del messaggio che un utente può inviare all'amministratore della rete aziendale locale se l'utente ritiene che il blocco sia un errore. Dopo che l'utente ha richiesto di fornire l'accesso, Kaspersky Endpoint Security invia un evento a Kaspersky Security Center: **Messaggio all'amministratore per il blocco dell'attività di un'applicazione**. La descrizione dell'evento contiene un messaggio all'amministratore con variabili sostituite. È possibile visualizzare questi eventi nella console di Kaspersky Security Center utilizzando la selezione di eventi predefinita **Richieste utente**. Se nell'organizzazione non è installato Kaspersky Security Center o non è presente alcuna connessione ad Administration Server, l'applicazione invierà un messaggio all'amministratore all'indirizzo e-mail specificato.

Monitoraggio integrità di sistema

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation.

A partire dalla versione 12.6, Kaspersky Endpoint Security for Windows include il componente Monitoraggio integrità di sistema anziché il componente Monitoraggio integrità file. Il componente Monitoraggio integrità di sistema include tutte le funzionalità di Monitoraggio integrità file e consente inoltre di monitorare le modifiche al Registro di sistema e la connessione dei dispositivi esterni.

Il componente Monitoraggio integrità di sistema monitora le modifiche nel sistema operativo che potrebbero indicare violazioni della sicurezza del computer. Quando vengono rilevate tali modifiche, Kaspersky Endpoint Security genera gli eventi corrispondenti e avvisa l'amministratore. Monitoraggio integrità di sistema può funzionare in modalità in tempo reale e può anche eseguire controlli dell'integrità del sistema su richiesta.

Monitoraggio integrità di sistema in tempo reale

In modalità in tempo reale, Monitoraggio integrità di sistema tiene traccia delle modifiche negli oggetti inclusi nell'ambito del componente (l'*ambito di monitoraggio*). Monitoraggio integrità di sistema consente inoltre di bloccare in tempo reale l'accesso non autorizzato a tali oggetti.

Controllo integrità di sistema su richiesta

Controllo integrità di sistema su richiesta è un'attività che è possibile eseguire manualmente o in base a una pianificazione. Per eseguire l'attività *Controllo integrità di sistema*, è necessario configurare l'ambito del componente (l'*ambito di monitoraggio*) e creare una linea di base. Una *linea di base* è uno stato registrato degli oggetti nel sistema che l'applicazione utilizza come riferimento per il confronto con lo stato corrente.

Impostazioni di Monitoraggio integrità di sistema

Parametro	Descrizione
Modalità operativa per le regole di blocco	• **Blocca**. In questa modalità, Monitoraggio integrità di sistema blocca le azioni con file e chiavi del Registro di sistema dall'ambito di monitoraggio e genera un evento corrispondente. • **Informa**. In questa modalità, Monitoraggio integrità di sistema consente le azioni con file e chiavi del Registro di sistema dall'ambito di monitoraggio e genera un evento corrispondente.
Monitoraggio integrità di sistema in tempo reale	In modalità in tempo reale, Monitoraggio integrità di sistema tiene traccia delle modifiche negli oggetti inclusi nell'ambito del componente (l'*ambito di monitoraggio*). Monitoraggio integrità di sistema consente inoltre di bloccare in tempo reale l'accesso non autorizzato a tali oggetti.
Monitora i dispositivi	Monitoraggio integrità di sistema monitora la connessione e la disconnessione dei dispositivi esterni.
Monitora i file e il Registro di sistema	Monitoraggio integrità di sistema monitora le modifiche a file, cartelle e Registro di sistema.
Controllo integrità di sistema	Controllo integrità di sistema su richiesta è un'attività che è possibile eseguire manualmente o in base a una pianificazione. Per eseguire l'attività *Controllo integrità di sistema*, è necessario configurare l'ambito del componente (l'*ambito di monitoraggio*) e creare una linea di base. Una *linea di base* è uno stato registrato degli oggetti nel sistema che l'applicazione utilizza come riferimento per il confronto con lo stato corrente.

Sensore Endpoint

Sensore Endpoint non è incluso in Kaspersky Endpoint Security 11.4.0.

È possibile gestire Sensore Endpoint in Kaspersky Security Center Web Console e in Kaspersky Security Center Administration Console. Non è possibile gestire Endpoint Sensor in Kaspersky Security Center Cloud Console.

Sensore Endpoint è progettato per l'interazione con Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* è una soluzione progettata per il rilevamento tempestivo di minacce sofisticate come attacchi mirati, minacce APT (Advanced Persistent Threat), attacchi zero-day e di altro tipo. Kaspersky Anti Targeted Attack Platform include tre unità funzionali:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

È possibile acquistare tutte le unità funzionali o le singole unità funzionali separatamente. Per informazioni dettagliate sulla soluzione, consultare la Guida di Kaspersky Anti Targeted Attack Platform.

La gestione di Sensore Endpoint prevede le seguenti limitazioni:

- È possibile configurare le impostazioni di Sensore Endpoint in un criterio a condizione che nel computer sia installata una versione di Kaspersky Endpoint Security dalla 11.0.0 alla 11.3.0. Per ulteriori informazioni sulla configurazione delle impostazioni di Sensore Endpoint utilizzando il criterio, consultare gli articoli della guida per le versioni precedenti di Kaspersky Endpoint Security.
- Se nel computer è installato Kaspersky Endpoint Security versione 11.4.0 e versioni successive, non è possibile configurare le impostazioni di Sensore Endpoint nel criterio.

Sensore Endpoint è installato nei computer client. In questi computer il componente monitora costantemente i processi, le connessioni di rete attive e i file modificati. Sensore Endpoint trasmette le informazioni al server KATA.

La funzionalità del componente è disponibile con i seguenti sistemi operativi:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64 bit);
- Windows Server 2012 Foundation / Standard / Enterprise (64 bit);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64 bit);
- Windows Server 2016 Essentials / Standard (64 bit).

Per informazioni dettagliate sul funzionamento di KATA, consultare la Guida di Kaspersky Anti Targeted Attack Platform.

Sandbox

Kaspersky Endpoint Security for Windows include un agente integrato per l'integrazione con la soluzione Kaspersky Sandbox. Il componente *Sandbox* rileva e blocca automaticamente le minacce avanzate sui computer. Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Sandbox). Per informazioni dettagliate sulla soluzione, consultare la Guida di Kaspersky Sandbox Help e la Guida di Kaspersky Anti Targeted Attack Platform.

A partire dalla versione 12.7, Kaspersky Endpoint Security for Windows supporta il componente Sandbox che fa parte della soluzione Kaspersky Anti Targeted Attack Platform. A differenza della soluzione Kaspersky Sandbox, il componente KATA Sandbox non solo consente la automatica dei file, ma anche la scansione manuale dei file dal menu di scelta rapida del file.

KATA Sandbox richiede la distribuzione di Kaspersky Anti Targeted Attack Platform 7.0 o versioni successive.

Il componente può essere gestito solo utilizzando Kaspersky Security Center Web Console. Non è possibile gestire questo componente tramite Administration Console (MMC).

Impostazioni del componente Sandbox

Parametro	Descrizione
Modalità di integrazione	**Kaspersky Sandbox**. Integrazione con la soluzione Kaspersky Sandbox. L'applicazione invia i file da sottoporre a scansione in Kaspersky Sandbox solo in modalità automatica. **KATA Sandbox**. Integrazione con il componente Sandbox della soluzione Kaspersky Anti Targeted Attack Platform. È possibile selezionare la modalità di invio dei file per la scansione: • **Manualmente**. L'utente invia manualmente il file per la scansione dal menu di scelta rapida (**Invia a Sandbox**). • **Automaticamente**. L'applicazione rileva automaticamente gli oggetti e li invia a Sandbox per la scansione. • **Combinato**.
Impostazioni della connessione al server	**Timeout (msec)**. Timeout della connessione per il server Sandbox (per Kaspersky Sandbox) o il server di Central Node (per KATA). Allo scadere del timeout configurato, Kaspersky Endpoint Security invia una richiesta al server successivo. È possibile aumentare il timeout della connessione per il server se la velocità di connessione è lenta o se la connessione è instabile. Il timeout della richiesta consigliato è di 0,5 secondi o meno. **Coda richieste**. Dimensione della cartella della coda di richieste. Quando si inviano più oggetti per la scansione in Sandbox, Kaspersky Endpoint Security crea una coda di richieste. Per impostazione predefinita, la dimensione della cartella della coda di richieste è limitata a 100 MB. Una volta raggiunta la dimensione massima, Sandbox interrompe l'aggiunta di nuove richieste alla coda e invia l'evento corrispondente a Kaspersky Security Center. È possibile configurare la dimensione della cartella della coda delle richieste in base alla configurazione del server. **Certificato TLS del server**. Per configurare una connessione attendibile con il server Sandbox (per Kaspersky Sandbox) o il server di Central Node (per KATA), è necessario preparare un certificato TLS. È quindi necessario aggiungere il certificato nel computer utilizzando un criterio. È inoltre necessario aggiungere il certificato al server Sandbox (per Kaspersky Sandbox) o al server di Central Node (per KATA). **Usa autenticazione a due vie** (solo per KATA Sandbox). Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.
Connessione ai server Sandbox	**Kaspersky Sandbox**. Impostazioni di connessione al server Sandbox. I server utilizzano immagini virtuali distribuite dei sistemi operativi Microsoft Windows per eseguire gli oggetti che devono essere sottoposti a scansione. È possibile immettere un indirizzo IP (IPv4 o IPv6) o un nome di dominio completo. **KATA Sandbox**. Impostazioni di connessione al server di Central Node. Central Node sceglie le impostazioni ottimali per la scansione e bilancia il carico tra i server Sandbox.
Azione se viene rilevata una minaccia	**Sposta la copia in Quarantena, elimina oggetto**. Se questa opzione è selezionata, Kaspersky Endpoint Security elimina l'oggetto dannoso trovato nel computer. Prima di eliminare l'oggetto, Kaspersky Endpoint Security crea una copia di backup nel caso in cui sia necessario ripristinare l'oggetto in un secondo momento. Kaspersky Endpoint Security sposta la copia di backup in Quarantena. **Esegui scansione delle aree critiche**. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue l'attività *Scansione delle aree critiche*. Per impostazione predefinita, Kaspersky Endpoint Security esamina la memoria del kernel, i processi in esecuzione e i settori di avvio del disco. **Crea attività di scansione IOC**. Se questa opzione è selezionata, Kaspersky Endpoint Security crea automaticamente l'attività *Scansione IOC (attività di scansione IOC autonoma)*. Per questa attività, è possibile configurare la modalità di esecuzione, l'ambito della scansione e l'azione al rilevamento IOC (*Sposta la copia in Quarantena, elimina oggetto* o *Esegui scansione delle aree critiche*). Per modificare altre impostazioni dell'attività di *Scansione IOC*, passare alle impostazioni dell'attività.
Ambito della scansione IOC	**Aree dei file critiche**. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue una scansione IOC solo nelle aree dei file critiche del computer: memoria del kernel e settori di avvio. **Aree dei file nell'unità di sistema del computer**. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue una scansione IOC sull'unità di sistema del computer.

Parametro	Descrizione
Esegui attività di scansione IOC	**Manualmente**. Modalità di esecuzione in cui è possibile avviare l'attività *Scansione IOC* manualmente nel momento più opportuno. **Automaticamente**. Modalità di esecuzione in cui Kaspersky Endpoint Security esegue automaticamente l'attività di *Scansione IOC* dopo il rilevamento di una minaccia. **Esegui solo quando il computer è inattivo**. Modalità di esecuzione in cui Kaspersky Endpoint Security esegue l'attività di *Scansione IOC* se lo screensaver è attivo o lo schermo è bloccato. Se l'utente sblocca il computer, Kaspersky Endpoint Security sospende l'attività. Ciò significa che il completamento dell'attività può richiedere diversi giorni.

Managed Detection and Response

Kaspersky Endpoint Security for Windows supporta l'integrazione con la soluzione Managed Detection and Response. La soluzione *Kaspersky Managed Detection and Response (MDR)* rileva e analizza automaticamente gli incidenti di sicurezza nell'infrastruttura. A tale scopo, MDR utilizza i dati di telemetria ricevuti dagli endpoint e dal Machine Learning. MDR invia i dati sugli incidenti agli esperti di Kaspersky. Gli esperti possono quindi elaborare l'incidente e, ad esempio, aggiungere una nuova voce ai database anti-virus. In alternativa, gli esperti possono proporre suggerimenti sull'elaborazione dell'incidente e, ad esempio, suggerire di isolare il computer dalla rete. Per informazioni dettagliate sul funzionamento della soluzione, consultare la Guida di Kaspersky Managed Detection and Response.

Impostazioni di Managed Detection and Response

Parametro	Descrizione
File di configurazione MDR	Il file BLOB contiene l'ID client e le informazioni sulla licenza per Kaspersky Managed Detection and Response. Il file BLOB si trova nell'archivio ZIP del file di configurazione MDR. È possibile ottenere l'archivio ZIP in Kaspersky Managed Detection and Response Console. Per informazioni dettagliate su un file BLOB, consultare la Guida di Kaspersky Managed Detection and Response.

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows include un agente integrato per la soluzione Kaspersky Endpoint Detection and Response Optimum (di seguito denominato anche "EDR Optimum"). A partire dalla versione 11.8.0, Kaspersky Endpoint Security for Windows include un agente integrato per la soluzione Kaspersky Endpoint Detection and Response Expert (di seguito denominata anche "EDR Expert"). *Kaspersky Endpoint Detection and Response* è una serie di soluzioni che consente di proteggere l'infrastruttura IT aziendale dalle minacce informatiche avanzate. La funzionalità delle soluzioni combina il rilevamento automatico delle minacce con la capacità di reagire a tali minacce per contrastare gli attacchi avanzati, inclusi nuovi exploit, ransomware, attacchi fileless, nonché metodi che utilizzano strumenti di sistemi legittimi. EDR Expert offre più funzionalità di monitoraggio e risposta delle minacce rispetto a EDR Optimal. Per informazioni dettagliate sulle soluzioni, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.

Kaspersky Endpoint Detection and Response esamina e analizza lo sviluppo delle minacce e fornisce *personale di sicurezza* o l'*Amministratore* con informazioni sul potenziale attacco necessarie per una risposta tempestiva. Kaspersky Endpoint Detection and Response mostra i dettagli degli avvisi in una finestra separata. Un *avviso* è un evento nell'infrastruttura IT aziendale che l'applicazione ha identificato come insolito o sospetto e che può rappresentare una minaccia per la sicurezza dell'infrastruttura IT aziendale. *Dettagli avviso* è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Per informazioni dettagliate sulla gestione dei dettagli degli avvisi, consultare la Guida di Kaspersky Endpoint Detection and Response Optimum e la Guida di Kaspersky Endpoint Detection and Response Expert.

È possibile configurare il componente Endpoint Detection and Response Optimum in Web Console e Cloud Console. Le impostazioni del componente Endpoint Detection and Response Expert (cloud) sono disponibili solo in Cloud Console.

Impostazioni di Endpoint Detection and Response

Parametro	Descrizione
Abilita registrazione delle attività di sistema avanzata	La telemetria estesa migliora la precisione del rilevamento IOC, ma utilizza più risorse del computer. È consigliabile abilitare la telemetria estesa nel computer per la scansione IOC retrospettiva. *Scansione IOC retrospettiva* è una modalità dell'attività *Scansione IOC* in cui Kaspersky Endpoint Security esegue la scansione degli indicatori di compromissione utilizzando i dati per un determinato periodo di tempo. Questa modalità è destinata alla ricerca di indicatori di compromissione tramite la telemetria del computer protetto, ad esempio attività di rete, processi, file e altri dati di telemetria. Se la telemetria estesa è disabilitata, Kaspersky Endpoint Security può ruotare le informazioni sugli indicatori di compromissione rilevati.
Isolamento di rete	Isolamento automatico del computer dalla rete in risposta alle minacce rilevate. Quando l'isolamento della rete è attivato, l'applicazione interrompe tutte le connessioni attive e blocca tutte le nuove connessioni TCP/IP sul computer. L'applicazione lascia attive solo le seguenti connessioni: • Connessioni elencate in Esclusioni dall'isolamento di rete. • Connessioni avviate dai servizi di Kaspersky Endpoint Security. • Connessioni avviate da Kaspersky Security Center Network Agent.
Sblocca automaticamente un dispositivo isolato tra (ore)	L'isolamento della rete può essere disattivato automaticamente dopo un periodo di tempo specificato o manualmente. Per impostazione predefinita, Kaspersky Endpoint Security disattiva Isolamento di rete 5 ore dopo l'inizio dell'isolamento.
Esclusioni dall'isolamento di rete	Elenco di regole per le esclusioni dall'isolamento di rete. Le connessioni di rete che soddisfano le regole non vengono bloccate sui computer quando Isolamento di rete è attivato. Per configurare le esclusioni dall'isolamento di rete, è possibile utilizzare un elenco di *profili di rete standard*. Per impostazione predefinita, le esclusioni includono i profili di rete che contengono regole che garantiscono il funzionamento costante dei dispositivi con il server DNS/DHCP e i ruoli client DNS/DHCP. È inoltre possibile modificare le impostazioni dei profili di rete standard o definire esclusioni manualmente. Le esclusioni specificate nelle proprietà dei criteri vengono applicate solo se Isolamento di rete viene attivato automaticamente in risposta a una minaccia rilevata. Le esclusioni specificate nelle proprietà del computer vengono applicate solo se Isolamento di rete è attivato manualmente nelle proprietà del computer in Kaspersky Security Center Console o nei dettagli degli avvisi.
Prevenzione dell'esecuzione	Controlla l'esecuzione dei file eseguibili e degli script, nonché l'apertura di file in formato Office. Ad esempio, è possibile impedire l'esecuzione di applicazioni considerate non sicure sul computer selezionato. Prevenzione dell'esecuzione supporta una serie di estensioni di file Office e una serie di interpreti di script. Per utilizzare il componente Prevenzione dell'esecuzione, è necessario aggiungere regole di prevenzione dell'esecuzione. *Regola di prevenzione dell'esecuzione* è un insieme di criteri che l'applicazione prende in considerazione quando reagisce all'esecuzione di un oggetto, ad esempio quando blocca l'esecuzione di un oggetto. L'applicazione identifica i file in base ai loro percorsi o checksum calcolati utilizzando gli algoritmi di hash MD5 e SHA256.

Parametro	Descrizione
Azione in caso di esecuzione o apertura di un oggetto vietato	**Blocca e aggiungi al registro eventi**. In questa modalità, l'applicazione blocca l'esecuzione di oggetti o l'apertura di documenti che soddisfano i criteri della regola di prevenzione. L'applicazione pubblica anche un evento sui tentativi di esecuzione di oggetti o apertura di documenti nel registro eventi di Windows e nel registro eventi di Kaspersky Security Center. **Aggiungi al registro eventi**. In questa modalità, Kaspersky Endpoint Security pubblica un evento sui tentativi di esecuzione di oggetti eseguibili o apertura di documenti che corrispondono ai criteri della regola di prevenzione nel registro eventi di Windows e in Kaspersky Security Center, ma non blocca il tentativo di esecuzione o apertura dell'oggetto o del documento. Questa modalità è selezionata per impostazione predefinita.
Regole di prevenzione dell'esecuzione	*Regola di prevenzione dell'esecuzione* è un insieme di criteri che l'applicazione prende in considerazione quando reagisce all'esecuzione di un oggetto, ad esempio quando blocca l'esecuzione di un oggetto. L'applicazione identifica i file in base ai loro percorsi o checksum calcolati utilizzando gli algoritmi di hash MD5 e SHA256.
Sandbox cloud	*Sandbox cloud* è una tecnologia che consente di rilevare le minacce avanzate in un computer. Kaspersky Endpoint Security inoltra automaticamente i file rilevati a Sandbox cloud per l'analisi. Sandbox cloud esegue questi file in un ambiente isolato per identificare le attività dannose e prendere decisioni sulla loro reputazione. I dati contenuti in questi file vengono quindi inviati a Kaspersky Security Network. Pertanto, se Sandbox cloud rileva un file dannoso, Kaspersky Endpoint Security eseguirà l'azione appropriata per eliminare questa minaccia in tutti i computer in cui viene rilevato tale file. La tecnologia Sandbox cloud è sempre abilitata ed è disponibile per tutti gli utenti di Kaspersky Security Network indipendentemente dal tipo di licenza in uso. Se questa casella di controllo è selezionata, Kaspersky Endpoint Security abiliterà il contatore delle minacce rilevate tramite Sandbox cloud nella finestra dell'applicazione principale in **Tecnologie di rilevamento delle minacce**. Kaspersky Endpoint Security indicherà anche la tecnologie di rilevamento delle minacce Sandbox cloud negli eventi delle applicazioni e nel *Rapporto sulle minacce* nella console Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security for Windows supporta l'integrazione con la soluzione Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* è una soluzione di sicurezza informatica aziendale che include le applicazioni Kaspersky che consentono a un'organizzazione di difendersi dalla maggior parte dei tipi di rischi informatici e coprire i più importanti scenari di propagazione delle minacce. I componenti di EDR Expert (on-premises) vengono distribuiti in Open Single Management Platform (OSMP). Questa piattaforma esegue scenari multipiattaforma in un'unica interfaccia e consente di integrare le applicazioni Kaspersky con applicazioni di terze parti in un sistema di protezione completo.

Uno degli elementi centrali della soluzione è *SIEM*. SIEM monitora gli eventi provenienti da tutti i componenti e correla questi eventi tra loro utilizzando regole definite dal fornitore e dall'utente. EDR Expert (on-premises) esamina i registri e la telemetria ricevuti dall'infrastruttura aziendale per rilevare automaticamente gli attacchi e consente di indagare sugli incidenti utilizzando un grafico di indagine unificato che combina tutti gli eventi raccolti in EDR Expert (on-premises), inclusi gli eventi delle applicazioni Kaspersky e prodotti di terze parti per la sicurezza delle informazioni.

Per la risposta a incidenti avanzati, EDR Expert (on-premises) utilizza scenari preimpostati e definiti dall'utente. È inoltre possibile utilizzare le azioni di reazione di applicazioni di terze parti e gli scenari di reazione che coinvolgono più applicazioni.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security for Windows supporta l'utilizzo con il componente Kaspersky Endpoint Detection and Response come parte della soluzione Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* è una soluzione progettata per il rilevamento tempestivo di minacce sofisticate come attacchi mirati, minacce APT (Advanced Persistent Threat), attacchi zero-day e di altro tipo. Kaspersky Anti Targeted Attack Platform include tre unità funzionali:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

È possibile acquistare tutte le unità funzionali o le singole unità funzionali separatamente. Per informazioni dettagliate sulla soluzione, consultare la Guida di Kaspersky Anti Targeted Attack Platform.

L'applicazione Kaspersky Endpoint Security viene installata nei singoli computer dell'infrastruttura IT aziendale e monitora continuamente i processi, le connessioni di rete aperte e i file modificati. Le informazioni sugli eventi nel computer (dati di telemetria) vengono inviate al server di Kaspersky Anti Targeted Attack Platform. In questo caso, Kaspersky Endpoint Security invia anche informazioni al server di Kaspersky Anti Targeted Attack Platform sulle minacce rilevate dall'applicazione, nonché informazioni sull'elaborazione dei risultati di tali minacce.

L'integrazione di EDR (KATA) e NDR (KATA) è configurata nella console di Kaspersky Security Center. L'agente integrato viene quindi gestito tramite la console di Kaspersky Anti Targeted Attack Platform, inclusa l'esecuzione delle attività, la gestione degli oggetti in quarantena, la visualizzazione dei rapporti e altre azioni.

Impostazioni Endpoint Detection and Response Expert (on-premises)

Parametro	Descrizione
Connessione ai server di raccolta della telemetria	Un *server di raccolta della telemetria* è un server che fa parte di una soluzione SIEM che raccoglie, normalizza, correla, analizza e archivia le informazioni sugli eventi che si verificano nel computer. Configurare quanto segue per la connessione ai server di raccolta della telemetria (KUMA): • **Timeout (sec)**. Timeout massimo del server di KUMA. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server. • **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un cripto-contenitore nella piattaforma Open Single Management (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). Dopo aver configurato le impostazioni del server, è necessario abilitare anche l'autenticazione a due vie nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password. Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.
Indirizzo e **Porta** (server di raccolta della telemetria)	Impostazioni per la connessione ai server di raccolta della telemetria. È possibile immettere un indirizzo IP (IPv4 o IPv6). È possibile aggiungere più indirizzi di server di raccolta della telemetria. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

Parametro	Descrizione
Invia telemetria ai server di raccolta della telemetria	Questa funzionalità consente di disattivare completamente l'invio dei dati di telemetria al server KATA. Ad esempio, se si utilizza Kaspersky Anti Targeted Attack Platform insieme a un'altra soluzione che usa anch'essa la telemetria, è possibile disattivare l'invio della telemetria per KATA (EDR). Ciò consente di ottimizzare il carico del server per queste soluzioni. Se è stata distribuita la soluzione Managed Detection and Response e KATA (EDR), è possibile utilizzare la telemetria MDR e creare attività Risposta alle minacce in KATA (EDR). • **Invia telemetria solo con IOA**. Questo consente di ottimizzare la telemetria e inviare solo la telemetria con IOA. *Indicatore di attacco (IOA)* è una regola che contiene una descrizione di un comportamento sospetto nel sistema che potrebbe indicare un attacco mirato. L'applicazione confronta il comportamento in corso nel sistema con queste regole e registra gli eventi indicativi di un attacco mirato. L'applicazione utilizza la tecnologia di *scansione in streaming*, che consente il monitoraggio in tempo reale di tali eventi. • **Ritardo di trasmissione eventi massimo (sec)**. L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione. L'impostazione predefinita è 30 secondi. • **Limita il numero di pacchetti di eventi per trasmissione**. L'applicazione si sincronizza con il server quando il buffer si riempie di eventi. L'impostazione predefinita è 1024 eventi. Questa funzione consente di disabilitare il buffering degli eventi prima della sincronizzazione con il server.
Abilita limitazione delle richieste	Questa funzionalità consente di ottimizzare il carico sul server. Se questa funzionalità è abilitata, l'applicazione limita la trasmissione degli eventi. Se il numero di eventi supera i limiti configurati, Kaspersky Endpoint Security interrompe l'invio degli eventi. Configurare le impostazioni di telemetria. • **Numero massimo di eventi all'ora**. L'applicazione analizza il flusso di dati di telemetria e limita l'invio degli eventi se il flusso di eventi supera il limite di eventi all'ora configurato. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora. L'impostazione predefinita è 3000 eventi all'ora. Se l'applicazione è installata in un server, il flusso di dati di telemetria è maggiore. Per i server, è consigliabile aumentare il valore a 60.000 eventi all'ora. • **Percentuale di eccedenza limite eventi**. L'applicazione ordina gli eventi in base al tipo (ad esempio, eventi di "Modifiche nel Registro di sistema") e limita la trasmissione degli eventi se il rapporto tra eventi dello stesso tipo e il numero totale di eventi supera il limite percentuale configurato. Kaspersky Endpoint Security riprende l'invio degli eventi quando il rapporto tra altri eventi e il numero totale di eventi diventa di nuovo sufficientemente elevato. L'impostazione predefinita è 15%.
Invia richiesta di sincronizzazione al server ogni (min)	Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security invia informazioni sulle attività e le impostazioni dell'applicazione modificate.
Connessione ai server di risposta	Un *server di risposta* è un server per la ricezione e la scansione dei dati, lo studio del comportamento degli oggetti e la pubblicazione dei risultati di tali studi. Configurare quanto segue per la connessione ai server di risposta: • **Timeout (sec)**. Timeout massimo del server di KUMA. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server. • **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server. È possibile ottenere un certificato TLS nella Open Single Management Platform (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un cripto-contenitore nella piattaforma Open Single Management (vedere le istruzioni nella Guida di Kaspersky Endpoint Detection and Response Expert (on-premises)). Dopo aver configurato le impostazioni del server, è necessario abilitare anche l'autenticazione a due vie nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password.
Indirizzo e **Porta** (server di risposta)	Impostazioni per la connessione ai server di risposta. È possibile immettere un indirizzo IP (IPv4 o IPv6). È possibile aggiungere più indirizzi di server di raccolta della telemetria. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

Parametro	Descrizione
Invia richiesta di sincronizzazione al server ogni (min)	Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security invia informazioni sulle attività e le impostazioni dell'applicazione modificate.
Connessione ai server KATA	Configurare quanto segue per la connessione al server di Central Node: • **Timeout (sec)**. Timeout massimo di risposta del server di Central Node. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server Central Node. • **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server di Central Node. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). • **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password. Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.
Indirizzo e **Porta** (server KATA)	Impostazioni per la connessione ai server di Kaspersky Anti Targeted Attack Platform. Immettere l'indirizzo IP (IPv4 o IPv6) e la porta del server di Central Node a cui connettersi. È possibile aggiungere più indirizzi server di Central Node. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.
Invia telemetria a KATA	Questa funzionalità consente di disattivare completamente l'invio dei dati di telemetria al server KATA. Ad esempio, se si utilizza Kaspersky Anti Targeted Attack Platform insieme a un'altra soluzione che usa anch'essa la telemetria, è possibile disattivare l'invio della telemetria per KATA (EDR). Ciò consente di ottimizzare il carico del server per queste soluzioni. Se è stata distribuita la soluzione Managed Detection and Response e KATA (EDR), è possibile utilizzare la telemetria MDR e creare attività Risposta alle minacce in KATA (EDR). Configurare le impostazioni di telemetria. • **Ritardo di trasmissione eventi massimo (sec)**. L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione. L'impostazione predefinita è 30 secondi. • **Numero massimo di pacchetti eventi**. L'applicazione si sincronizza con il server quando il buffer si riempie di eventi. L'impostazione predefinita è 1024 eventi.
Abilita limitazione delle richieste	Questa funzionalità consente di ottimizzare il carico sul server. Se questa funzionalità è abilitata, l'applicazione limita la trasmissione degli eventi. Se il numero di eventi supera i limiti configurati, Kaspersky Endpoint Security interrompe l'invio degli eventi. Configurare le impostazioni di telemetria. • **Numero massimo di eventi all'ora**. L'applicazione analizza il flusso di dati di telemetria e limita l'invio degli eventi se il flusso di eventi supera il limite di eventi all'ora configurato. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora. L'impostazione predefinita è 3000 eventi all'ora. Se l'applicazione è installata in un server, il flusso di dati di telemetria è maggiore. Per i server, è consigliabile aumentare il valore a 60.000 eventi all'ora. • **Percentuale di eccedenza limite eventi**. L'applicazione ordina gli eventi in base al tipo (ad esempio, eventi di "Modifiche nel Registro di sistema") e limita la trasmissione degli eventi se il rapporto tra eventi dello stesso tipo e il numero totale di eventi supera il limite percentuale configurato. Kaspersky Endpoint Security riprende l'invio degli eventi quando il rapporto tra altri eventi e il numero totale di eventi diventa di nuovo sufficientemente elevato. L'impostazione predefinita è 15%.

Network Detection and Response (KATA)

Kaspersky Endpoint Security for Windows supporta l'utilizzo con il componente Kaspersky Network Detection and Response come parte della soluzione Kaspersky Anti Targeted Attack Platform (EDR (KATA)). *Kaspersky Anti Targeted Attack Platform* è una soluzione progettata per il rilevamento tempestivo di minacce sofisticate come attacchi mirati, minacce APT (Advanced Persistent Threat), attacchi zero-day e di altro tipo. Kaspersky Anti Targeted Attack Platform include tre unità funzionali:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

È possibile acquistare tutte le unità funzionali o le singole unità funzionali separatamente. Per informazioni dettagliate sulla soluzione, consultare la Guida di Kaspersky Anti Targeted Attack Platform.

L'applicazione Kaspersky Endpoint Security viene installata nei singoli computer dell'infrastruttura IT aziendale e monitora continuamente i processi, le connessioni di rete aperte e i file modificati. Le informazioni sugli eventi nel computer (dati di telemetria) vengono inviate al server di Kaspersky Anti Targeted Attack Platform. In questo caso, Kaspersky Endpoint Security invia anche informazioni al server di Kaspersky Anti Targeted Attack Platform sulle minacce rilevate dall'applicazione, nonché informazioni sull'elaborazione dei risultati di tali minacce.

L'integrazione di EDR (KATA) e NDR (KATA) è configurata nella console di Kaspersky Security Center. L'agente integrato viene quindi gestito tramite la console di Kaspersky Anti Targeted Attack Platform, inclusa l'esecuzione delle attività, la gestione degli oggetti in quarantena, la visualizzazione dei rapporti e altre azioni.

Parametri di Network Detection and Response (KATA)

Parametro	Descrizione
Impostazioni della connessione al server	**Timeout (sec)**. Timeout massimo di risposta del server di Central Node. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server Central Node. **Certificato TLS del server**. Certificato TLS per stabilire una connessione attendibile con il server di Central Node. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password. Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.
Indirizzo e **Porta**	Impostazioni per la connessione ai server di Kaspersky Anti Targeted Attack Platform. Immettere l'indirizzo IP (IPv4 o IPv6) e la porta del server di Central Node a cui connettersi. È possibile aggiungere più indirizzi server di Central Node. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.
Invia richiesta di sincronizzazione al server NDR ogni (min)	Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security invia informazioni sulle attività e le impostazioni dell'applicazione modificate.

Parametro	Descrizione
Ritardo di trasmissione eventi massimo (sec)	L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione. L'impostazione predefinita è 30 secondi.
Abilita limitazione delle richieste	Questa funzionalità consente di ottimizzare il carico sul server. Se questa funzionalità è abilitata, l'applicazione limita la trasmissione degli eventi. Se il numero di eventi supera i limiti configurati, Kaspersky Endpoint Security interrompe l'invio degli eventi.
Numero massimo di eventi all'ora	L'applicazione analizza il flusso di dati di telemetria e limita l'invio degli eventi se il flusso di eventi supera il limite di eventi all'ora configurato. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora. L'impostazione predefinita è 3000 eventi all'ora. Se l'applicazione è installata in un server, il flusso di dati di telemetria è maggiore. Per i server, è consigliabile aumentare il valore a 60.000 eventi all'ora.
Percentuale di eccedenza limite eventi	L'applicazione ordina gli eventi in base al tipo (ad esempio, eventi di "Modifiche nel Registro di sistema") e limita la trasmissione degli eventi se il rapporto tra eventi dello stesso tipo e il numero totale di eventi supera il limite percentuale configurato. Kaspersky Endpoint Security riprende l'invio degli eventi quando il rapporto tra altri eventi e il numero totale di eventi diventa di nuovo sufficientemente elevato. L'impostazione predefinita è 15%.

Integrazione di KUMA

Kaspersky Endpoint Security for Windows supporta la soluzione Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* è una soluzione SIEM (Security Information and Event Management) per l'infrastruttura IT delle organizzazioni. KUMA consente di rilevare, analizzare e attenuare le minacce alla sicurezza prima che possano causare danni.

Impostazioni di integrazione di KUMA

Parametro	Descrizione
Ritardo massimo nell'invio degli eventi (sec)	L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione. L'impostazione predefinita è 30 secondi.
Connessione ai server KUMA	**Timeout (sec)**. Tempo massimo di attesa di una risposta dal server KUMA (per impostazione predefinita, il valore è 5 secondi). Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server di KUMA. **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server di KUMA. È possibile ottenere un certificato TLS nella console Kaspersky Unified Monitoring and Analysis Platform (vedere le istruzioni nella Guida di Kaspersky Unified Monitoring and Analysis Platform). Per stabilire una connessione attendibile, nella console KUMA, nelle impostazioni del connettore TCP, è necessario selezionare l'estensione **With verification** Modalità TLS (vedere le impostazioni per il connettore di tipo TCP nella Guida di Kaspersky Unified Monitoring and Analysis Platform). **Usa autenticazione a due vie**. Autenticazione a due vie durante la creazione di una connessione sicura tra KES e KUMA. Per utilizzare l'autenticazione a due vie, nella console KUMA, nelle impostazioni del connettore, è necessario selezionare la modalità TLS **Custom PFX with client authentication** (vedere le impostazioni del connettore nella Guida di Kaspersky Unified Monitoring and Analysis Platform). Quindi è necessario scaricare un certificato del server e impostare una password per proteggere il contenitore crittografico. Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore crittografico senza una password.
Server KUMA	Connessione alle impostazioni dei server di Kaspersky Unified Monitoring and Analysis Platform. È possibile immettere un indirizzo IP (IPv4 o IPv6). È possibile aggiungere più indirizzi server KUMA. Kaspersky Endpoint Security tenta di connettersi al server utilizzando il primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi utilizzando il secondo indirizzo IP nell'elenco e così via.

Criptaggio dell'intero disco

È possibile selezionare una tecnologia di criptaggio: Criptaggio disco Kaspersky o Crittografia unità BitLocker (di seguito denominato semplicemente "BitLocker").

Criptaggio disco Kaspersky

Criptaggio disco Kaspersky non è supportato nei computer basati su Arm.

Una volta criptati i dischi rigidi di sistema, al successivo avvio del computer l'utente deve eseguire l'autenticazione utilizzando l'Agente di Autenticazione prima di poter accedere ai dischi rigidi e caricare il sistema operativo. Questo richiede l'immissione della password del token o della smart card connessa al computer oppure il nome utente e la password dell'account per l'Agente di Autenticazione creato dall'amministratore della rete LAN tramite l'attività *Gestisci account dell'Agente di Autenticazione*. Questi account sono basati sugli account di Microsoft Windows con cui gli utenti eseguono l'accesso al sistema operativo. È inoltre possibile utilizzare la tecnologia SSO Single Sign-On, che consente di accedere automaticamente al sistema operativo utilizzando il nome utente e la password dell'account dell'Agente di Autenticazione.

L'autenticazione dell'utente nell'Agente di Autenticazione può essere eseguita in due modi:

- Immettere il nome e la password dell'account per l'Agente di Autenticazione creato dall'amministratore della rete LAN utilizzando gli strumenti di Kaspersky Security Center.
- Immettere la password di un token o di una smart card connessa al computer.

  L'utilizzo di un token o di una smart card è disponibile solo se i dischi rigidi del computer sono stati criptati utilizzando l'algoritmo di criptaggio AES256. Se i dischi rigidi del computer sono stati criptati utilizzando l'algoritmo di criptaggio AES56, l'aggiunta del file del certificato elettronico al comando verrà negata.

Crittografia unità BitLocker

BitLocker è una tecnologia di criptaggio integrata nei sistemi operativi Windows. Kaspersky Endpoint Security consente di controllare e gestire Bitlocker utilizzando l'infrastruttura Kaspersky Next. BitLocker cripta i volumi logici. BitLocker non può essere utilizzato per il criptaggio delle unità rimovibili. Per informazioni dettagliate su BitLocker, consultare la documentazione di Microsoft.

Quando si cripta il disco, BitLocker inserisce il caricatore di avvio e altri file ausiliari nella system partition. Questa partizione non è criptata. Il sistema operativo crea automaticamente la partizione di sistema durante l'installazione di Windows. Se il disco è completamente partizionato prima dell'installazione di Windows, il sistema operativo non è in grado di creare una partizione di sistema. In questo caso, quando si avvia il criptaggio del disco BitLocker, il sistema operativo richiede all'utente di ripartizionare il disco e creare una partizione di sistema. Dopo la creazione di una partizione di sistema, il sistema operativo avvia il criptaggio BitLocker.

BitLocker consente la memorizzazione sicura delle chiavi di accesso utilizzando un Trusted Platform Module. Per *Trusted Platform Module* (TPM) si intende un microchip sviluppato per garantire funzioni di base relative alla sicurezza (ad esempio per archiviare le chiavi di criptaggio). Un Trusted Platform Module viene solitamente installato nella scheda madre del computer e interagisce con tutti gli altri componenti di sistema tramite il bus hardware. L'utilizzo di TPM è il modo più sicuro per memorizzare le chiavi di accesso BitLocker, dal momento che consente la verifica dell'integrità di sistema prima dell'avvio. È comunque possibile criptare le unità in un computer senza un TPM. In questo caso, la chiave di accesso verrà criptata con una password. BitLocker utilizza i seguenti metodi di autenticazione:

- TPM.
- TPM e PIN.
- Password.

Dopo il criptaggio del disco rigido di sistema, l'utente deve eseguire l'autenticazione BitLocker per avviare il sistema operativo. Dopo l'autenticazione, BitLocker consente all'utente di accedere. BitLocker non supporta la tecnologia SSO (Single Sign-On).

Dopo il criptaggio di un'unità, BitLocker crea una chiave di ripristino. Kaspersky Endpoint Security invia la chiave di ripristino a Kaspersky Security Center in modo da poter ripristinare l'accesso al disco, se ad esempio un utente ha dimenticato la propria password.

Se un utente cripta un disco utilizzando BitLocker, Kaspersky Endpoint Security invierà la chiave di ripristino e informazioni sul criptaggio del disco a Kaspersky Security Center.

Se si utilizzano criteri di gruppo Windows, disattivare la gestione BitLocker nelle impostazioni dei criteri. Le impostazioni dei criteri Windows potrebbero entrare in conflitto con le impostazioni dei criteri Kaspersky Endpoint Security. Durante il criptaggio di un'unità, potrebbero verificarsi errori.

Impostazioni del componente Criptaggio disco Kaspersky

Parametro	Descrizione
Modalità di criptaggio	**Cripta tutti i dischi rigidi**. Se questa opzione è selezionata, l'applicazione cripta tutti i dischi rigidi quando viene applicato il criterio. Se nel computer sono installati diversi sistemi operativi, dopo il criptaggio sarà possibile caricare solo il sistema operativo in cui è installata l'applicazione. **Decripta tutti i dischi rigidi**. Se questa opzione è selezionata, l'applicazione decripta tutti i dischi rigidi criptati precedentemente quando viene applicato il criterio. **Mantieni invariato**. Se questo elemento è selezionato, l'applicazione mantiene le unità nello stato precedente quando viene applicato il criterio. Se l'unità era criptata, rimane criptata. Se l'unità era decriptata, rimane decriptata. Questo elemento è selezionato per impostazione predefinita.
Durante il criptaggio, crea automaticamente gli account dell'Agente di Autenticazione per gli utenti Windows	Se questa casella di controllo è selezionata, l'applicazione crea gli account dell'Agente di Autenticazione in base all'elenco degli account utente di Windows nel computer. Per impostazione predefinita, Kaspersky Endpoint Security utilizza tutti gli account locali e di dominio con i quali l'utente ha effettuato l'accesso al sistema operativo negli ultimi 30 giorni.

Parametro	Descrizione
Impostazioni di creazione dell'account per l'Agente di Autenticazione	**Tutti gli account nel computer**. Tutti gli account nel computer che sono stati attivi in qualsiasi momento. **Tutti gli account di dominio nel computer**. Tutti gli account nel computer che appartengono a qualche dominio e che sono stati attivi in qualsiasi momento. **Tutti gli account locali nel computer**. Tutti gli account locali nel computer che sono stati attivi in qualsiasi momento. **Account di servizio con una password monouso**. L'account di servizio è necessario per accedere al computer, ad esempio quando l'utente dimentica la password. È inoltre possibile utilizzare l'account di servizio come account di riserva. È necessario inserire il nome dell'account (per impostazione predefinita, `ServiceAccount`). Kaspersky Endpoint Security crea automaticamente una password. È possibile trovare la password nella console di Kaspersky Security Center. **Amministratore locale**. Kaspersky Endpoint Security crea un account utente dell'Agente di Autenticazione per l'amministratore locale del computer. **Responsabile computer**. Kaspersky Endpoint Security crea un account utente dell'Agente di Autenticazione per l'account del responsabile del computer. È possibile vedere quale account ha il ruolo di responsabile del computer nelle proprietà del computer in Active Directory. Per impostazione predefinita, il ruolo di responsabile del computer non è definito, ovvero non corrisponde ad alcun account. **Account attivo**. Kaspersky Endpoint Security crea automaticamente un account dell'Agente di Autenticazione per l'account attivo al momento del criptaggio del disco.
Crea automaticamente gli account dell'Agente di Autenticazione per tutti gli utenti di questo computer al momento dell'accesso	Se questa casella di controllo è selezionata, l'applicazione controlla le informazioni sugli account utente di Windows nel computer prima di avviare l'Agente di Autenticazione. Se Kaspersky Endpoint Security rileva un account utente Windows che non dispone di un account dell'Agente di Autenticazione, l'applicazione creerà un nuovo account per accedere alle unità criptate. Il nuovo account dell'Agente di Autenticazione avrà le seguenti impostazioni predefinite: solo accesso protetto da password e modifica della password alla prima autenticazione. Pertanto, non è necessario aggiungere manualmente gli account dell'Agente di Autenticazione utilizzando l'attività *Gestisci account dell'Agente di Autenticazione* per i computer con unità già criptate.
Salva il nome utente immesso nell'Agente di Autenticazione	Se la casella di controllo è selezionata, l'applicazione salva il nome dell'account Agente di Autenticazione. Non verrà richiesto di immettere il nome dell'account durante il successivo tentativo di eseguire l'autenticazione nell'Agente di Autenticazione con lo stesso account.
Cripta solo lo spazio su disco utilizzato (riduce i tempi di criptaggio)	Questa casella di controllo consente di abilitare o disabilitare l'opzione che limita l'area di criptaggio ai soli settori occupati del disco rigido. Questo limite consente di ridurre il tempo di criptaggio. L'abilitazione o la disabilitazione della funzionalità **Cripta solo lo spazio su disco utilizzato (riduce i tempi di criptaggio)** dopo l'avvio del criptaggio non comporta la modifica di questa impostazione finché i dischi rigidi non vengono decriptati. È necessario selezionare o deselezionare la casella di controllo prima di avviare il criptaggio. Se la casella di controllo è selezionata, vengono criptate solo le parti del disco rigido che sono occupate da file. Kaspersky Endpoint Security cripta automaticamente i nuovi dati man mano che vengono aggiunti. Se la casella di controllo è deselezionata, viene criptato l'intero disco rigido, inclusi i frammenti residui dei file precedentemente eliminati e modificati. Questa opzione è consigliata per i nuovi dischi rigidi in cui non sono stati modificati o eliminati dati. Se si applica il criptaggio a un disco rigido già in uso, è consigliabile criptare l'intero disco rigido. Questo garantisce la protezione di tutti i dati, anche dei dati eliminati potenzialmente ripristinabili. Per impostazione predefinita, la casella di controllo è deselezionata.
Usa Legacy USB Support (opzione non consigliata)	Questa casella di controllo abilita o disabilita la funzionalità Legacy USB Support. *Legacy USB Support* **è** una funzione BIOS/UEFI che consente di utilizzare i dispositivi USB (ad esempio un token di sicurezza) durante la fase di avvio del computer prima dell'avvio del sistema operativo (modalità BIOS). Legacy USB Support non influisce sul supporto dei dispositivi USB dopo l'avvio del sistema operativo. Se la casella di controllo è selezionata, il supporto dei dispositivi USB durante l'avvio iniziale del computer sarà abilitato. Quando la funzione Legacy USB Support è abilitata, l'Agente di Autenticazione in modalità BIOS non supporta l'utilizzo dei token tramite USB. È consigliabile utilizzare questa opzione solo se si verifica un problema di compatibilità hardware e solo per i computer in cui si è verificato il problema.

Parametro	Descrizione
Impostazioni password	Impostazioni di sicurezza della password dell'account dell'Agente di Autenticazione Quando si utilizza la tecnologia Single Sign-On, l'Agente di Autenticazione ignora i requisiti di sicurezza della password specificati in Kaspersky Security Center. È possibile impostare i requisiti di sicurezza della password nelle impostazioni del sistema operativo.
Utilizza la tecnologia SSO (Single Sign-On)	La tecnologia SSO rende possibile l'utilizzo delle stesse credenziali per accedere ai dischi rigidi criptati e al sistema operativo. Se la casella di controllo è selezionata, è necessario immettere le credenziali dell'account per accedere ai dischi rigidi criptati e quindi accedere automaticamente al sistema operativo. Se la casella di controllo è deselezionata, per accedere ai dischi rigidi criptati e quindi accedere al sistema operativo è necessario immettere separatamente le credenziali per l'acceso ai dischi rigidi criptati e le credenziali dell'account utente del sistema operativo.
Esegui il wrapping dei fornitori di credenziali di terzi	Kaspersky Endpoint Security supporta il provider di credenziali di terzi ADSelfService Plus. Quando si utilizzano provider di credenziali di terzi, Agente di autenticazione intercetta la password prima del caricamento del sistema operativo. Ciò significa che un utente deve immettere una password solo una volta quando accede a Windows. Dopo aver effettuato l'accesso a Windows, l'utente può utilizzare le funzionalità di un provider di credenziali di terzi, ad esempio per l'autenticazione nei servizi aziendali. I provider di credenziali di terzi consentono inoltre agli utenti di reimpostare in modo indipendente la propria password. In questo caso, Kaspersky Endpoint Security aggiorna automaticamente la password per Agente di autenticazione. Se si utilizza un provider di credenziali di terzi non supportato dall'applicazione, è possibile che si verifichino alcune limitazioni nel funzionamento della tecnologia Single Sign-On.
Guida	**Autenticazione**. Testo della guida visualizzato nella finestra dell'Agente di Autenticazione quando si inseriscono le credenziali dell'account. **Cambia password**. Testo della guida visualizzato nella finestra dell'Agente di Autenticazione quando si modifica la password per l'account dell'Agente di Autenticazione. **Ripristina password**. Testo della guida visualizzato nella finestra dell'Agente di Autenticazione quando si ripristina la password per l'account dell'Agente di Autenticazione.

Impostazioni del componente Crittografia unità BitLocker

Parametro	Descrizione
Modalità di criptaggio	**Cripta tutti i dischi rigidi**. Se questa opzione è selezionata, l'applicazione cripta tutti i dischi rigidi quando viene applicato il criterio. Se nel computer sono installati diversi sistemi operativi, dopo il criptaggio sarà possibile caricare solo il sistema operativo in cui è installata l'applicazione. **Decripta tutti i dischi rigidi**. Se questa opzione è selezionata, l'applicazione decripta tutti i dischi rigidi criptati precedentemente quando viene applicato il criterio. **Mantieni invariato**. Se questo elemento è selezionato, l'applicazione mantiene le unità nello stato precedente quando viene applicato il criterio. Se l'unità era criptata, rimane criptata. Se l'unità era decriptata, rimane decriptata. Questo elemento è selezionato per impostazione predefinita.
Consenti l'utilizzo dell'autenticazione BitLocker che richiede l'input da tastiera prima dell'avvio nei tablet	Utilizzo dell'autenticazione che richiede l'input di dati in un ambiente di preavvio, anche se la piattaforma non dispone di funzionalità di input in fase di preavvio (ad esempio, con le tastiere touchscreen nei tablet). Il touchscreen dei computer tablet non è disponibile nell'ambiente di preavvio. Per completare l'autenticazione BitLocker nei computer tablet, l'utente deve connettere ad esempio una tastiera USB. Se la casella di controllo è selezionata, l'utilizzo dell'autenticazione tramite input di preavvio è consentito. È consigliabile utilizzare questa impostazione solo per i dispositivi dotati di strumenti alternativi per l'input dei dati, ad esempio una tastiera USB in aggiunta alle tastiere touchscreen. Se la casella di controllo è deselezionata, Crittografia unità BitLocker non è disponibile nei tablet.
Usa criptaggio hardware (Windows 8 e versioni successive)	Se la casella di controllo è selezionata, l'applicazione applica il criptaggio hardware. Questo consente di aumentare la velocità del criptaggio e di utilizzare meno risorse del computer.

Parametro	Descrizione
Cripta solo lo spazio su disco utilizzato (Windows 8 e versioni successive)	Questa casella di controllo consente di abilitare o disabilitare l'opzione che limita l'area di criptaggio ai soli settori occupati del disco rigido. Questo limite consente di ridurre il tempo di criptaggio. L'abilitazione o la disabilitazione della funzionalità **Cripta solo lo spazio su disco utilizzato (riduce i tempi di criptaggio)** dopo l'avvio del criptaggio non comporta la modifica di questa impostazione finché i dischi rigidi non vengono decriptati. È necessario selezionare o deselezionare la casella di controllo prima di avviare il criptaggio. Se la casella di controllo è selezionata, vengono criptate solo le parti del disco rigido che sono occupate da file. Kaspersky Endpoint Security cripta automaticamente i nuovi dati man mano che vengono aggiunti. Se la casella di controllo è deselezionata, viene criptato l'intero disco rigido, inclusi i frammenti residui dei file precedentemente eliminati e modificati. Questa opzione è consigliata per i nuovi dischi rigidi in cui non sono stati modificati o eliminati dati. Se si applica il criptaggio a un disco rigido già in uso, è consigliabile criptare l'intero disco rigido. Questo garantisce la protezione di tutti i dati, anche dei dati eliminati potenzialmente ripristinabili. Per impostazione predefinita, la casella di controllo è deselezionata.
Metodo di autenticazione	**Solo password (Windows 8 e versioni successive)** Se questa opzione è selezionata, Kaspersky Endpoint Security richiede una password quando si tenta di accedere a un'unità crittografata. Questa opzione può essere selezionata quando non viene utilizzato un Trusted Platform Module (TPM). **Trusted platform module (TPM)** Se questa opzione è selezionata, BitLocker utilizza Trusted Platform Module (TPM). Per *Trusted Platform Module* (TPM) si intende un microchip sviluppato per garantire funzioni di base relative alla sicurezza (ad esempio per archiviare le chiavi di criptaggio). Un Trusted Platform Module in genere è installato nella scheda madre del computer e interagisce con tutti gli altri componenti del sistema tramite il bus hardware. Per i computer che eseguono Windows 7 o Windows Server 2008 R2, è disponibile solo il criptaggio mediante un modulo TPM. Se non è installato un modulo TPM, non è possibile eseguire il criptaggio BitLocker. L'utilizzo di una password in questi computer non è supportato. Un dispositivo dotato di un Trusted Platform Module può creare chiavi di criptaggio che possono essere decriptate solo con il dispositivo. Un Trusted Platform Module cripta le chiavi di criptaggio con la relativa chiave di archiviazione radice. La chiave di archiviazione radice è memorizzata nel Trusted Platform Module. Questo fornisce un livello di protezione aggiuntivo contro i tentativi di violare le chiavi di criptaggio. Questa azione è selezionata per impostazione predefinita. È possibile impostare un ulteriore livello di protezione per l'accesso alla chiave di criptaggio, nonché criptare la chiave con una password o un PIN: • **Usa PIN per TPM**. Se questa casella di controllo è selezionata, è possibile utilizzare un codice PIN per ottenere l'accesso a una chiave di criptaggio archiviata in un Trusted Platform Module (TPM). Se questa casella di controllo è deselezionata, l'utilizzo di codici PIN non è consentito. Per accedere alla chiave di criptaggio, è necessario immettere la password. • **Trusted platform module (TPM) o password se TMP non è disponibile**. Se questa opzione è selezionata, l'utente può utilizzare una password per ottenere l'accesso alle chiavi di criptaggio quando un Trusted Platform Module non è disponibile. Se la casella di controllo è deselezionata e TPM non è disponibile, il criptaggio dell'intero disco non verrà avviato. Il metodo di autenticazione selezionato deve essere configurato specificando i requisiti di password o PIN: • **Lunghezza minima PIN (caratteri)** (il valore predefinito è 6). • **Lunghezza minima password (caratteri)** (il valore predefinito è 8). • **Numero massimo di password/PIN memorizzati** (il valore predefinito è 5). • **Limita periodo di validità password / PIN per TPM (giorni)** (disabilitato per impostazione predefinita). • **Usa PIN avanzato (lettere e numeri)**. *PIN avanzato* consente di utilizzare altri caratteri oltre a quelli numerici: lettere latine maiuscole e minuscole, caratteri speciali e spazi. Disabilitato per impostazione predefinita.
Ricrea automaticamente la chiave di ripristino (giorni)	Aggiorna automaticamente la password per ripristinare l'accesso a un'unità protetta da BitLocker. Se la casella di controllo è selezionata, specificare il periodo di validità della password della chiave di ripristino. In questo modo, si contribuisce a impedire il riutilizzo della password della chiave di ripristino.

Criptaggio a livello di file

Il criptaggio dei file non è supportato nei computer basati su Arm.

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server.

È possibile compilare elenchi di file (per estensione o gruppi di estensioni) e cartelle nelle unità locali del computer, nonché creare regole per il criptaggio dei file creati da applicazioni specifiche. Dopo l'applicazione di un criterio, Kaspersky Endpoint Security cripta e decripta i seguenti file:

- file aggiunti singolarmente agli elenchi per il criptaggio e il decriptaggio;
- file memorizzati in cartelle aggiunte agli elenchi per il criptaggio e il decriptaggio;
- File creati da applicazioni distinte.

Il criptaggio dei file presenta le seguenti funzionalità speciali:

- Kaspersky Endpoint Security cripta/decripta i file nelle cartelle predefinite solo per i profili utente locali del sistema operativo. Kaspersky Endpoint Security non cripta o decripta i file nelle cartelle predefinite di profili utente mobili, profili utente bloccati, profili utente temporanei o cartelle reindirizzate.
- Kaspersky Endpoint Security non esegue il criptaggio dei file la cui modifica può danneggiare il sistema operativo e le applicazioni installate. Ad esempio, i seguenti file e cartelle con tutte le cartelle nidificate sono inclusi nell'elenco delle esclusioni di criptaggio:
  - %WINDIR%;
  - %PROGRAMFILES% e %PROGRAMFILES(X86)%;
  - File del Registro di sistema di Windows.

  L'elenco delle esclusioni di criptaggio non può essere visualizzato o modificato. Anche se i file e le cartelle presenti nell'elenco delle esclusioni di criptaggio possono essere aggiunti all'elenco di criptaggio, non verranno criptati durante il criptaggio dei file.

Impostazioni del componente Criptaggio a livello di file

Parametro	Descrizione
Modalità di criptaggio	**Mantieni invariato**. Se questo elemento è selezionato, Kaspersky Endpoint Security mantiene invariati i file e le cartelle, senza criptarli o decriptarli. **In base alle regole**. Se questo elemento è selezionato, Kaspersky Endpoint Security cripta i file e le cartelle in base alle regole di criptaggio, decripta i file e le cartelle in base alle regole di decriptaggio e regola l'accesso delle applicazioni ai file criptati in base alle regole dell'applicazione. **Decripta tutto**. Se questo elemento è selezionato, Kaspersky Endpoint Security decripta tutti i file e le cartelle criptati.

Parametro	Descrizione
Criptaggio	Questa scheda mostra le regole di criptaggio per i file archiviati nelle unità locali. È possibile aggiungere file come segue: • **Cartelle predefinite**. Kaspersky Endpoint Security consente di aggiungere le seguenti aree: **Documenti**. File nella cartella *Documenti* standard del sistema operativo e relative sottocartelle. **Preferiti**. File nella cartella *Preferiti* standard del sistema operativo e relative sottocartelle. **Desktop**. File nella cartella *Desktop* standard del sistema operativo e relative sottocartelle. **File temporanei**. File temporanei relativi all'esecuzione delle applicazioni installate nel computer. Le applicazioni di Microsoft Office creano ad esempio file temporanei contenenti copie di backup dei documenti. **File di Outlook**. File relativi all'esecuzione del client di posta di Outlook: file di dati (PST), file di dati offline (OST), file della rubrica offline (OAB) e file della rubrica personale (PAB). • **Cartella personalizzata**. È possibile digitare il percorso della cartella. Quando si aggiunge il percorso di una cartella, attenersi alle seguenti regole: Utilizzare una variabile di ambiente (ad esempio `%FOLDER%\UserFolder\`). È possibile utilizzare una variabile di ambiente solo una volta e solo all'inizio del percorso. Non utilizzare percorsi relativi. Non utilizzare i caratteri `*` e `?`. Non utilizzare percorsi UNC. Utilizzare `;` o `,` come carattere separatore. • **File per estensione**. È possibile selezionare i gruppi di estensioni dall'elenco, ad esempio il gruppo di estensioni *Archivi*. È inoltre possibile aggiungere manualmente l'estensione del file.
Decriptaggio	Questa scheda mostra le regole di decriptaggio dei file archiviati nelle unità locali.
Regole per le applicazioni	La scheda visualizza una tabella che contiene le regole di accesso ai file criptati per le applicazioni e le regole di criptaggio per i file creati o modificati dalle singole applicazioni.
Pacchetti criptati	Requisiti di sicurezza della password da soddisfare durante la creazione di pacchetti criptati.

Criptaggio unità rimovibili

Il criptaggio delle unità rimovibili non è supportato nei computer basati su Arm.

Il componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Windows per server.

Kaspersky Endpoint Security supporta il criptaggio dei file nei file system FAT32 e NTFS. Se un'unità rimovibile con un file system non supportato è connessa al computer, l'attività di criptaggio per l'unità rimovibile termina con un errore e Kaspersky Endpoint Security assegna lo stato di sola lettura all'unità rimovibile.

Per proteggere i dati nelle unità rimovibili, è possibile utilizzare i seguenti tipi di criptaggio:

- Full Disk Encryption (FDE).

  Criptaggio dell'intera unità rimovibile, incluso il file system.

  Non è possibile accedere ai dati criptati al di fuori della rete aziendale. Inoltre, non è possibile accedere ai dati criptati all'interno della rete aziendale se il computer non è connesso a Kaspersky Security Center (ad es. su un computer "guest").

- File Level Encryption (FLE).

  Criptaggio dei soli file in un'unità rimovibile. Il file system rimane invariato.

Il criptaggio dei file nelle unità rimovibili offre la possibilità di accedere ai dati al di fuori della rete aziendale, utilizzando una modalità speciale chiamata *modalità portatile*.

Durante il criptaggio, Kaspersky Endpoint Security crea una chiave master. Kaspersky Endpoint Security salva la chiave master nei seguenti archivi:

- Kaspersky Security Center.
- Computer dell'utente.

  La chiave master è criptata con la chiave segreta dell'utente.
- Unità rimovibile.

  La chiave master è criptata con la chiave pubblica di Kaspersky Security Center.

Al termine del criptaggio, i dati nell'unità rimovibile sono accessibili all'interno della rete aziendale come se fosse un'unità rimovibile convenzionale senza criptaggio.

Accesso ai dati criptati

Quando viene collegata un'unità rimovibile con dati criptati, Kaspersky Endpoint Security esegue le seguenti azioni:

1. Verifica la presenza di una chiave master nella memoria locale nel computer dell'utente.

   Se viene rilevata la chiave master, l'utente ottiene l'accesso ai dati nell'unità rimovibile.

   Se non viene rilevata la chiave master, Kaspersky Endpoint Security esegue le seguenti azioni:

   a. Invia una richiesta a Kaspersky Security Center.

      Dopo aver ricevuto la richiesta, Kaspersky Security Center invia una risposta contenente la chiave master.

   b. Kaspersky Endpoint Security salva la chiave master nella memoria locale nel computer dell'utente per le operazioni successive con l'unità rimovibile criptata.
2. Decripta i dati.

Funzionalità speciali di criptaggio dell'unità rimovibile

Il criptaggio delle unità rimovibili ha le seguenti funzionalità speciali:

- Il criterio con le impostazioni preimpostate per il criptaggio delle unità rimovibili viene creato per uno specifico gruppo di computer gestiti. Di conseguenza, il risultato dell'applicazione del criterio di Kaspersky Security Center configurato per il criptaggio/decriptaggio delle unità rimovibili dipende dal computer a cui è connessa l'unità rimovibile.
- Kaspersky Endpoint Security non cripta/decripta i file con stato di sola lettura archiviati nelle unità rimovibili.

- I seguenti tipi di dispositivi sono supportati come unità rimovibili:
  - Supporti dati connessi tramite il bus USB
  - Dischi rigidi connessi tramite i bus USB e FireWire
  - Unità SSD connesse tramite i bus USB e FireWire

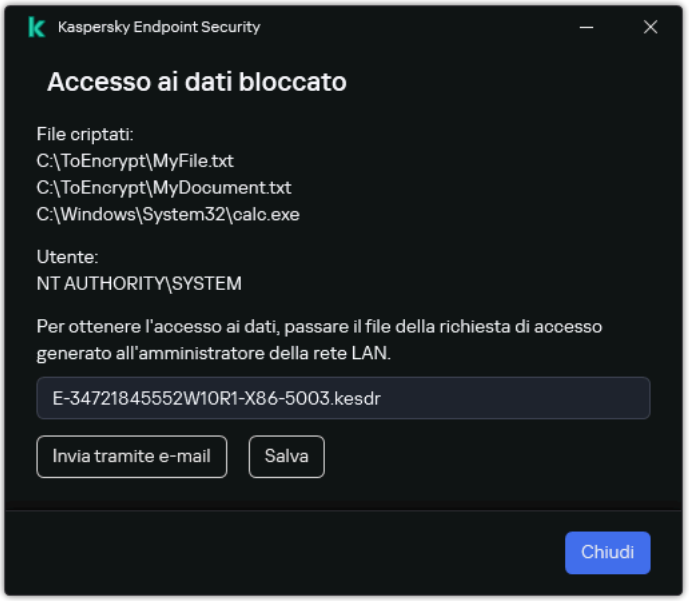
Criptaggio delle impostazioni dei componenti delle unità rimovibili

Parametro	Descrizione
Modalità di criptaggio	**Cripta intera unità rimovibile**. Se questa opzione è selezionata, quando viene applicato il criterio con le impostazioni di criptaggio specificate per le unità rimovibili, Kaspersky Endpoint Security cripta le unità rimovibili a livello di settore, inclusi i file system. **Cripta tutti i file**. Se questa opzione è selezionata, quando viene applicato il criterio con le impostazioni di criptaggio specificate per le unità rimovibili, Kaspersky Endpoint Security cripta tutti i file archiviati nelle unità rimovibili. Kaspersky Endpoint Security non riesegue il criptaggio dei file che sono già criptati. I contenuti del file system di un'unità rimovibile, inclusi i nomi e la struttura di cartelle dei file criptati, non vengono criptati e rimangono accessibili. **Cripta solo i nuovi file**. Se questa opzione è selezionata, quando viene applicato il criterio con le impostazioni di criptaggio specificate per le unità rimovibili, Kaspersky Endpoint Security cripta solo i file aggiunti o modificati nelle unità rimovibili dopo l'ultima applicazione del criterio di Kaspersky Security Center. Questa modalità di criptaggio è utile quando un'unità rimovibile viene utilizzata sia per scopi personali che lavorativi. Questa modalità di criptaggio consente di mantenere invariati tutti i file precedenti e cripta solo i file creati dall'utente in un computer in cui è installato Kaspersky Endpoint Security ed è abilitata la funzionalità di criptaggio. Di conseguenza, l'accesso ai file personali è sempre disponibile, indipendentemente dal fatto che Kaspersky Endpoint Security sia installato o meno nel computer con la funzionalità di criptaggio abilitata. **Decripta intera unità rimovibile**. Se questo elemento è selezionato, quando viene applicato il criterio con le impostazioni di criptaggio specificate per le unità rimovibili, Kaspersky Endpoint Security decripta tutti i file criptati nelle unità rimovibili e i file system delle unità rimovibili se sono stati criptati in precedenza. **Mantieni invariato**. Se questo elemento è selezionato, l'applicazione mantiene le unità nello stato precedente quando viene applicato il criterio. Se l'unità era criptata, rimane criptata. Se l'unità era decriptata, rimane decriptata. Questo elemento è selezionato per impostazione predefinita.
Modalità portatile	Questa casella di controllo consente di abilitare o disabilitare la preparazione di un'unità rimovibile che rende possibile l'accesso ai file archiviati su questa unità rimovibile nei computer all'esterno della rete aziendale. Se questa casella di controllo è selezionata, Kaspersky Endpoint Security richiede all'utente di specificare una password prima di criptare i file in un'unità rimovibile al momento dell'applicazione del criterio. La password è necessaria per accedere ai file criptati su un'unità rimovibile nei computer all'esterno della rete aziendale. È possibile configurare la complessità della password. La modalità portatile è disponibile per le modalità **Cripta tutti i file** o **Cripta solo i nuovi file**.
Cripta solo lo spazio su disco utilizzato	Questa casella di controllo consente di abilitare o disabilitare la modalità di criptaggio in cui vengono criptati solo i settori occupati del disco rigido. Questa modalità è consigliata per le nuove unità in cui non sono stati modificati o eliminati dati. Se la casella di controllo è selezionata, vengono criptate solo le parti dell'unità che sono occupate da file. Kaspersky Endpoint Security cripta automaticamente i nuovi dati man mano che vengono aggiunti. Se la casella di controllo è deselezionata, viene criptata l'intera unità, inclusi i frammenti residui dei file precedentemente eliminati e modificati. La possibilità di criptare esclusivamente lo spazio occupato è disponibile solo per la modalità **Cripta intera unità rimovibile**. Dopo aver avviato il criptaggio, l'abilitazione o la disabilitazione della funzione **Cripta solo lo spazio su disco utilizzato** non modificherà questa impostazione. È necessario selezionare o deselezionare la casella di controllo prima di avviare il criptaggio.

Parametro	Descrizione
Regole personalizzate	Questa tabella contiene i dispositivi per cui sono state definite le regole di criptaggio personalizzate. È possibile creare regole di criptaggio per singole unità rimovibili nei modi seguenti: • Aggiungere un'unità rimovibile dall'elenco dei dispositivi attendibili per Controllo dispositivi. • Aggiungere manualmente un'unità rimovibile: • Per ID dispositivo (Hardware ID o HWID) • Per modello di dispositivo: Vendor ID (VID) e Product ID (PID)
Consenti il criptaggio delle unità rimovibili in modalità offline	Se questa casella di controllo è selezionata, Kaspersky Endpoint Security cripta le unità rimovibili anche quando non è disponibile la connessione a Kaspersky Security Center. In questo caso, i dati richiesti per decriptare le unità rimovibili sono archiviati nel disco rigido del computer a cui è connessa l'unità rimovibile e non vengono trasmessi a Kaspersky Security Center. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non cripta le unità rimovibili senza una connessione a Kaspersky Security Center.
Impostazioni password di criptaggio/Portable File Manager	Impostazioni di sicurezza della password per Portable File Manager.

Modelli (criptaggio dei dati)

Dopo il criptaggio dei dati, Kaspersky Endpoint Security potrebbe limitare l'accesso ai dati, ad esempio a causa di una modifica nell'infrastruttura dell'organizzazione e di una modifica in Kaspersky Security Center Administration Server. Se un utente non ha accesso ai dati criptati, può richiedere all'amministratore l'accesso ai dati. In altre parole, l'utente deve inviare un file della richiesta di accesso all'amministratore. L'utente deve quindi caricare il file di risposta ricevuto dall'amministratore su Kaspersky Endpoint Security. Kaspersky Endpoint Security consente di richiedere l'accesso ai dati all'amministratore tramite e-mail (vedere la figura seguente).



Richiesta di accesso ai dati criptati

Viene fornito un modello per segnalare l'impossibilità di accedere ai dati criptati. Per comodità dell'utente, è possibile compilare i seguenti campi:

- **Destinatario**. Immettere l'indirizzo e-mail del gruppo di amministrazione con i diritti per le funzionalità di criptaggio dei dati.
- **Soggetto**. Immettere l'oggetto dell'e-mail con la richiesta di accesso ai file criptati. È ad esempio possibile aggiungere tag per filtrare i messaggi.
- **Messaggio dell'utente**. Se necessario, modificare il contenuto del messaggio. È possibile utilizzare le variabili per ottenere i dati necessari (ad esempio la variabile `%USER_NAME%`).

Esclusioni

Un'*area attendibile* è un elenco configurato dall'amministratore di sistema di oggetti e applicazioni che non vengono monitorati da Kaspersky Endpoint Security durante l'esecuzione.

L'amministratore crea l'area attendibile in modo indipendente, tenendo conto delle caratteristiche degli oggetti utilizzati e delle applicazioni installate nel computer. Può essere necessario includere oggetti e applicazioni nell'area attendibile quando Kaspersky Endpoint Security blocca l'accesso a un determinato oggetto o applicazione, se si è certi che l'oggetto o l'applicazione sia sicuro. Un amministratore può inoltre consentire a un utente di creare la propria area attendibile locale per un computer specifico. In questo modo gli utenti possono creare i propri elenchi locali di esclusioni e applicazioni attendibili oltre all'area attendibile generale in un criterio.

A partire da Kaspersky Endpoint Security 12.5 for Windows, è possibile aggiungere la telemetria EDR all'area attendibile. Questo consente di ottimizzare i dati inviati dall'applicazione al server di raccolta della telemetria per la soluzione Kaspersky Anti Targeted Attack Platform (EDR).

A partire da Kaspersky Endpoint Security 12.6 for Windows, le esclusioni dalle scansioni e le applicazioni attendibili vengono aggiunte all'area attendibile. Le esclusioni dalle scansioni predefinite e le applicazioni attendibili consentono di configurare rapidamente Kaspersky Endpoint Security nei server SQL, server Microsoft Exchange e System Center Configuration Manager. Ciò significa che non è necessario impostare manualmente un'area attendibile per l'applicazione nei server.

A partire da Kaspersky Endpoint Security 12.8 for Windows, è possibile installare l'applicazione in modalità Light Agent per proteggere gli ambienti virtuali. Le esclusioni dalla scansione e le applicazioni attendibili predefinite possono contribuire a configurare rapidamente Kaspersky Endpoint Security negli ambienti virtuali Citrix e VMware.

Esclusioni dalla scansione

Un'*esclusione dalla scansione* è un set di condizioni che devono essere soddisfatte perché Kaspersky Endpoint Security non esegua la scansione di un determinato oggetto alla ricerca di virus e altre minacce. Le esclusioni dalla scansione consentono di utilizzare senza rischi il software legittimo che utenti malintenzionati possono sfruttare per danneggiare il computer o i dati dell'utente. Tali applicazioni non hanno necessariamente uno scopo dannoso, ma possono essere sfruttate dagli hacker. Per informazioni dettagliate sulle applicazioni legittime che gli intrusi possono utilizzare per compromettere il computer o i dati dell'utente, visitare il sito Web dell'Enciclopedia Kaspersky.

Tali applicazioni possono essere bloccate da Kaspersky Endpoint Security. Per impedirne il blocco, è possibile configurare le esclusioni dalla scansione per le applicazioni in uso. A tale scopo, aggiungere all'area attendibile il nome o la maschera per il nome elencati nell'Enciclopedia IT di Kaspersky. Ad esempio, spesso si utilizza l'applicazione Radmin per l'amministrazione remota dei computer. Kaspersky Endpoint Security considera sospetta questa attività e potrebbe bloccarla. Per impedire il blocco dell'applicazione, creare un'esclusione dalla scansione con il nome o la maschera per il nome elencati nell'Enciclopedia IT di Kaspersky.

Se un'applicazione che si occupa della raccolta e dell'invio delle informazioni per l'elaborazione è installata nel computer, Kaspersky Endpoint Security può classificare questa applicazione come malware. Per evitare che questo accada, è possibile escludere l'applicazione dalla scansione configurando Kaspersky Endpoint Security come descritto in questo documento.

Le esclusioni dalla scansione possono essere utilizzate dai seguenti componenti e attività dell'applicazione configurati dall'amministratore di sistema:

- Rilevamento del Comportamento.
- Prevenzione Exploit.
- Prevenzione Intrusioni Host.
- Protezione minacce file.
- Protezione minacce Web.
- Protezione minacce di posta.
- Attività *Scansione malware*

Elenco di applicazioni attendibili

L'*elenco delle applicazioni attendibili* è un elenco di applicazioni per cui Kaspersky Endpoint Security non monitora le attività sui file e di rete (incluse le attività dannose) e l'accesso al Registro di sistema. Per impostazione predefinita, Kaspersky Endpoint Security monitora gli oggetti aperti, eseguiti o salvati da qualsiasi processo di applicazione e controlla l'attività di tutte le applicazioni e il traffico di rete che generano. Dopo aver aggiunto un'applicazione all'elenco delle applicazioni attendibili, Kaspersky Endpoint Security interrompe il monitoraggio delle attività dell'applicazione.

La differenza tra le esclusioni dalla scansione e le applicazioni attendibili è che per le esclusioni Kaspersky Endpoint Security non esamina i file, mentre per le applicazioni attendibili non controlla i processi avviati. Se un'applicazione attendibile crea un file dannoso in una cartella non inclusa nelle esclusioni dalla scansione, Kaspersky Endpoint Security rileverà il file ed eliminerà la minaccia. Se la cartella viene aggiunta alle esclusioni, Kaspersky Endpoint Security ignorerà questo file.

Se ad esempio si considerano sicuri gli oggetti utilizzati dall'applicazione Blocco note di Microsoft Windows, ovvero si ritiene attendibile questa applicazione, è possibile aggiungere Blocco note di Microsoft Windows all'elenco delle applicazioni attendibili affinché gli oggetti utilizzati da questa applicazione non vengano monitorati. In questo modo, si aumenteranno le prestazioni del computer, specialmente quando si utilizzano applicazioni server.

Inoltre, determinate azioni classificate da Kaspersky Endpoint Security come sospette possono essere sicure nel contesto della funzionalità di numerose applicazioni. Ad esempio, l'intercettazione del testo digitato sulla tastiera è un processo di routine per le applicazioni che commutano automaticamente i layout di tastiera, come Punto Switcher. Per tenere conto delle caratteristiche specifiche di tali applicazioni ed escluderne le attività dal monitoraggio, è consigliabile aggiungere le applicazioni di questo tipo all'elenco delle applicazioni attendibili.

Le applicazioni attendibili consentono di evitare problemi di compatibilità tra Kaspersky Endpoint Security e altre applicazioni (ad esempio, il problema della doppia scansione del traffico di rete di un computer di terzi da parte di Kaspersky Endpoint Security e di un'altra applicazione antivirus).

Il file eseguibile e il processo dell'applicazione attendibile sono comunque sottoposti a scansione alla ricerca di virus e altro malware. Utilizzando le esclusioni dalla scansione, è possibile escludere completamente un'applicazione dalla scansione da parte di Kaspersky Endpoint Security.

Impostazioni delle esclusioni

Parametro	Descrizione

Tipi di oggetti rilevati

Indipendentemente dalle impostazioni configurate dell'applicazione, Kaspersky Endpoint Security rileva e blocca sempre virus, worm e Trojan. Dal momento che possono danneggiare in modo significativo il computer.

- **Virus e worm**

  Sottocategoria: virus e worm (Viruses_and_Worms)

  Livello di pericolo: Alto

  I virus e worm classici eseguono azioni non autorizzate dall'utente. Possono creare copie di se stessi in grado di replicarsi.

  Virus classici

  Dopo essere penetrato nel computer, un virus classico infetta un file, si attiva, esegue azioni dannose e aggiunge copie di se stesso in altri file.

  Un virus classico si propaga solo nelle risorse locali del computer; non può penetrare in altri computer autonomamente. Può raggiungere un altro computer solo se aggiunge una copia di se stesso a un file memorizzato in una cartella condivisa o in un CD inserito oppure se l'utente inoltra un messaggio e-mail con un file allegato infetto.

  Il codice dei virus classici può penetrare in varie aree dei computer, dei sistemi operativi e delle applicazioni. A seconda dell'ambiente, i virus vengono suddivisi in *virus di file*, *virus di avvio*, *virus di script* e *virus macro*.

  I virus possono infettare i file utilizzando un'ampia varietà di tecniche. I *virus di Overwriting* scrivono il proprio codice sul codice del file infetto, cancellandone il contenuto. Il file infetto smette di funzionare e non può essere ripristinato. I *virus Parasitic* modificano i file, lasciandoli parzialmente o completamente funzionanti. I *virus Companion* non modificano i file, ma creano duplicati. Quando si apre un file infetto, ne viene avviato un duplicato, che di fatto è un virus. Si rilevano inoltre i seguenti tipi di virus: *virus Link*, *virus OBJ*, *virus LIB*, *virus del codice sorgente* e molti altri.

  Worm

  Come nel caso dei virus classici, il codice di un worm viene attivato ed esegue azioni dannose dopo essere penetrato in un computer. La caratteristica distintiva dei worm è la loro capacità di trasmettersi da un computer all'altro, senza che l'utente ne sia consapevole, inviando copie di se stessi attraverso vari canali.

  La principale caratteristica che consente di differenziare i vari tipi di worm è la loro modalità di propagazione. Nella seguente tabella viene fornita una panoramica dei diversi tipi di worm, classificati in base alla modalità di propagazione.

  Modalità di propagazione dei worm

Tipo	Nome	Descrizione
Email-Worm	Email-Worm	Si propagano tramite la posta elettronica. Un messaggio infetto contiene un file allegato con una copia di un worm oppure un collegamento a un file caricato su un sito Web, che può essere stato violato o creato appositamente a tale scopo. Quando l'utente apre il file allegato, il worm si attiva. Allo stesso modo, facendo clic sul collegamento, scaricando e aprendo il file, il worm inizia a eseguire le azioni dannose per cui è progettato. Il worm continua quindi a diffondere copie di se stesso, cercando altri indirizzi di posta elettronica e inviando messaggi infetti.
IM-Worm	Worm del client IM	Si diffondono attraverso client IM. In genere, tali worm inviano messaggi che contengono un collegamento a un file con una copia del worm in un sito Web, utilizzando l'elenco di contatti dell'utente. Quando l'utente scarica e apre il file, il worm si attiva.
IRC-Worm	Worm di chat Internet	Penetrano nei computer attraverso le Internet Relay Chats, sistemi utilizzati per comunicare con altre persone in tempo reale via Internet. Questo tipo di worm pubblica in una chat Internet un file contenente una copia di se stesso o un collegamento a tale file. Quando l'utente scarica e apre il file, il worm si attiva.
Net-Worm	Worm di rete	Questi worm si propagano tramite le reti di computer. A differenza di altri tipi di worm, questi worm vengono propagati senza la partecipazione dell'utente. I worm di questo tipo cercano nella rete locale i computer che utilizzano programmi con vulnerabilità. A tale scopo, inviano uno pacchetto di rete appositamente predisposto (exploit), che contiene il codice del worm o parte di esso. Se nella rete è presente un computer vulnerabile, questo riceve il pacchetto. Quando è penetrato completamente nel computer, il worm si attiva.
P2P-Worm	Worm di file sharing	Si propagano attraverso le reti peer-to-peer di file sharing. Per penetrare in una rete peer-to-peer, il worm si replica in una cartella di file sharing, in genere presente nel computer dell'utente. La rete peer-to-peer visualizza informazioni sul file, in modo che gli utenti della rete possano trovare, scaricare e aprire il file infetto come qualsiasi altro file. I worm più complessi imitano i protocolli di rete di una specifica rete peer-to-peer: offrono risposte positive alle ricerche e propongono copie di se stessi per il download.
Worm	Altri tipi di worm	Gli altri tipi di worm includono: • Worm che propagano copie di se stessi tramite le risorse di rete. Utilizzando le funzioni del sistema operativo, esplorano le cartelle di rete disponibili, si connettono a computer su Internet e cercano di ottenere un accesso completo alle unità disco. A differenza dei worm descritti in precedenza, alcuni non si attivano autonomamente, ma l'utente deve aprire un file contenente una copia del worm per attivarlo. • Worm che non utilizzano alcuno dei metodi descritti nella tabella precedente per diffondersi (ad esempio, quelli distribuiti tramite telefoni cellulari).

- **Trojan (compreso il ransomware)**

  Sottocategoria: Trojan

  Livello di pericolo: Alto

A differenza dei worm e dei virus, i programmi Trojan non replicano se stessi. Possono ad esempio penetrare in un computer tramite la posta elettronica o attraverso un browser, quando l'utente visita una pagina Web infetta. I programmi Trojan vengono avviati dall'utente. Iniziano a eseguire la loro azione dannosa non appena sono eseguiti.

Il comportamento dei diversi programmi Trojan nei computer infetti può variare. La funzione principale di un programma Trojan è bloccare, modificare e cancellare i dati, compromettendo il funzionamento dei computer o delle reti. I programmi Trojan possono inoltre ricevere e inviare file, eseguirli, visualizzare messaggi, accedere a pagine Web, scaricare e installare programmi e riavviare il computer.

Gli hacker spesso utilizzano "set" di vari programmi Trojan.

Nella seguente tabella sono descritti i diversi tipi di comportamento dei programmi Trojan.

Tipi di comportamento dei programmi Trojan in un computer infetto

Tipo	Nome	Descrizione
Trojan-ArcBomb	Programmi Trojan – "archivi bomba"	Una volta decompressi, questi archivi aumentano di dimensioni al punto tale da compromettere il funzionamento del computer. Quando l'utente tenta di decomprimere l'archivio, il computer può iniziare a rallentare o bloccarsi e il disco può riempirsi di dati "vuoti". Gli "archivi bomba" sono particolarmente pericolosi per i file server e i server di posta. Se un server utilizza un sistema automatico di elaborazione delle informazioni in arrivo, un "archivio bomba" può causarne l'arresto.
Backdoor	Programmi Trojan di amministrazione remota	Sono considerati il tipo di Trojan più pericoloso in assoluto. Dal punto di vista funzionale, sono simili alle applicazioni di amministrazione remota installate nei computer. Si installano senza che l'utente ne sia consapevole e consentono a un intruso di gestire il computer in remoto.
Programma Trojan	Trojan	Includono le seguenti applicazioni dannose: • **Programmi Trojan classici**. Questi programmi eseguono solo le funzioni principali dei programmi Trojan: blocco, modifica o cancellazione di dati allo scopo di compromettere il funzionamento dei computer o delle reti. Non dispongono delle caratteristiche avanzate di altri tipi di programmi Trojan descritti in questa tabella. • **Programmi Trojan versatili**. Dispongono delle caratteristiche avanzate tipiche di diversi tipi di programmi Trojan.
Trojan-Ransom	Trojan ransom	Questi programmi "prendono in ostaggio" le informazioni sul computer dell'utente, modificandole o bloccandole, oppure compromettono il funzionamento del computer in modo che l'utente non sia più in grado di utilizzare i dati. L'intruso richiede quindi all'utente un riscatto in cambio della promessa di inviare un'applicazione in grado di ripristinare l'utilizzabilità del computer e dei dati.
Trojan-Clicker	Trojan clicker	Accedono a pagine Web dal computer dell'utente, inviando direttamente comandi al browser o sostituendo gli indirizzi Web specificati nei file del sistema operativo. Utilizzando questi programmi, un intruso può sferrare attacchi di rete e aumentare il traffico verso determinati siti Web per aumentare la frequenza di visualizzazione dei banner pubblicitari.
Trojan-Downloader	Trojan downloader	Accedono a una pagina Web, da cui scaricano e installano altre applicazioni dannose nel computer dell'utente. Contengono il nome dell'applicazione dannosa da scaricare o la ricevono dalla pagina Web a cui si collegano.
Trojan-Dropper	Trojan dropper	Contengono altri programmi Trojan che copiano nel disco rigido e quindi installano nel computer. Gli intrusi possono utilizzare i Trojan dropper per: • Installare un'applicazione dannosa senza che l'utente ne sia consapevole: i Trojan dropper non visualizzano alcun messaggio oppure visualizzano messaggi falsi, ad esempio notificando un errore in un archivio o l'utilizzo di una versione incompatibile del sistema operativo. • Impedire il rilevamento di un'altra applicazione dannosa: non tutti i programmi anti-virus sono in grado di rilevare un'applicazione dannosa contenuta all'interno di un Trojan dropper.
Trojan-Notifier	Trojan notifier	Segnalano a un intruso che il computer infetto è accessibile, inviando informazioni sul computer, come l'indirizzo IP, il numero della porta aperta o l'indirizzo e-mail. Comunicano con l'intruso via e-mail, tramite FTP, accedendo alla sua pagina Web o attraverso altri metodi. I Trojan notifier vengono spesso utilizzati in set che comprendono diversi programmi Trojan. Comunicano all'intruso che altri programmi Trojan sono stati installati nel computer dell'utente.
Trojan-Proxy	Trojan proxy	Consentono all'intruso di accedere in modo anonimo alle pagine Web utilizzando il computer dell'utente e vengono spesso utilizzati per inviare posta spam.
Trojan-PSW	Password-stealing-ware	I password-stealing-ware sono un tipo di programma Trojan che ruba gli account utente, ad esempio le informazioni di registrazione del software. Recuperano le informazioni riservate nei file di sistema e nel registro e le inviano all'autore dell'attacco via e-mail, tramite FTP, accedendo al sito Web dell'intruso o attraverso altri metodi. Alcuni di questi programmi Trojan sono classificati in tipi distinti descritti in questa tabella. Esistono programmi Trojan che trafugano conti bancari (Trojan-Banker), i dati degli utenti di client IM (Trojan-IM) e i dati degli utenti di giochi online (Trojan-GameThief).
Trojan-Spy	Programmi Trojan per lo spionaggio dell'utente	Vengono utilizzati per spiare l'utente, raccogliendo informazioni sulle sue azioni durante l'utilizzo del computer. Possono intercettare i dati inseriti dall'utente tramite la tastiera, acquisire schermate e raccogliere elenchi di applicazioni attive. Una volta ricevute tali informazioni, le trasferiscono all'intruso via e-mail, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.
Trojan-DDoS	Programmi Trojan per l'esecuzione di attacchi di rete	Inviano numerose richieste dal computer dell'utente a un server remoto. Il server esaurisce le risorse per l'elaborazione delle richieste ricevute e smette di funzionare (attacchi Denial-of-Service, o semplicemente DoS). Gli hacker spesso infettano numerosi computer con questi programmi, in modo da poterli utilizzare per attaccare simultaneamente un singolo server. I programmi DoS sferrano un attacco da un singolo computer, rivelando la propria presenza all'utente. I programmi DDoS (Distributed DoS) sferrano attacchi da diversi computer senza che l'utente del computer infetto ne sia consapevole.
Trojan-IM	Programmi Trojan che trafugano i dati personali degli utenti di client IM	Trafugano numeri di conti e password degli utenti di client IM. Tali informazioni vengono quindi trasferite all'intruso via e-mail, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.
Rootkit	Rootkit	Nascondono altre applicazioni dannose e la loro attività, prolungando quindi la presenza di tali applicazioni nel sistema operativo. Possono inoltre nascondere file e processi nella memoria di un computer infetto o chiavi di registro utilizzate dalle applicazioni dannose. I rootkit possono nascondere lo scambio di dati tra le applicazioni installate nel computer dell'utente e altri computer in rete.
Trojan-SMS	Programmi Trojan sotto forma di messaggi SMS	Infettano i telefoni cellulari e inviano messaggi SMS a numeri a pagamento.

Trojan-GameThief	Programmi Trojan che trafugano i dati personali degli utenti di giochi online	Rubano le credenziali degli account degli utenti di giochi online. Tali informazioni vengono quindi trasferite all'intruso via e-mail, tramite FTP, accedendo al suo sito Web o attraverso altri metodi.
Trojan-Banker	Programmi Trojan che trafugano conti bancari	Sottraggono i dati di conti bancari o sistemi e-money. Tali informazioni vengono quindi trasferite all'hacker via e-mail, tramite FTP, accedendo a una pagina Web o attraverso altri metodi.
Trojan-Mailfinder	Programmi Trojan che raccolgono indirizzi e-mail	Raccolgono gli indirizzi e-mail sul computer e li trasferiscono all'intruso via e-mail, tramite FTP, accedendo al suo sito Web o attraverso altri metodi. L'intruso può utilizzare gli indirizzi raccolti per inviare spam.

- **Strumenti dannosi**

  Sottocategoria: Strumenti dannosi

  Livello di pericolo: Medio

  A differenza di altri tipi di malware, gli strumenti dannosi non eseguono specifiche azioni al momento dell'esecuzione. Possono essere memorizzati e avviati senza problemi sul computer dell'utente. Le funzionalità di questi programmi possono essere utilizzate per creare virus, worm e programmi Trojan, sferrare attacchi di rete contro server remoti, violare computer ed eseguire altre azioni dannose.

  Nella seguente tabella sono descritte le varie caratteristiche degli strumenti dannosi, raggruppate per tipo.

  Caratteristiche degli strumenti dannosi

Tipo	Nome	Descrizione
Constructor	Constructor	Consentono di creare nuovi virus, worm e programmi Trojan. Alcuni constructor presentano un'interfaccia standard di Windows che consente di selezionare il tipo di applicazione dannosa da creare, il modo per contrastare i debugger e altre caratteristiche.
DoS	Attacchi di rete	Inviano numerose richieste dal computer dell'utente a un server remoto. Il server esaurisce le risorse per l'elaborazione delle richieste ricevute e smette di funzionare (attacchi Denial-of-Service, o semplicemente DoS).
Exploit	Exploit	Un *exploit* è un set di dati o un codice di programma che utilizza le vulnerabilità dell'applicazione in cui viene elaborato per eseguire azioni dannose sul computer. Gli exploit possono ad esempio scrivere o leggere file o accedere a pagine Web infette. I diversi exploit utilizzano le vulnerabilità di diverse applicazioni o servizi di rete. Un exploit viene trasmesso tramite la rete a diversi computer, sotto forma di pacchetto di rete, alla ricerca di computer con servizi di rete vulnerabili. Gli exploit contenuti in un file DOC utilizzano le vulnerabilità degli editor di testo. Possono iniziare a eseguire le funzioni programmate dall'hacker quando l'utente apre un file infetto. Un exploit contenuto in un messaggio e-mail ricerca le vulnerabilità in tutti i client di posta elettronica. Può iniziare a eseguire azioni dannose non appena l'utente apre un messaggio infetto in questo client di posta elettronica. Gli exploit vengono utilizzati per propagare i worm di rete. Gli exploit Nuker sono pacchetti di rete che rendono i computer non operativi.
FileCryptor	Strumenti di criptaggio	Criptano altre applicazioni dannose per nasconderle alle applicazioni anti-virus.
Flooder	Programmi per il flooding delle reti	Inviano numerosi messaggi tramite i canali di rete. Questi strumenti comprendono ad esempio i programmi utilizzati per il flooding delle Internet Relay Chat. Questo tipo di software non include i programmi che eseguono il flooding del traffico di posta elettronica, dei client IM e dei sistemi SMS. Tali programmi vengono classificati in categorie distinte nella presente tabella (Email-Flooder, IM-Flooder e SMS-Flooder).
HackTool	Strumenti di hackeraggio	Vengono utilizzati per violare i computer in cui sono installati oppure per generare attacchi contro un altro computer (ad esempio, aggiungendo nuovi account di sistema senza l'autorizzazione dell'utente o cancellando i log di sistema al fine di nascondere le tracce della propria presenza nel sistema operativo). Questi strumenti includono sniffer che eseguono funzioni dannose, come ad esempio intercettare le password. Gli sniffer sono programmi che consentono di visualizzare il traffico di rete.
Hoax	Hoax	Questi programmi spaventano l'utente con messaggi simili a quelli generati dai virus: possono "rilevare" un virus in un file sicuro o visualizzare un messaggio relativo alla formattazione del disco, senza eseguirla effettivamente.
Spoofer	Strumenti di spoofing	Inviano messaggi e richieste di rete con l'indirizzo di un mittente fittizio. Gli spoofer vengono ad esempio utilizzati dagli intrusi per nascondere la propria identità e presentarsi come mittenti attendibili.
VirTool	Strumenti per la modifica di applicazioni dannose	Consentono di modificare altri programmi malware per nasconderli alle applicazioni anti-virus.
Email-Flooder	Programmi per il flooding degli indirizzi e-mail	Inviano numerosi messaggi a vari indirizzi di posta elettronica. La grande quantità di messaggi ricevuti impedisce agli utenti di visualizzare i messaggi legittimi.
IM-Flooder	Programmi che "contaminano" il traffico dei client IM	Inviano un numero elevato di messaggi agli utenti dei client IM. La grande quantità di messaggi impedisce agli utenti di visualizzare i messaggi legittimi.
SMS-Flooder	Programmi per il flooding del traffico con messaggi SMS	Inviano numerosi messaggi SMS ai telefoni cellulari.

- **Adware**

  Sottocategoria: Software pubblicitario (adware);

  Livello di pericolo: Medio

  Gli adware visualizzano informazioni pubblicitarie all'utente. Mostrano banner pubblicitari nell'interfaccia di altri programmi e ridirigono le query di ricerca verso siti pubblicitari. Alcuni programmi adware raccolgono informazioni di marketing sull'utente e le inviano ai loro sviluppatori, come ad esempio i nomi dei siti Web visitati o il contenuto delle ricerche effettuate. A differenza dei programmi di tipo Trojan-Spy, gli adware inviano queste informazioni allo sviluppatore con l'autorizzazione dell'utente.

- **Auto-dialer**

  Sottocategoria: software legittimo utilizzabile da malintenzionati per danneggiare il computer o i dati personali.

  Livello di pericolo: Medio

  Molte applicazioni di questo tipo sono utili, pertanto numerosi utenti le eseguono. Queste applicazioni includono client IRC, auto-dialer, programmi per il download di file, monitor delle attività di sistema dei computer, utilità per la gestione delle password e server Internet per FTP, HTTP e Telnet.

  Se tuttavia gli intrusi ottengono l'accesso a questi programmi o se li installano nel computer dell'utente, alcune delle funzionalità dei programmi possono essere utilizzate per violare la sicurezza.

  Queste applicazioni variano a seconda della funzione; i diversi tipi sono descritti nella seguente tabella.

Tipo	Nome	Descrizione
Client-IRC	Client di chat Internet	Gli utenti installano questi programmi per comunicare con altre persone nelle Internet Relay Chat. Gli intrusi li usano per diffondere malware.
Downloader	Programmi per il download di file	Questi programmi possono eseguire segretamente il download di file da pagine Web.
Monitor	Programmi di monitoraggio	Questi programmi consentono il monitoraggio dei computer in cui sono installati (visualizzazione delle applicazioni attive e di come scambiano dati con le applicazioni in altri computer).
PSWTool	Strumenti di recupero delle password	Consentono di visualizzare e ripristinare le password dimenticate. Gli intrusi li installano segretamente nei computer degli utenti esattamente con lo stesso obiettivo.
RemoteAdmin	Programmi di amministrazione remota	Questi programmi vengono spesso utilizzati dagli amministratori di sistema. Questi programmi consentono di accedere all'interfaccia di un computer remoto per monitorarlo e gestirlo. Gli intrusi li installano segretamente nei computer degli utenti esattamente con lo stesso obiettivo: monitorare e gestire computer remoti. I programmi legittimi di amministrazione remota sono diversi dai programmi Trojan di amministrazione remota di tipo Backdoor. I programmi Trojan sono in grado di infiltrarsi autonomamente nel sistema operativo e di installarsi, mentre i programmi legittimi non presentano questa caratteristica.
Server-FTP	Server FTP	Questi programmi operano come server FTP. Gli intrusi li installano nei computer degli utenti per ottenere l'accesso remoto tramite il protocollo FTP.
Server-Proxy	Server proxy	Questi programmi operano come server proxy. Gli intrusi li installano nei computer degli utenti per inviare spam a nome dell'utente.
Server-Telnet	Server Telnet	Questi programmi operano come server Telnet. Gli intrusi li installano nei computer degli utenti per ottenere l'accesso remoto tramite il protocollo Telnet.
Server-Web	Server Web	Questi programmi operano come server Web. Gli intrusi li installano nei computer degli utenti per ottenere l'accesso remoto tramite il protocollo HTTP.
RiskTool	Strumenti per l'utilizzo del computer locale	Questi strumenti offrono agli utenti opzioni aggiuntive per l'utilizzo del computer. Consentono di nascondere i file o le finestre delle applicazioni attive e di chiudere i processi attivi.
NetTool	Strumenti di rete	Questi strumenti offrono all'utente opzioni aggiuntive per l'utilizzo di altri computer della rete. Consentono di riavviare altri computer, rilevare le porte aperte e avviare le applicazioni installate in tali computer.
Client-P2P	Programmi client Peer-to-Peer	Consentono di utilizzare le reti peer-to-peer. Gli intrusi possono utilizzarli per diffondere malware.
Client-SMTP	Client SMTP	Inviano messaggi e-mail a insaputa dell'utente. Gli intrusi li installano nei computer degli utenti per inviare spam a nome dell'utente.
WebToolbar	Barre degli strumenti Web	Aggiungono barre degli strumenti per l'utilizzo di motori di ricerca alle interfacce di altre applicazioni.
FraudTool	Programmi fraudolenti	Questi programmi si camuffano da altri programmi reali. Vi sono ad esempio programmi anti-virus fraudolenti che visualizzano messaggi sul rilevamento di malware. senza tuttavia rilevare o disinfettare alcun oggetto.

- **Software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali**

  Sottocategoria: software legittimo utilizzabile da malintenzionati per danneggiare il computer o i dati personali.

  Livello di pericolo: Medio

  Molte applicazioni di questo tipo sono utili, pertanto numerosi utenti le eseguono. Queste applicazioni includono client IRC, auto-dialer, programmi per il download di file, monitor delle attività di sistema dei computer, utilità per la gestione delle password e server Internet per FTP, HTTP e Telnet.

  Se tuttavia gli intrusi ottengono l'accesso a questi programmi o se li installano nel computer dell'utente, alcune delle funzionalità dei programmi possono essere utilizzate per violare la sicurezza.

  Queste applicazioni variano a seconda della funzione; i diversi tipi sono descritti nella seguente tabella.

Tipo	Nome	Descrizione
Client-IRC	Client di chat Internet	Gli utenti installano questi programmi per comunicare con altre persone nelle Internet Relay Chat. Gli intrusi li usano per diffondere malware.
Downloader	Programmi per il download di file	Questi programmi possono eseguire segretamente il download di file da pagine Web.
Monitor	Programmi di monitoraggio	Questi programmi consentono il monitoraggio dei computer in cui sono installati (visualizzazione delle applicazioni attive e di come scambiano dati con le applicazioni in altri computer).

PSWTool	Strumenti di recupero delle password	Consentono di visualizzare e ripristinare le password dimenticate. Gli intrusi li installano segretamente nei computer degli utenti esattamente con lo stesso obiettivo.
RemoteAdmin	Programmi di amministrazione remota	Questi programmi vengono spesso utilizzati dagli amministratori di sistema. Questi programmi consentono di accedere all'interfaccia di un computer remoto per monitorarlo e gestirlo. Gli intrusi li installano segretamente nei computer degli utenti esattamente con lo stesso obiettivo: monitorare e gestire computer remoti. I programmi legittimi di amministrazione remota sono diversi dai programmi Trojan di amministrazione remota di tipo Backdoor. I programmi Trojan sono in grado di infiltrarsi autonomamente nel sistema operativo e di installarsi, mentre i programmi legittimi non presentano questa caratteristica.
Server-FTP	Server FTP	Questi programmi operano come server FTP. Gli intrusi li installano nei computer degli utenti per ottenere l'accesso remoto tramite il protocollo FTP.
Server-Proxy	Server proxy	Questi programmi operano come server proxy. Gli intrusi li installano nei computer degli utenti per inviare spam a nome dell'utente.
Server-Telnet	Server Telnet	Questi programmi operano come server Telnet. Gli intrusi li installano nei computer degli utenti per ottenere l'accesso remoto tramite il protocollo Telnet.
Server-Web	Server Web	Questi programmi operano come server Web. Gli intrusi li installano nei computer degli utenti per ottenere l'accesso remoto tramite il protocollo HTTP.
RiskTool	Strumenti per l'utilizzo del computer locale	Questi strumenti offrono agli utenti opzioni aggiuntive per l'utilizzo del computer. Consentono di nascondere i file o le finestre delle applicazioni attive e di chiudere i processi attivi.
NetTool	Strumenti di rete	Questi strumenti offrono all'utente opzioni aggiuntive per l'utilizzo di altri computer della rete. Consentono di riavviare altri computer, rilevare le porte aperte e avviare le applicazioni installate in tali computer.
Client-P2P	Programmi client Peer-to-Peer	Consentono di utilizzare le reti peer-to-peer. Gli intrusi possono utilizzarli per diffondere malware.
Client-SMTP	Client SMTP	Inviano messaggi e-mail a insaputa dell'utente. Gli intrusi li installano nei computer degli utenti per inviare spam a nome dell'utente.
WebToolbar	Barre degli strumenti Web	Aggiungono barre degli strumenti per l'utilizzo di motori di ricerca alle interfacce di altre applicazioni.
FraudTool	Programmi fraudolenti	Questi programmi si camuffano da altri programmi reali. Vi sono ad esempio programmi anti-virus fraudolenti che visualizzano messaggi sul rilevamento di malware. senza tuttavia rilevare o disinfettare alcun oggetto.

- **Oggetti compressi che potrebbero nascondere codice dannoso**

  Sottocategoria: file compressi che possono causare danni.

  Livello di pericolo: Medio.

  Il file viene compresso tramite uno speciale programma di compressione utilizzato per la compressione del malware: virus, worm, Trojan. Kaspersky Endpoint Security esamina il modulo del programma di decompressione contenuti negli archivi autoestraenti.

  Per nascondere il malware dal rilevamento da parte di un anti-virus, gli hacker lo comprimono utilizzando programmi di compressione speciali. Gli esperti di Kaspersky hanno identificato i programmi di compressione più diffusi tra gli hacker.

- **Oggetti con compressione multipla**

  Sottocategoria: file compressi che possono causare danni.

  Livello di pericolo: Medio.

  Il file viene compresso tramite uno speciale programma di compressione utilizzato per la compressione del malware: virus, worm, Trojan. Kaspersky Endpoint Security esamina il modulo del programma di decompressione contenuti negli archivi autoestraenti.

  Per nascondere il malware dal rilevamento da parte di un anti-virus, gli hacker lo comprimono utilizzando programmi di compressione speciali. Gli esperti di Kaspersky hanno identificato i programmi di compressione più diffusi tra gli hacker.

Esclusioni

Questa tabella contiene informazioni sulle esclusioni dalla scansione.

È consigliabile specificare percorsi relativi anziché percorsi assoluti. Questo consente di escludere non solo gli oggetti del file system, ma anche gli oggetti fileless. Ad esempio, `*\Program Files (x86)\Folder\Subfolder`.

È possibile escludere gli oggetti dalle scansioni utilizzando i seguenti metodi:

- Specificare il percorso del file o della cartella.
- Immettere l'hash dell'oggetto.

- Utilizzare le maschere:
  - Il carattere `*` (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\*\*.txt` includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle.
  - Due caratteri `*` consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\**\*.txt` includerà tutti i percorsi dei file con estensione TXT situati nelle cartelle nidificate all'interno della `Folder`, ad eccezione della `Folder` stessa. La maschera deve includere almeno un livello di nidificazione. La maschera `C:\**\*.txt` non è una maschera valida.
  - Il carattere `?` (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri `\` e `/` (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera `C:\Folder\???.txt` includerà i percorsi di tutti i file che si trovano nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

    È possibile usare le maschere ovunque in un percorso di file o cartella. Ad esempio, se si desidera che l'ambito della scansione includa la cartella Downloads per tutti gli account utente sul computer, immettere la maschera `C:\Users\*\Downloads\`.

    Kaspersky Endpoint Security supporta le variabili di ambiente

    > Kaspersky Endpoint Security non supporta la variabile di ambiente `%userprofile%` quando si genera un elenco di esclusioni utilizzando la console Kaspersky Security Center. Per applicare la voce a tutti gli account utente, è possibile utilizzare il carattere * (ad esempio, `C:\Users\*\Documents\File.exe`). Ogni volta che si aggiunge una nuova variabile di ambiente, è necessario riavviare l'applicazione.

- Immettere il nome del tipo di oggetto in base alla classificazione dell'Enciclopedia Kaspersky (ad esempio `Email-Worm`, `Rootkit` o `RemoteAdmin`). È possibile utilizzare maschere con il carattere `?` (sostituisce un singolo carattere) e il carattere `*` (sostituisce un numero qualsiasi di caratteri). Se ad esempio viene specificata la maschera `Client*`, l'applicazione esclude gli oggetti `Client-IRC`, `Client-P2P` e `Client-SMTP` dalle scansioni.

> Kaspersky Endpoint Security nasconde l'elenco delle esclusioni dalle scansioni nell'interfaccia utente dell'applicazione se la configurazione delle esclusioni dalle scansioni è bloccata dall'amministratore nella console (simbolo del "lucchetto chiuso") e le esclusioni delle scansioni locali sono vietate (la casella di controllo **Consenti l'utilizzo delle esclusioni locali** è deselezionata).

Applicazioni attendibili

In questa tabella sono elencate le applicazioni attendibili, le cui attività non vengono monitorate da Kaspersky Endpoint Security durante l'esecuzione.

Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.

> Kaspersky Endpoint Security non supporta la variabile di ambiente `%userprofile%` quando si genera un elenco di applicazioni attendibili nella console Kaspersky Security Center. Per applicare la voce a tutti gli account utente, è possibile utilizzare il carattere * (ad esempio, `C:\Users\*\Documents\File.exe`). Ogni volta che si aggiunge una nuova variabile di ambiente, è necessario riavviare l'applicazione.

Il componente Controllo applicazioni gestisce l'avvio di ogni applicazione indipendentemente dal fatto che questa sia inclusa o meno nella tabella delle applicazioni attendibili.

> Kaspersky Endpoint Security nasconde l'elenco consolidato delle applicazioni attendibili nell'interfaccia utente dell'applicazione se la configurazione delle applicazioni attendibili è bloccata dall'amministratore nella console (simbolo del "lucchetto chiuso") e le applicazioni attendibili locali sono vietate (la casella di controllo **Consenti l'utilizzo delle applicazioni attendibili locali** è deselezionata).

Unisci i valori quando vengono ereditati *(disponibile solo in Kaspersky Security Center Console)*	In questo modo vengono uniti l'elenco delle esclusioni dalla scansione e delle applicazioni attendibili nei criteri padre e figlio di Kaspersky Security Center. Per unire gli elenchi, il criterio figlio deve essere configurato per ereditare le impostazioni del criterio padre di Kaspersky Security Center. Se la casella di controllo è selezionata, gli elementi dell'elenco del criterio padre di Kaspersky Security Center vengono visualizzati nei criteri figlio. In questo modo è possibile creare ad esempio un elenco consolidato di applicazioni attendibili per l'intera organizzazione. Gli elementi dell'elenco ereditati in un criterio figlio non possono essere eliminati o modificati. Gli elementi nell'elenco delle esclusioni dalla scansione e nell'elenco delle applicazioni attendibili uniti durante l'ereditarietà possono essere eliminati e modificati solo nel criterio padre. È possibile aggiungere, modificare o eliminare elementi dell'elenco nei criteri di livello inferiore. Se gli elementi negli elenchi del criterio padre e figlio corrispondono, questi elementi vengono visualizzati come lo stesso elemento del criterio padre. Se la casella di controllo non è selezionata, gli elementi degli elenchi non vengono uniti quando ereditano le impostazioni dei criteri di Kaspersky Security Center. Questa funzionalità consente inoltre di unire gli elenchi nei profili dei criteri. Per unire gli elenchi, nel profilo con priorità più alta abilitare l'ereditarietà delle impostazioni da un profilo con priorità più bassa. Per ulteriori dettagli sulle priorità dei profili dei criteri, consultare la Guida di Kaspersky Security Center.
Consenti l'utilizzo delle esclusioni locali/Consenti l'utilizzo delle applicazioni attendibili locali *(disponibile solo in Kaspersky Security Center Console)*	*Esclusioni locali e applicazioni attendibili locali (area attendibile locale)*: elenco di oggetti e applicazioni definito dall'utente in Kaspersky Endpoint Security per un computer specifico. Kaspersky Endpoint Security non monitora oggetti e applicazioni dell'area attendibile locale. In questo modo gli utenti possono creare i propri elenchi locali di esclusioni e applicazioni attendibili oltre all'area attendibile generale in un criterio. Se la casella di controllo è selezionata, un utente può creare un elenco locale di esclusioni dalla scansione e un elenco locale di applicazioni attendibili. Un amministratore può utilizzare Kaspersky Security Center per visualizzare, aggiungere, modificare o eliminare gli elementi dell'elenco nelle proprietà del computer. Se la casella di controllo è deselezionata, un utente può accedere solo agli elenchi generali delle esclusioni dalla scansione e delle applicazioni attendibili generati nel criterio.
Telemetria EDR (KATA)/NDR (KATA) *(disponibile solo in Kaspersky Security Center Console)*	Questa tabella contiene informazioni sulle esclusioni di telemetria EDR.
Telemetria KUMA *(disponibile solo in Kaspersky Security Center Console)*	Elenco di eventi da inviare a Kaspersky Unified Monitoring and Analysis Platform (KUMA). Kaspersky Endpoint Security opera nei seguenti modi: • **Invia tutti gli eventi**. In questa modalità, l'applicazione invia tutti gli eventi dal registro di Windows ad eccezione degli eventi aggiunti alle regole di esclusione. • **Invia solo gli eventi selezionati**. In questa modalità, l'applicazione invia solo gli eventi aggiunti nelle regole di inclusione.
Archivio di certificati di sistema attendibili	Se è selezionato uno degli archivi di certificati di sistema attendibili, Kaspersky Endpoint Security esclude le applicazioni firmate con una firma digitale attendibile dalle scansioni. Kaspersky Endpoint Security assegna automaticamente tali applicazioni al gruppo **Attendibili**. Se è selezionato **Non usare**, Kaspersky Endpoint Security esamina le applicazioni indipendentemente dal fatto che dispongano o meno di una firma digitale. Kaspersky Endpoint Security inserisce un'applicazione in un gruppo di attendibilità in base al livello di pericolosità che l'applicazione può rappresentare per il computer.

Impostazioni applicazione

È possibile configurare le seguenti impostazioni generali dell'applicazione:

- Modalità operativa
- Auto-difesa
- Prestazioni
- Informazioni di debug
- Stato del computer quando vengono applicate le impostazioni

Parametro	Descrizione
Avvia l'applicazione all'avvio del computer (consigliato)	Quando questa opzione è selezionata, Kaspersky Endpoint Security viene avviato dopo il caricamento del sistema operativo, proteggendo il computer durante l'intera sessione. Quando questa opzione è deselezionata, Kaspersky Endpoint Security non viene avviato dopo l'avvio del sistema operativo, finché non viene avviato dall'utente. La protezione del computer è disabilitata e i dati dell'utente potrebbero essere esposti a minacce.
Utilizza la tecnologia Disinfezione avanzata (richiede una quantità considerevole di risorse del computer)	In genere, Kaspersky Endpoint Security interrompe il malware rilevato prima che il computer venga infettato. La tecnologia Disinfezione avanzata protegge il computer dal malware già attivo (infezione attiva), riducendo al minimo il rischio di perdita di dati e la diffusione delle minacce. Se questa tecnologia è abilitata, quando viene rilevata un'attività dannosa, Kaspersky Endpoint Security mostra una notifica pop-up. Nella notifica, Kaspersky Endpoint Security propone all'utente la possibilità di eseguire la disinfezione avanzata del computer. Dopo l'approvazione di questa procedura da parte dell'utente, Kaspersky Endpoint Security neutralizza la minaccia, quindi riavvia il computer. La tecnologia avanzata di disinfezione utilizza considerevoli risorse di elaborazione, pertanto potrebbe rallentare le altre applicazioni. Quando l'applicazione è in fase di rilevamento di un'infezione attiva, è possibile che alcune funzionalità del sistema operativo non siano disponibili. La disponibilità del sistema operativo viene ripristinata al termine dell'esecuzione di Disinfezione avanzata e al riavvio del computer. Se Kaspersky Endpoint Security è installato in un computer in cui viene eseguito Windows for Servers, Kaspersky Endpoint Security non mostra la notifica. Pertanto, l'utente non può selezionare un'azione per disinfettare una minaccia attiva. Per disinfettare una minaccia, è necessario abilitare la tecnologia Disinfezione avanzata nelle impostazioni dell'applicazione e abilitare immediatamente Disinfezione avanzata nelle impostazioni dell'attività *Scansione malware*. Quindi, è necessario avviare l'attività *Scansione malware*.
Usa Kaspersky Security Center come server proxy per l'attivazione *(disponibile solo in Kaspersky Security Center Console)*	Se questa casella di controllo è selezionata, l'applicazione utilizza Kaspersky Security Center Administration Server come server proxy per la connessione ai server di attivazione. Questo è necessario quando si utilizza un codice di attivazione per attivare l'applicazione in un segmento di rete isolato senza accesso a Internet. Se si attiva l'applicazione con un file chiave, l'accesso a Internet non è necessario.
Abilita Auto-difesa	Se questa funzionalità è abilitata, Kaspersky Endpoint Security impedisce la modifica o l'eliminazione dei file dell'applicazione sul disco rigido, dei processi in memoria e delle voci del Registro di sistema.
Blocca gestione esterna dei servizi applicativi	Se questa funzionalità è abilitata, Kaspersky Endpoint Security non consente la gestione dei servizi applicativi utilizzando applicazioni di terze parti (ad esempio CMD). Quando viene effettuato un tentativo di gestione dei servizi dell'applicazione utilizzando applicazioni di terze parti, viene visualizzata una notifica nella barra delle applicazioni di Microsoft Windows (se il servizio di notifica non è stato disabilitato dall'utente). È possibile consentire la gestione esterna dei servizi applicativi solo nei computer che non supportano la tecnologia AM-PPL o nei computer in cui la tecnologia è disabilitata.
Rimanda attività pianificate durante l'alimentazione a batteria	Se questa casella di controllo è selezionata, la modalità di risparmio energetico è abilitata quando il computer è alimentato a batteria. Le attività pianificate vengono rimandate. È possibile avviare manualmente le attività di scansione e aggiornamento, se necessario. Quando è abilitata la modalità di risparmio energetico e il computer è alimentato a batteria, le attività seguenti non vengono eseguite anche se sono pianificate: • *Scansione completa*. • *Scansione delle aree critiche*. • *Scansione personalizzata*. • *Controllo integrità applicazione*. • *Scansione IOC*. • *Aggiornamento di database e moduli dell'applicazione* (solo patch) L'applicazione ignora gli aggiornamenti pianificati del database solo quando il laptop è alimentato a batteria e il livello della batteria è inferiore al 30% (valore predefinito). È possibile modificare il livello minimo di carica della batteria al di sotto del quale l'applicazione inizia a ignorare gli aggiornamenti pianificati dei database anti-virus modificando il Registro di sistema. In tutti gli altri casi, Kaspersky Endpoint Security aggiorna i database in base alla pianificazione, indipendentemente dal fatto che il laptop sia collegato o alimentato a batteria oppure che l'applicazione sia in modalità di risparmio energetico.

Parametro	Descrizione
Cedi risorse ad altre applicazioni	Il consumo di risorse del computer da parte di Kaspersky Endpoint Security durante la scansione del computer può aumentare il carico sui sottosistemi della CPU e del disco rigido. Ciò potrebbe rallentare altre applicazioni. Per ottimizzare le prestazioni, Kaspersky Endpoint Security fornisce una *modalità per trasferire le risorse ad altre applicazioni*. In questa modalità, il sistema operativo può ridurre la priorità dei thread delle attività di scansione di Kaspersky Endpoint Security quando il carico della CPU è elevato. In questo modo, è possibile ridistribuire le risorse del sistema operativo ad altre applicazioni. Pertanto, le attività di scansione riceveranno meno tempo di CPU. Di conseguenza, Kaspersky Endpoint Security impiegherà più tempo per eseguire la scansione del computer. Per impostazione predefinita, l'applicazione è configurata in modo da cedere risorse ad altre applicazioni.
Limita l'utilizzo della CPU per le attività di scansione	Per ottimizzare le prestazioni di Kaspersky Endpoint Security, è possibile limitare l'utilizzo della CPU tramite l'attività *Scansione malware*. Se la casella di controllo è selezionata, il carico medio su tutti i core della CPU dall'attività *Scansione malware* si avvicina al valore specificato. Per impostazione predefinita, la casella di controllo è deselezionata.
Abilita scrittura di dump	Se la casella di controllo è selezionata, Kaspersky Endpoint Security esegue la scrittura dei dump quando si verificano arresti anomali. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non esegue la scrittura dei dump. L'applicazione inoltre elimina i file di dump esistenti dal disco rigido del computer.
Abilita protezione dei file di dump e di traccia	Se la casella di controllo è selezionata, l'accesso ai file di dump viene concesso all'amministratore di sistema e all'amministratore locale, nonché all'utente che ha abilitato la scrittura di dump. Solo gli amministratori di sistema e locali possono accedere ai file di traccia. Se la casella di controllo è deselezionata, qualsiasi utente può accedere ai file di dump e di traccia.
Stato del computer quando vengono applicate le impostazioni *(disponibile solo in Kaspersky Security Center Console)*	Impostazioni per la visualizzazione degli stati dei computer client in cui è installato Kaspersky Endpoint Security in Web Console quando si verificano errori durante l'applicazione di un criterio o l'esecuzione di un'attività. Sono disponibili i seguenti stati: *OK*, *Avviso* e *Critico*.
Installa gli aggiornamenti senza riavviare il computer	L'upgrade dell'applicazione senza il riavvio del computer consente di assicurare il funzionamento costante dei server. È possibile eseguire l'upgrade dell'applicazione senza riavvio a partire dalla versione 11.10.0. Per eseguire l'upgrade a una versione precedente dell'applicazione, è necessario riavviare il computer. A partire dalla versione 11.11.0, è possibile eseguire le seguenti operazioni senza riavviare il computer: • installare le patch • modificare l'insieme dei componenti dell'applicazione • installare Kaspersky Endpoint Security su Kaspersky Security for Windows Server Il valore predefinito del parametro varia a seconda del tipo di sistema operativo. Se l'applicazione è installata in una workstation, l'upgrade dell'applicazione senza un'opzione di riavvio è disabilitato. Se l'applicazione è installata in un server, l'upgrade dell'applicazione senza un'opzione di riavvio è abilitato.
Compatibilità con software di amministrazione remota *(disponibile solo in Kaspersky Security Center Console)*	Se l'utilizzo di Kaspersky Endpoint Security insieme a RAT (Remote Administration Tool) causa problemi, è possibile abilitare la modalità di compatibilità. I problemi potrebbero essere correlati all'incompatibilità dei RAT con la funzionalità Secure Desktop dell'applicazione. Lo scopo di questa funzionalità è confermare azioni che possono potenzialmente abbassare il livello di sicurezza del computer. Questa funzionalità consente a un'applicazione di visualizzare una finestra di dialogo di conferma isolata da altri processi. Questa funzionalità utilizza diritti elevati per proteggere la richiesta. In questo modo, solo l'utente può confermare l'azione e non il malware. Se questa opzione è selezionata, la modalità di compatibilità RAT è abilitata. L'applicazione mostra una finestra di dialogo di conferma senza questa funzionalità. Può ridurre il livello di sicurezza del computer. Si sconsiglia di abilitare la modalità di compatibilità se Kaspersky Endpoint Security non causa problemi con RAT. Se questa opzione è deselezionata, la modalità di compatibilità RAT è disabilitata. Per impostazione predefinita, la casella di controllo è deselezionata. Esempio: quando si utilizza il browser in modalità RemoteApp, Kaspersky Endpoint Security potrebbe non mostrare una finestra di conferma quando si visita un sito Web con un certificato non attendibile poiché RemoteApp non supporta la funzionalità Secure Desktop dell'applicazione. Ciò può causare la mancata risposta del browser. Affinché il browser funzioni correttamente in modalità RemoteApp, è necessario abilitare la modalità compatibilità. È inoltre possibile provare ad abilitare la modalità compatibilità se si riscontrano problemi con la funzionalità Secure Desktop quando si utilizza altro software di terzi.

Rapporti e archivi

Rapporti

Nei rapporti vengono registrate informazioni sull'esecuzione di ciascun componente di Kaspersky Endpoint Security, sugli eventi di criptaggio dei dati, sulle prestazioni di ogni attività di scansione, attività di aggiornamento e attività di Controllo integrità, nonché sull'esecuzione complessiva dell'applicazione.

I rapporti vengono archiviati nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.

Backup

Backup archivia le copie di backup dei file eliminati o modificati durante la disinfezione. Una *copia di backup* è una copia del file creata prima della disinfezione o dell'eliminazione del file. Le copie di backup dei file vengono archiviate in un formato speciale e non rappresentano una minaccia.

Le copie di backup dei file vengono archiviate nella cartella `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Agli utenti del gruppo Amministratori è concessa l'autorizzazione completa per l'accesso a questa cartella. All'utente il cui account è stato utilizzato per installare Kaspersky Endpoint Security vengono concessi diritti di accesso limitati alla cartella.

Kaspersky Endpoint Security non consente la possibilità di configurare le autorizzazioni per l'accesso dell'utente alle copie di backup dei file.

Quarantena

Quarantena è una memoria locale speciale sul computer. L'utente può mettere in quarantena i file che considera pericolosi per il computer. I file in quarantena vengono archiviati in uno stato criptato e non minacciano la sicurezza del dispositivo. Kaspersky Endpoint Security utilizza la Quarantena solo quando è integrato con le soluzioni Kaspersky Detection and Response. In altri casi, Kaspersky Endpoint Security inserisce il file pertinente in Backup. Per ulteriori dettagli sulla gestione di Quarantena come parte delle soluzioni, consultare la Guida di Kaspersky Sandbox Help, la Guida di Kaspersky Endpoint Detection and Response Optimum, la Guida di Kaspersky Endpoint Detection and Response Expert, la Guida di Kaspersky Anti Targeted Attack Platform e la Guida di Kaspersky Endpoint Detection and Response Expert (on-premises).

La Quarantena può essere configurata solo tramite Web Console. È inoltre possibile utilizzare Web Console per gestire gli oggetti in quarantena (ripristino, eliminazione, aggiunta ecc.) È possibile ripristinare gli oggetti in locale sul computer utilizzando la riga di comando.

Kaspersky Endpoint Security utilizza l'account di sistema (SYSTEM) per mettere in quarantena i file.

Parametro	Descrizione
Elimina i rapporti dopo (giorni)	Se la casella di controllo è selezionata, il periodo di archiviazione massimo dei rapporti si limita all'intervallo di tempo definito. Per impostazione predefinita, il periodo massimo di archiviazione dei rapporti è di 30 giorni. Al termine di tale periodo di tempo, Kaspersky Endpoint Security elimina automaticamente le voci meno recenti dal file del rapporto.
Limita la dimensione del rapporto a (MB)	Se la casella di controllo è selezionata, le dimensioni massime del file del rapporto si limitano al valore definito. Per impostazione predefinita, la dimensione massima dei file è di 1024 MB. Per evitare il superamento della dimensione massima dei file del rapporto, Kaspersky Endpoint Security elimina automaticamente le voci meno recenti dal file del rapporto quando viene raggiunta la dimensione massima dei file.
Elimina oggetti dopo (giorni)	Se la casella di controllo è selezionata, il periodo di archiviazione massimo del file si limita all'intervallo di tempo definito. Per impostazione predefinita, il periodo massimo di archiviazione dei file è di 30 giorni. Al termine del periodo massimo di archiviazione, Kaspersky Endpoint Security elimina i file meno recenti da Backup.
Limita la dimensione del backup a (MB)	Se la casella di controllo è selezionata, le dimensioni di archiviazione massime si limitano al valore definito. Per impostazione predefinita, la dimensione massima è di 1024 MB. Per evitare il superamento delle dimensioni di archiviazione massime, Kaspersky Endpoint Security elimina automaticamente i file più vecchi dall'archivio al raggiungimento delle dimensioni massime di archiviazione.
Limita le dimensioni della Quarantena	Se la casella di controllo è selezionata, le dimensioni massime della quarantena si limitano al valore definito. Per impostazione predefinita, la dimensione massima è di 1024 MB. Quando la Quarantena raggiunge la dimensione massima, Kaspersky Endpoint Security invia l'evento *Spazio insufficiente nell'archivio Quarantena* a Kaspersky Security Center e pubblica l'evento nel registro eventi di Windows. Nel frattempo, l'applicazione interrompe l'inserimento in quarantena dei nuovi oggetti. È necessario svuotare manualmente la Quarantena.
Invia notifica quando l'archivio Quarantena raggiunge (%)	Valore soglia della Quarantena. Ad esempio, è possibile impostare la soglia di quarantena su 50%. Quando la Quarantena raggiunge la soglia, Kaspersky Endpoint Security invia l'evento corrispondente a Kaspersky Security Center e pubblica l'evento nel registro eventi di Windows. Nel frattempo, l'applicazione continua a mettere in quarantena i nuovi oggetti.
Trasferimento dei dati ad Administration Server *(disponibile solo in Kaspersky Security Center)*	Categorie di eventi nei computer client le cui informazioni devono essere trasmesse ad Administration Server. È possibile disabilitare il trasferimento di alcuni dati per ottimizzare lo spazio su disco in Administration Server. L'applicazione invia gli eventi delle seguenti categorie: • **Informazioni sui file in Quarantena**. È possibile visualizzare l'elenco dei file in quarantena nella console di Kaspersky Security Center, nella cartella **Avanzate → Archivi → Quarantena**. Kaspersky Endpoint Security utilizza la Quarantena solo quando è integrato con le soluzioni Kaspersky Detection and Response. • **Informazioni sui file in Backup**. È possibile visualizzare l'elenco dei file nel backup nella console di Kaspersky Security Center, nella cartella **Avanzate → Archivi → Backup**. • **Informazioni sui file non elaborati**. È possibile visualizzare l'elenco dei file non elaborati nella console di Kaspersky Security Center, nella cartella **Avanzate → Archivi → Minacce attive**. • **Informazioni sui dispositivi installati**. È possibile visualizzare l'elenco dei dispositivi connessi nella console di Kaspersky Security Center nella cartella **Avanzate → Archivi → Hardware**. L'elenco dei dispositivi è inoltre disponibile nelle proprietà del computer e nel criterio di Kaspersky Endpoint Security for Windows (sezione **Controllo dispositivi**). • **Informazioni sulle applicazioni avviate**. È possibile visualizzare l'elenco dei file eseguibili nella console di Kaspersky Security Center, nella cartella **Avanzate → Gestione applicazioni → File eseguibili**. L'elenco dei file eseguibili è inoltre disponibile nelle proprietà del computer. • **Informazioni sugli errori di criptaggio dei file**. È possibile visualizzare l'elenco degli errori di criptaggio dei file nella console di Kaspersky Security Center, nella cartella **Avanzate → Criptaggio e protezione dei dati → Eventi di criptaggio**. L'elenco degli errori è inoltre disponibile nelle proprietà del computer. • **Rapporto sullo stato delle regole di Controllo adattivo delle anomalie**. È possibile visualizzare il rapporto nella console di Kaspersky Security Center nel nodo **Administration Server** nella scheda **Rapporti**. Questo rapporto è disponibile anche nelle proprietà del criterio di Kaspersky Endpoint Security for Windows (sezione **Controllo adattivo delle anomalie**). • **Rapporto sulle regole attivate di Controllo adattivo delle anomalie**. È possibile visualizzare il rapporto nella console di Kaspersky Security Center nel nodo **Administration Server** nella scheda **Rapporti**. Questo rapporto è disponibile anche nelle proprietà del criterio di Kaspersky Endpoint Security for Windows (sezione **Controllo adattivo delle anomalie**). • **Informazioni su una catena di sviluppo delle minacce**. È possibile visualizzare i dettagli di rilevamento in Kaspersky Security Center Web Console nella sezione **Monitoraggio → Avvisi**. Le informazioni sulla catena di sviluppo delle minacce vengono utilizzate dalle soluzioni Kaspersky Endpoint Detection and Response.

Impostazioni di Rete

È possibile configurare il server proxy utilizzato per la connessione a Internet e l'aggiornamento dei database anti-virus, selezionare la modalità di monitoraggio della porta di rete e configurare una scansione delle connessioni criptate.

Parametro	Descrizione
Limita il traffico sulle connessioni a consumo	Se questa casella è selezionata, l'applicazione limita il proprio traffico di rete in caso di limitazioni della connessione a Internet. Kaspersky Endpoint Security identifica una connessione Internet mobile a elevata velocità come connessione con limitazioni e identifica una connessione Wi-Fi come connessione senza limitazioni. Limitazione traffico di rete funziona nei computer che eseguono Windows 8 o versioni successive.
Inocula script nel traffico Web per interagire con le pagine Web	Se la casella è selezionata, Kaspersky Endpoint Security inocula uno script per l'interazione con le pagine Web nel traffico Web. Questo script garantisce il corretto funzionamento del componente Controllo Web. Lo script consente la registrazione degli eventi di Controllo Web. Senza questo script, non è possibile abilitare il monitoraggio dell'attività Internet dell'utente. Gli esperti di Kaspersky consigliano di inoculare questo script per l'interazione con le pagine Web nel traffico per garantire il corretto funzionamento di Controllo Web.
Impostazioni del server proxy	Impostazioni del server proxy utilizzato per l'accesso a Internet degli utenti dei computer client. Kaspersky Endpoint Security utilizza queste impostazioni per determinati componenti della protezione, oltre che per l'aggiornamento dei database e dei moduli dell'applicazione. Per la configurazione automatica di un server proxy, Kaspersky Endpoint Security utilizza il protocollo WPAD (Web Proxy Auto-Discovery Protocol). Se non è possibile determinare l'indirizzo IP del server proxy utilizzando questo protocollo, l'applicazione utilizza l'indirizzo del server proxy specificato nelle impostazioni del browser Microsoft Internet Explorer.
Ignora il server proxy per gli indirizzi locali	Se la casella di controllo è selezionata, Kaspersky Endpoint Security non utilizza un server proxy durante un aggiornamento da una cartella condivisa.
Impostazioni di autenticazione del server proxy	Per autenticare l'applicazione nel server proxy per l'accesso a Internet, è necessario immettere le credenziali dell'utente. Kaspersky Endpoint Security supporta l'autenticazione automatica nel server proxy. Se l'autenticazione automatica non riesce, l'applicazione richiede di immettere le credenziali. **Non usare l'autenticazione**. **Autenticazione NTLM**. Autenticazione NTLM con l'account utente corrente (impostazione predefinita). **Autenticazione NTLM con nome utente e password**. Autenticazione NTLM con le credenziali specificate manualmente. **Nome utente e password**. Autenticazione con le credenziali specificate manualmente. **Autenticazione automatica**. **Autenticazione Kerberos**. Autenticazione Kerberos con l'account utente corrente. Per garantire il corretto funzionamento dell'autenticazione Kerberos quando si utilizzano record CNAME per l'indirizzo del server proxy, è necessario registrare un nome dell'entità servizio (SPN, Service Principal Name) per ogni record CNAME. **Autenticazione Kerberos con nome utente e password**. Autenticazione Kerberos con le credenziali specificate manualmente. Se è selezionata l'autenticazione Kerberos, Kaspersky Endpoint Security può, in base alle impostazioni del server proxy, eseguire l'autenticazione utilizzando il protocollo NTLM o Kerberos.
Porte monitorate	**Monitora tutte le porte di rete**. In questa modalità di monitoraggio delle porte di rete, i componenti della protezione (Protezione minacce file, Protezione minacce Web e Protezione minacce di posta) monitorano i flussi di dati trasmessi tramite qualsiasi porta di rete aperta del computer. **Monitora solo le porte di rete selezionate**. In questa modalità di monitoraggio delle porte di rete i componenti della protezione monitorano le porte selezionate del computer e l'attività di rete delle applicazioni selezionate. L'elenco delle porte di rete normalmente utilizzate per la trasmissione del traffico di posta elettronica e di rete è configurato in base ai suggerimenti degli esperti di Kaspersky. **Monitora tutte le porte per le applicazioni dell'elenco consigliato da Kaspersky**. Viene utilizzato un elenco predefinito di applicazioni le cui porte di rete sono monitorate da Kaspersky Endpoint Security. Questo elenco include ad esempio Google Chrome, Adobe Reader, Java e altre applicazioni. **Monitora tutte le porte per le applicazioni specificate**. Viene utilizzato un elenco di applicazioni le cui porte di rete sono monitorate da Kaspersky Endpoint Security.

Parametro	Descrizione
Scansione delle connessioni criptate	Kaspersky Endpoint Security esamina il traffico di rete criptato trasmesso tramite i seguenti protocolli: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security supporta le seguenti modalità di scansione delle connessioni criptate: • **Non esaminare le connessioni criptate**. Kaspersky Endpoint Security non avrà accesso ai contenuti dei siti Web i cui indirizzi iniziano con `https://`. • **Esamina le connessioni criptate su richiesta da parte dei componenti della protezione**. Kaspersky Endpoint Security esaminerà il traffico criptato solo quando richiesto dai componenti Protezione minacce Web, Protezione minacce di posta e Controllo Web. • **Esamina sempre le connessioni criptate**. Kaspersky Endpoint Security esaminerà il traffico di rete criptato anche se i componenti della protezione sono disabilitati. Kaspersky Endpoint Security non esegue la scansione delle connessioni criptate stabilite da applicazioni attendibili per le quali la scansione del traffico è disabilitata. Kaspersky Endpoint Security non esegue la scansione delle connessioni criptate dall'elenco predefinito di siti Web attendibili. L'elenco predefinito di siti Web attendibili viene creato dagli esperti di Kaspersky. Questo elenco viene aggiornato con i database anti-virus dell'applicazione. È possibile visualizzare l'elenco predefinito di siti Web attendibili esclusivamente nell'interfaccia di Kaspersky Endpoint Security. Non è possibile visualizzare l'elenco in Kaspersky Security Center Console.
Certificati radice attendibili	Elenco dei certificati radice attendibili. Kaspersky Endpoint Security consente di installare i certificati radice attendibili nei computer degli utenti se, ad esempio, è necessario distribuire un nuovo centro di certificazione. L'applicazione consente di aggiungere un certificato a uno speciale archivio certificati di Kaspersky Endpoint Security. In questo caso, il certificato viene considerato attendibile solo per l'applicazione Kaspersky Endpoint Security. In altre parole, l'utente può accedere a un sito Web con il nuovo certificato nel browser. Se un'altra applicazione tenta di accedere al sito Web, è possibile che si verifichi un errore di connessione a causa di un problema di certificato. Per aggiungere all'archivio certificati di sistema, è possibile utilizzare i criteri di gruppo di Active Directory.
Visita di un dominio con un certificato non attendibile	• **Consenti**. Quando si visita un dominio con un certificato non attendibile, Kaspersky Endpoint Security consente la connessione di rete. Quando si apre un dominio con un certificato non attendibile in un browser, Kaspersky Endpoint Security visualizza una pagina HTML con un avviso e il motivo per cui è consigliabile non visitare il dominio. Un utente può fare clic sul collegamento dalla pagina HTML di avviso per ottenere l'accesso alla risorsa Web richiesta. Se un'applicazione o un servizio di terzi stabilisce una connessione con un dominio dotato di un certificato non attendibile, Kaspersky Endpoint Security crea il proprio certificato per esaminare il traffico. Il nuovo certificato presenta lo stato *Non attendibili.* Ciò è necessario per avvisare l'applicazione di terzi della connessione non attendibile perché in questo caso la pagina HTML non può essere visualizzata e la connessione può essere stabilita in background. • **Blocca**. Quando si visita un dominio con un certificato non attendibile, Kaspersky Endpoint Security blocca la connessione di rete. Quando si apre un dominio con un certificato non attendibile in un browser, Kaspersky Endpoint Security visualizza una pagina HTML con il motivo per cui il dominio è bloccato.
Visita di un dominio con un errore di scansione delle connessioni criptate	• **Blocca**. Se si verifica un errore di scansione delle connessioni criptate, Kaspersky Endpoint Security blocca la connessione di rete. • **Consenti e aggiungi dominio alle esclusioni**. Se si verifica un errore di scansione delle connessioni criptate, Kaspersky Endpoint Security aggiunge il dominio che ha generato l'errore all'elenco dei domini con errori di scansione e non monitora il traffico di rete criptato quando viene visitato questo dominio. È possibile visualizzare un elenco dei domini con errori di scansione delle connessioni criptate solo nell'interfaccia locale dell'applicazione. Per cancellare i contenuti dell'elenco è necessario selezionare **Blocca**. Kaspersky Endpoint Security genera anche un evento per l'errore di scansione della connessione criptata.
Blocca le connessioni SSL 2.0	Se la casella di controllo è selezionata, l'applicazione monitora e blocca le connessioni di rete stabilite tramite il protocollo SSL 2.0. Se la casella di controllo è deselezionata, l'applicazione non blocca le connessioni di rete stabilite tramite il protocollo SSL 2.0. L'applicazione tuttavia non monitora il traffico di rete su questo protocollo.
Blocca le connessioni SSL 3.0	Se la casella di controllo è selezionata, l'applicazione blocca le connessioni di rete stabilite tramite il protocollo SSL 3.0. Se la casella di controllo è deselezionata, l'applicazione non blocca le connessioni di rete stabilite tramite il protocollo SSL 3.0. L'applicazione monitora il traffico di rete tramite questo protocollo. Tutti i componenti dell'applicazione funzionano senza restrizioni.
Blocca le connessioni TLS 1.0	Se la casella di controllo è selezionata, l'applicazione blocca le connessioni di rete stabilite tramite il protocollo TLS 1.0. Se la casella di controllo è deselezionata, l'applicazione non blocca le connessioni di rete stabilite tramite il protocollo TLS 1.0. L'applicazione monitora il traffico di rete tramite questo protocollo. Tutti i componenti dell'applicazione funzionano senza restrizioni.

Parametro	Descrizione
Decripta una connessione criptata con il sito Web che utilizza il certificato EV	I certificati EV (Extended Validation Certificate) confermano l'autenticità dei siti Web e ottimizzano la sicurezza della connessione. I browser utilizzano un'icona a forma di lucchetto nella barra degli indirizzi per indicare che un sito Web dispone di un certificato EV. I browser possono inoltre colorare in modo parziale o completo la barra degli indirizzi di verde. Se la casella di controllo è selezionata, l'applicazione decripta e monitora le connessioni criptate con siti Web che utilizzano un certificato EV. Se la casella di controllo è deselezionata, l'applicazione non ha accesso ai contenuti del traffico HTTPS. Per questo motivo l'applicazione monitora il traffico HTTPS solo in base all'indirizzo del sito Web, ad esempio `https://bing.com`. Se si apre un sito Web con un certificato EV per la prima volta, la connessione criptata verrà decriptata indipendentemente dal fatto che la casella di controllo sia selezionata o meno.
Configura indirizzi attendibili	Viene utilizzato un elenco di indirizzi Web per cui Kaspersky Endpoint Security non esamina le connessioni di rete. In questo caso, Kaspersky Endpoint Security non esamina il traffico HTTPS degli indirizzi Web attendibili quando i componenti Protezione minacce Web, Protezione minacce di posta e Controllo Web sono in esecuzione. È possibile immettere un nome di dominio o un indirizzo IP. Kaspersky Endpoint Security supporta il carattere `*` per l'immissione di una maschera nel nome di dominio. Kaspersky Endpoint Security non supporta il simbolo `*` per gli indirizzi IP. È possibile selezionare un intervallo di indirizzi IP usando una maschera di sottorete (ad esempio 198.51.100.0/24). Esempi: • `domain.com` – Il record comprende i seguenti indirizzi: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Il record è esclusivo dei sottodomini (ad esempio, `subdomain.domain.com`). • `subdomain.domain.com` – Il record comprende i seguenti indirizzi: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Il record è esclusivo del dominio `domain.com`. • `*.domain.com` – Il record comprende i seguenti indirizzi: `https://movies.domain.com`, `https://images.domain.com/page123`. Il record è esclusivo del dominio `domain.com`.
Configura applicazioni attendibili	Elenco delle applicazioni le cui attività non vengono monitorate da Kaspersky Endpoint Security durante l'esecuzione. È possibile selezionare i tipi di attività delle applicazioni che Kaspersky Endpoint Security non monitorerà (ad esempio non esaminare il traffico di rete). Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri `*` e `?` durante l'immissione di una maschera.
Per eseguire la scansione delle connessioni criptate nelle applicazioni con il proprio archivio certificati, utilizzare *(disponibile solo nell'interfaccia di Kaspersky Endpoint Security)*	Se questa casella di controllo è selezionata, l'applicazione esamina il traffico criptato nel browser Mozilla Firefox e nel client di posta Thunderbird. L'accesso ad alcuni siti Web tramite il protocollo HTTPS potrebbe essere bloccato. Per esaminare il traffico nel browser Mozilla Firefox e nel client di posta Thunderbird, è necessario abilitare Scansione delle connessioni criptate. Se Scansione delle connessioni criptate è disabilitata, l'applicazione non esamina il traffico nel browser Mozilla Firefox e nel client di posta Thunderbird. L'applicazione utilizza il certificato radice di Kaspersky per decriptare e analizzare il traffico criptato. È possibile selezionare l'archivio certificati che conterrà il certificato radice di Kaspersky. • **Archivio certificati Windows (scelta consigliata)**. Il certificato radice di Kaspersky viene aggiunto a questo archivio durante l'installazione di Kaspersky Endpoint Security. • **Archivio certificati personali**. Mozilla Firefox e Thunderbird utilizzano i propri archivi di certificati. Se è selezionato l'archivio certificati Mozilla, è necessario aggiungere manualmente il certificato radice Kaspersky a questo archivio tramite le proprietà del browser.

Interfaccia

È possibile configurare le impostazioni dell'interfaccia dell'applicazione.

Parametro	Descrizione
Interazione con l'utente *(disponibile solo in Kaspersky Security Center Console)*	**Visualizza interfaccia semplificata**. In un computer client, la finestra principale dell'applicazione non è accessibile ed è disponibile solo l'icona nell'area di notifica di Windows. Nel menu di scelta rapida dell'icona l'utente può eseguire un numero limitato di operazioni con Kaspersky Endpoint Security. Kaspersky Endpoint Security mostra inoltre solo le notifiche che richiedono l'azione dell'utente sopra l'icona dell'applicazione. **Visualizza interfaccia utente**. In un computer client sono disponibili la finestra principale di Kaspersky Endpoint Security e l'icona nell'area di notifica Windows. Nel menu di scelta rapida dell'icona l'utente può eseguire operazioni con Kaspersky Endpoint Security. Kaspersky Endpoint Security visualizza inoltre le notifiche sopra l'icona dell'applicazione. **Nascondi sezione Monitor attività applicazioni**. Sul computer client, nella finestra principale di Kaspersky Endpoint Security, il pulsante **Monitor attività applicazioni** non è disponibile. *Monitor attività applicazioni* è uno strumento progettato per la visualizzazione in tempo reale di informazioni sulle attività delle applicazioni nel computer di un utente. **Non visualizzare l'interfaccia utente**. In un computer client non vengono visualizzati segni di esecuzione di Kaspersky Endpoint Security. L'icona nell'area di notifica di Windows e le notifiche non sono disponibili.
Accesso alle attività locali	Se la casella di controllo è selezionata, le attività locali vengono visualizzate nell'interfaccia locale di Kaspersky Endpoint Security. Se non sono presenti ulteriori restrizioni a livello di criterio, l'utente può configurare ed eseguire le attività. Tuttavia, la configurazione della pianificazione dell'esecuzione delle attività rimane non disponibile per l'utente. L'utente può eseguire le attività solo manualmente. Se questa casella di controllo è deselezionata, le attività locali vengono nascoste nell'interfaccia dell'applicazione. In questa modalità, le attività locali non vengono eseguite in base alla pianificazione. Non è possibile avviare o configurare le attività nell'interfaccia locale di Kaspersky Endpoint Security o durante l'utilizzo della riga di comando. Un utente può comunque avviare una scansione di un file o una cartella selezionando l'opzione **Ricerca virus** nel menu di scelta rapida del file o della cartella. L'attività di scansione viene avviata con i valori predefiniti delle impostazioni per l'attività Scansione personalizzata.
Visualizza attività di gruppo	Se la casella di controllo è selezionata, le attività di gruppo vengono visualizzate nell'interfaccia locale di Kaspersky Endpoint Security. L'utente può visualizzare l'elenco di tutte le attività nell'interfaccia dell'applicazione. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security visualizza un elenco di attività vuoto.
Gestisci attività di gruppo	Se la casella di controllo è selezionata, gli utenti possono avviare e arrestare le attività di gruppo specificate nella console di Kaspersky Security Center. Gli utenti possono avviare e arrestare le attività nell'interfaccia dell'applicazione o nell'interfaccia dell'applicazione semplificata. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security avvia automaticamente le attività pianificate oppure l'amministratore avvia le attività manualmente nella console di Kaspersky Security Center.
Configura notifiche	Tabella con le impostazioni delle notifiche degli eventi dei vari livelli di importanza che possono verificarsi durante l'esecuzione di un componente, un'attività o dell'intera applicazione. Kaspersky Endpoint Security visualizza le notifiche di questi eventi sullo schermo, le invia tramite e-mail o le registra.
Configura le notifiche via e-mail	Impostazioni del server SMTP per l'invio delle notifiche sugli eventi registrati durante il funzionamento dell'applicazione. Per impostazione predefinita, Kaspersky Endpoint Security utilizza le impostazioni di notifica e-mail di Kaspersky Security Center. Per ulteriori dettagli sulle impostazioni di notifica e-mail, consultare la Guida di Kaspersky Security Center. Se è necessario configurare la singola notifica e-mail è possibile modificare le seguenti impostazioni: • **Indirizzo mittente**. Indirizzo e-mail del mittente. L'utilizzo di un indirizzo inesistente non è consigliato. • **Server SMTP**. Uno o più indirizzi di server e-mail dell'organizzazione (ad esempio, `mail.company.com`). È possibile immettere un indirizzo IP (IPv4 o IPv6). Per autenticare l'utente sul server SMTP, inserire le credenziali del mittente nei campi corrispondenti. Per testare le notifiche e-mail, è possibile inviare un messaggio di prova. • **Indirizzo destinatario**. Indirizzi e-mail dei destinatari a cui l'applicazione invierà le notifiche. • **Modalità di invio**. Modalità di invio delle notifiche e-mail. Kaspersky Endpoint Security può inviare messaggi immediatamente quando si verifica un evento; in alternativa, può seguire una pianificazione preconfigurata.
Mostra lo stato dell'applicazione nell'area di notifica	Categorie degli eventi dell'applicazione che determinano la modifica dell'icona di Kaspersky Endpoint Security nell'area di notifica della barra delle applicazioni di Microsoft Windows (o) e generano una notifica pop-up.
Notifiche dello stato dei database anti-malware locali	Impostazioni delle notifiche sui database anti-virus non aggiornati utilizzati dall'applicazione.
Protezione tramite password	Se l'interruttore è attivato, Kaspersky Endpoint Security richiede all'utente una password quando tenta di eseguire un'operazione nell'ambito di Protezione tramite password. L'ambito di Protezione tramite password include le operazioni vietate (ad esempio la disabilitazione dei componenti della protezione) e gli account utente a cui si applica l'ambito di Protezione tramite password. Dopo l'abilitazione di Protezione tramite password, Kaspersky Endpoint Security richiede all'utente di impostare una password per l'account KLAdmin.

Parametro	Descrizione
Assistenza agli utenti/Collegamenti a risorse Web *(disponibile solo in Kaspersky Security Center Console)*	Elenco dei collegamenti a risorse Web che contengono informazioni sull'assistenza tecnica per Kaspersky Endpoint Security. I collegamenti aggiunti saranno visualizzati nella finestra **Assistenza** dell'interfaccia locale di Kaspersky Endpoint Security al posto dei collegamenti standard.
Assistenza agli utenti/Descrizione *(disponibile solo in Kaspersky Security Center Console)*	Messaggio visualizzato nella finestra **Assistenza** dell'interfaccia locale di Kaspersky Endpoint Security.

Gestione impostazioni

È possibile salvare le impostazioni correnti di Kaspersky Endpoint Security in un file e utilizzarle per configurare rapidamente l'applicazione in un altro computer. È inoltre possibile utilizzare un file di configurazione durante la distribuzione dell'applicazione tramite Kaspersky Security Center con un pacchetto di installazione. È possibile ripristinare le impostazioni predefinite in qualsiasi momento.

Le impostazioni di gestione della configurazione dell'applicazione sono disponibili solo nell'interfaccia di Kaspersky Endpoint Security.

Impostazioni di gestione della configurazione dell'applicazione

Impostazioni	Descrizione
Importa	Consente di estrarre le impostazioni dell'applicazione da un file in formato CFG e di applicarle.
Esporta	Consente di salvare le impostazioni correnti dell'applicazione in un file in formato CFG.
Ripristina	È possibile ripristinare le impostazioni dell'applicazione consigliate da Kaspersky in qualsiasi momento. Quando le impostazioni sono state ripristinate, viene impostato il livello di sicurezza **Consigliato** per tutti i componenti di protezione.

Aggiornamento di database e moduli software dell'applicazione

L'aggiornamento dei database e dei moduli dell'applicazione di Kaspersky Endpoint Security assicura il massimo livello di protezione del computer. In tutto il mondo appaiono quotidianamente nuovi virus e altri tipi di malware. I database di Kaspersky Endpoint Security contengono informazioni sulle minacce e sui metodi per eliminarle. Per rilevare rapidamente le minacce, è importante eseguire periodicamente l'aggiornamento dei database e dei moduli dell'applicazione.

La funzionalità Aggiornamenti (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) potrebbe non essere disponibile nell'applicazione negli Stati Uniti.

Gli aggiornamenti periodici richiedono una licenza valida. Se non è disponibile alcuna licenza, è possibile eseguire un aggiornamento una sola volta.

Il computer deve essere connesso a Internet per consentire il download del pacchetto di aggiornamento dai server degli aggiornamenti Kaspersky. Per impostazione predefinita, le impostazioni di connessione a Internet vengono determinate automaticamente. Se si utilizza un server proxy, è necessario configurare le impostazioni del server proxy.

Gli aggiornamenti vengono scaricati tramite il protocollo HTTPS. Possono inoltre essere scaricati tramite il protocollo HTTP quando non è possibile scaricare gli aggiornamenti tramite il protocollo HTTPS.

Durante l'esecuzione di un aggiornamento, vengono scaricati e installati nel computer i seguenti oggetti:

- Database di Kaspersky Endpoint Security. La protezione del computer viene garantita dai database che contengono le firme di virus e altre minacce e informazioni sulle modalità per neutralizzarli. I componenti della protezione utilizzano queste informazioni per cercare e neutralizzare i file infetti nel computer. I database vengono costantemente aggiornati con i record relativi alle nuove minacce e i metodi per contrastarle. È pertanto consigliabile aggiornare periodicamente i database.

  Oltre ai database di Kaspersky Endpoint Security, vengono aggiornati i driver di rete che consentono ai componenti dell'applicazione di intercettare il traffico di rete.

- Moduli dell'applicazione. Oltre ai database di Kaspersky Endpoint Security, è possibile aggiornare i moduli dell'applicazione. L'aggiornamento dei moduli dell'applicazione consente di correggere le vulnerabilità di Kaspersky Endpoint Security, aggiungere nuove funzioni o migliorare quelle esistenti.

Durante un aggiornamento, i moduli dell'applicazione e i database nel computer vengono confrontati con la versione aggiornata disponibile nella sorgente degli aggiornamenti. Se i database e i moduli dell'applicazione correnti sono differenti dalle rispettive versioni più recenti, la parte mancante di aggiornamenti viene installata nel computer.

Se i database sono obsoleti, il pacchetto di aggiornamento può essere di grandi dimensioni, causando traffico internet aggiuntivo (fino a decine di MB).

Le informazioni sullo stato corrente dei database di Kaspersky Endpoint Security vengono visualizzate nella finestra principale dell'applicazione o nella descrizione comandi visualizzata quando si passa il cursore sull'icona dell'applicazione nell'area di notifica.

Le informazioni sui risultati dell'aggiornamento e su tutti gli eventi che si verificano durante l'esecuzione dell'attività vengono registrate in un rapporto di Kaspersky Endpoint Security.

Se l'applicazione funziona in modalità Light Agent, considerazioni speciali sono coinvolte nell'aggiornamento dei database e dei moduli dell'applicazione.

Impostazioni di aggiornamento dei database e dei moduli dell'applicazione

Parametro	Descrizione
Pianificazione aggiornamento database	**Automaticamente**. In questa modalità, l'applicazione verifica con una certa frequenza se sono disponibili nuovi pacchetti di aggiornamento nella sorgente degli aggiornamenti. La frequenza del controllo dei pacchetti di aggiornamento aumenta durante gli attacchi di virus e si riduce in assenza di attacchi. Quando viene rilevato un nuovo pacchetto di aggiornamento, Kaspersky Endpoint Security lo scarica e installa gli aggiornamenti nel computer. **Manualmente**. Questa modalità di esecuzione dell'attività di aggiornamento consente di avviare manualmente l'attività. **In base alla pianificazione**. In questa modalità di esecuzione, Kaspersky Endpoint Security esegue l'attività di aggiornamento in base alla pianificazione specificata dall'utente. Se si seleziona questa modalità di esecuzione, è anche possibile avviare manualmente l'attività di aggiornamento di Kaspersky Endpoint Security.

Parametro	Descrizione
Esegui attività non effettuate	Se la casella di controllo è selezionata, Kaspersky Endpoint Security avvia l'attività ignorata appena possibile. L'attività può ad esempio essere ignorata se il computer è spento all'orario impostato per l'avvio dell'attività pianificata. Quando l'applicazione ha l'opportunità di eseguire le attività non effettuate, esegue le attività in modo casuale entro un determinato intervallo di tempo per distribuire il carico sul computer. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non esegue le attività ignorate. Viene invece eseguita l'attività successiva, in base alla pianificazione corrente.
Sorgenti degli aggiornamenti	Una *sorgente degli aggiornamenti* è una risorsa che contiene gli aggiornamenti per i database e i moduli dell'applicazione di Kaspersky Endpoint Security. Le sorgenti degli aggiornamenti includono il server Kaspersky Security Center, i server degli aggiornamenti Kaspersky e cartelle di rete o locali. Se i server di aggiornamento Kaspersky non sono disponibili, Kaspersky Endpoint Security può utilizzare domini alternativi per aggiornare i database e i moduli del software applicativo. Per informazioni dettagliate, consultare la Knowledge Base dell'Assistenza tecnica. L'elenco predefinito di sorgenti degli aggiornamenti include Kaspersky Security Center e i server degli aggiornamenti Kaspersky. È possibile aggiungere all'elenco altre sorgenti degli aggiornamenti. È possibile specificare server HTTP/FTP e cartelle condivise come sorgenti degli aggiornamenti. Kaspersky Endpoint Security non supporta gli aggiornamenti dai server HTTPS, a meno che non si tratti dei server degli aggiornamenti Kaspersky. Se sono state selezionate più risorse come sorgenti degli aggiornamenti, Kaspersky Endpoint Security tenta di connettersi a esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco e recupera gli aggiornamenti dalla prima disponibile. Per impostazione predefinita, Kaspersky Endpoint Security utilizza il server Kaspersky Security Center come prima sorgente di aggiornamenti. Questo aiuta a conservare il traffico durante l'aggiornamento. Se un criterio non viene applicato al computer, i server Kaspersky vengono selezionati come prima sorgente degli aggiornamenti nelle impostazioni dell'attività locale *Aggiornamento di database e moduli dell'applicazione* perché l'applicazione potrebbe non avere accesso al server Kaspersky Security Center. Se l'applicazione è in esecuzione in modalità Light Agent, una cartella nella SVM è selezionata come sorgente degli aggiornamenti.
Esegui aggiornamenti dei database come	Per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività di aggiornamento tramite l'account utente con cui è stato eseguito l'accesso al sistema operativo. Tuttavia, Kaspersky Endpoint Security potrebbe essere aggiornato da una sorgente degli aggiornamenti a cui l'utente non può accedere perché non dispone dei diritti richiesti (ad esempio da una cartella condivisa che contiene un pacchetto di aggiornamento) oppure da una sorgente degli aggiornamenti per cui l'autenticazione sul server proxy non è configurata. Nelle impostazioni dell'applicazione, è possibile specificare un utente che dispone di tali diritti e avviare l'attività di aggiornamento di Kaspersky Endpoint Security utilizzando tale account utente.

Parametro	Descrizione
Scarica aggiornamenti dei moduli dell'applicazione	Download degli aggiornamenti del modulo dell'applicazione con gli aggiornamenti del database dell'applicazione. Se la casella di controllo è selezionata, Kaspersky Endpoint Security notifica all'utente gli aggiornamenti dei moduli dell'applicazione disponibili e include gli aggiornamenti dei moduli dell'applicazione nel pacchetto di aggiornamento quando viene eseguita l'attività di aggiornamento. Il modo in cui vengono applicati gli aggiornamenti dei moduli dell'applicazione è determinato dalle seguenti impostazioni: • **Installa aggiornamenti critici e approvati**. Se questa opzione è selezionata, quando sono disponibili aggiornamenti dei moduli dell'applicazione, Kaspersky Endpoint Security installa automaticamente gli aggiornamenti critici e tutti gli altri aggiornamenti dei moduli dell'applicazione solo una volta che la relativa installazione viene approvata in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center. • **Installa solo gli aggiornamenti approvati**. Se questa opzione è selezionata, quando sono disponibili aggiornamenti dei moduli dell'applicazione, Kaspersky Endpoint Security li installa solo una volta che la relativa installazione viene approvata in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center. Questa opzione è selezionata per impostazione predefinita. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non notifica all'utente gli aggiornamenti dei moduli dell'applicazione disponibili e non include gli aggiornamenti dei moduli dell'applicazione nel pacchetto di aggiornamento quando viene eseguita l'attività di aggiornamento. Se gli aggiornamenti dei moduli dell'applicazione richiedono la lettura e l'accettazione delle condizioni del Contratto di licenza con l'utente finale, l'applicazione li installa una volta che il Contratto di licenza con l'utente finale è stato accettato. La casella di controllo è selezionata per impostazione predefinita.
Copia aggiornamenti nella cartella	Se questa casella di controllo è selezionata, Kaspersky Endpoint Security copia il pacchetto di aggiornamento nella cartella condivisa specificata sotto la casella di controllo. Gli altri computer della rete LAN sono quindi in grado di ricevere il pacchetto di aggiornamento da questa cartella condivisa. Questo riduce il traffico Internet, dal momento che il pacchetto di aggiornamento viene scaricato solo una volta. Per impostazione predefinita, è specificata la cartella seguente: `C:\ProgramData\Kaspersky Lab\KES.14.2\Update distribution\`.
Server proxy per gli aggiornamenti *(disponibile solo nell'interfaccia di Kaspersky Endpoint Security)*	Impostazioni del server proxy per l'accesso a Internet degli utenti dei computer client per aggiornare i moduli e i database dell'applicazione. Per la configurazione automatica di un server proxy, Kaspersky Endpoint Security utilizza il protocollo WPAD (Web Proxy Auto-Discovery Protocol). Se non è possibile determinare l'indirizzo IP del server proxy utilizzando questo protocollo, Kaspersky Endpoint Security utilizza l'indirizzo del server proxy specificato nelle impostazioni del browser Microsoft Internet Explorer.
Ignora il server proxy per gli indirizzi locali *(disponibile solo nell'interfaccia di Kaspersky Endpoint Security)*	Se la casella di controllo è selezionata, Kaspersky Endpoint Security non utilizza un server proxy durante un aggiornamento da una cartella condivisa.

Appendice 2. Gruppi di attendibilità delle applicazioni

Kaspersky Endpoint Security categorizza tutte le applicazioni avviate nel computer in gruppi di attendibilità. Le applicazioni vengono assegnate ai gruppi di attendibilità in base al loro livello di pericolosità per il sistema operativo.

I gruppi di attendibilità sono i seguenti:

- **Attendibili**. Questo gruppo include le applicazioni per cui sono soddisfatte una o più delle seguenti condizioni:
  - Le applicazioni dispongono di firme digitali di produttori attendibili.
  - Le applicazioni sono registrate nel database di applicazioni attendibili di Kaspersky Security Network.
  - L'applicazione è stata inserita dall'utente nel gruppo *Attendibili*.

  Per queste applicazioni non è vietata alcuna operazione.

- **Restrizione bassa**. Questo gruppo include le applicazioni per cui sono soddisfatte le seguenti condizioni:
  - Le applicazioni non dispongono di firme digitali di produttori attendibili.
  - Le applicazioni non sono registrate nel database di applicazioni attendibili di Kaspersky Security Network.
  - L'applicazione è stata inserita dall'utente nel gruppo *Restrizione bassa*.

  Queste applicazioni sono soggette a restrizioni minime per l'accesso alle risorse del sistema operativo.
- **Restrizione alta**. Questo gruppo include le applicazioni per cui sono soddisfatte le seguenti condizioni:
  - Le applicazioni non dispongono di firme digitali di produttori attendibili.
  - Le applicazioni non sono registrate nel database di applicazioni attendibili di Kaspersky Security Network.
  - L'applicazione è stata inserita dall'utente nel gruppo *Restrizione alta*.

  Queste applicazioni sono soggette a restrizioni elevate per l'accesso alle risorse del sistema operativo.
- **Non attendibili**. Questo gruppo include le applicazioni per cui sono soddisfatte le seguenti condizioni:
  - Le applicazioni non dispongono di firme digitali di produttori attendibili.
  - Le applicazioni non sono registrate nel database di applicazioni attendibili di Kaspersky Security Network.
  - L'applicazione è stata inserita dall'utente nel gruppo *Non attendibili*.

  Per queste applicazioni, tutte le operazioni sono bloccate.

Appendice 3. Estensioni file per la scansione rapida delle unità rimovibili

com – file eseguibile di un'applicazione di dimensioni non superiori a 64 KB

exe – file eseguibile o archivio autoestraente

sys – file di sistema di Microsoft Windows

prg – testo di un programma dBase™, Clipper, Microsoft Visual FoxPro® o WAVmaker

bin – file binario

bat – file batch

cmd – riga di comando per Microsoft Windows NT (simile a un file bat per DOS), OS/2

dpl – libreria compressa Borland Delphi

dll – libreria a collegamento dinamico

scr – schermata iniziale di Microsoft Windows

cpl – modulo del Pannello di controllo di Microsoft Windows

ocx – oggetto Microsoft OLE (Object Linking and Embedding)

tsp – programma eseguito in modalità split-time

drv – driver di dispositivo

vxd – driver di dispositivo virtuale di Microsoft Windows

pif – file di informazioni sul programma

lnk – file di collegamento di Microsoft Windows

reg – file chiave del Registro di sistema di Microsoft Windows

ini – file di configurazione che contiene dati di configurazione per Microsoft Windows, Windows NT e determinate applicazioni

cla – classe Java

vbs – script Visual Basic®

vbe – estensione video BIOS

js, jse – testo sorgente JavaScript

htm – documento ipertestuale

htt – intestazione ipertesto di Microsoft Windows

hta – programma di ipertesto per Microsoft Internet Explorer®

asp – script Active Server Pages

chm – file HTML compilato

pht – file HTML integrato con script PHP

php – script incorporato in file HTML

wsh – file Microsoft Windows Script Host

wsf – script Microsoft Windows

the – sfondo del desktop di Microsoft Windows 95

hlp – file della Guida di Windows

msg – messaggio e-mail di Microsoft Mail

plg – messaggio di posta elettronica

mbx – messaggio e-mail di Microsoft Office Outlook salvato

doc* – documenti di Microsoft Office Word, quali doc per i documenti di Microsoft Office Word, docx per i documenti di Microsoft Office Word 2007 con supporto XML e docm per i documenti di Microsoft Office Word 2007 con supporto per le macro

dot* – modelli di documenti di Microsoft Office Word, quali dot per i modelli di documenti Microsoft Office Word, dotx per i modelli di documenti di Microsoft Office Word 2007, dotm per i modelli di documenti di Microsoft Office Word 2007 con supporto per le macro

fpm – programma di database, file di avvio di Microsoft Visual FoxPro

rtf – documento Rich Text Format

shs – frammento di Windows Shell Scrap Object Handler

dwg – database di disegni AutoCAD®

msi – pacchetto di Microsoft Windows Installer

otm – progetto VBA per Microsoft Office Outlook

pdf – documento di Adobe Acrobat

swf – oggetto pacchetto di Shockwave® Flash

jpg, jpeg – formato grafico compresso per immagini

emf – formato di file Enhanced Metafile;

ico – oggetto file icona

Ov? – file eseguibili di Microsoft Office Word

xl* – documenti e file di Microsoft Office Excel, quali xla (estensione di Microsoft Office Excel), xlc per i diagrammi, xlt per i modelli di documento, xlsx per le cartelle di lavoro di Microsoft Office Excel 2007, xltm per le cartelle di lavoro di Microsoft Office Excel 2007 con supporto per le macro, xlsb per le cartelle di lavoro di Microsoft Office Excel 2007 in formato binario (non XML), xltx per i modelli di Microsoft Office Excel 2007, xlsm per i modelli di Microsoft Office Excel 2007 con supporto per le macro, xlam per i plug-in di Microsoft Office Excel 2007 con supporto per le macro

pp* – documenti e file di Microsoft Office PowerPoint®, quali pps per le diapositive di Microsoft Office PowerPoint, ppt per le presentazioni, pptx per le presentazioni di Microsoft Office PowerPoint 2007, pptm per le presentazioni di Microsoft Office PowerPoint 2007 con supporto per le macro, potx per i modelli di presentazione di Microsoft Office PowerPoint 2007, potm per i modelli di presentazione di Microsoft Office PowerPoint 2007 con supporto per le macro, ppsx per le presentazioni di Microsoft Office PowerPoint 2007, ppsm per le presentazioni di Microsoft Office PowerPoint 2007 con supporto per le macro, ppam per i plug-in di Microsoft Office PowerPoint 2007 con supporto per le macro

md* – documenti e file di Microsoft Office Access®, quali mda per i gruppi di lavoro di Microsoft Office Access e mdb per i database

sldx – diapositiva di Microsoft PowerPoint 2007

sldm – diapositiva di Microsoft PowerPoint 2007 con supporto per le macro

thmx – tema di Microsoft Office 2007

Appendice 4. Tipi di file per il filtro allegati di Protezione minacce di posta

Si tenga presente che il formato effettivo di un file potrebbe non corrispondere all'estensione del nome del file.

Se è stato abilitato il filtro degli allegati e-mail, il componente Protezione minacce di posta può rinominare o eliminare i file con le seguenti estensioni:

com – file eseguibile di un'applicazione di dimensioni non superiori a 64 KB

exe – file eseguibile o archivio autoestraente

sys – file di sistema di Microsoft Windows

prg – testo di un programma dBase™, Clipper, Microsoft Visual FoxPro® o WAVmaker

bin – file binario

bat – file batch

cmd – riga di comando per Microsoft Windows NT (simile a un file bat per DOS), OS/2

dpl – libreria compressa Borland Delphi

dll – libreria a collegamento dinamico

scr – schermata iniziale di Microsoft Windows

cpl – modulo del Pannello di controllo di Microsoft Windows

ocx – oggetto Microsoft OLE (Object Linking and Embedding)

tsp – programma eseguito in modalità split-time

drv – driver di dispositivo

vxd – driver di dispositivo virtuale di Microsoft Windows

pif – file di informazioni sul programma

lnk – file di collegamento di Microsoft Windows

reg – file chiave del Registro di sistema di Microsoft Windows

ini – file di configurazione che contiene dati di configurazione per Microsoft Windows, Windows NT e determinate applicazioni

cla – classe Java

vbs – script Visual Basic®

vbe – estensione video BIOS

js, jse – testo sorgente JavaScript

htm – documento ipertestuale

htt – intestazione ipertesto di Microsoft Windows

hta – programma di ipertesto per Microsoft Internet Explorer®

asp – script Active Server Pages

chm – file HTML compilato

pht – file HTML integrato con script PHP

php – script incorporato in file HTML

wsh – file Microsoft Windows Script Host

wsf – script Microsoft Windows

the – sfondo del desktop di Microsoft Windows 95

hlp – file della Guida di Windows

msg – messaggio e-mail di Microsoft Mail

plg – messaggio di posta elettronica

mbx – messaggio e-mail di Microsoft Office Outlook salvato

doc* – documenti di Microsoft Office Word, quali doc per i documenti di Microsoft Office Word, docx per i documenti di Microsoft Office Word 2007 con supporto XML e docm per i documenti di Microsoft Office Word 2007 con supporto per le macro

dot* – modelli di documenti di Microsoft Office Word, quali dot per i modelli di documenti Microsoft Office Word, dotx per i modelli di documenti di Microsoft Office Word 2007, dotm per i modelli di documenti di Microsoft Office Word 2007 con supporto per le macro

fpm – programma di database, file di avvio di Microsoft Visual FoxPro

rtf – documento Rich Text Format

shs – frammento di Windows Shell Scrap Object Handler

dwg – database di disegni AutoCAD®

msi – pacchetto di Microsoft Windows Installer

otm – progetto VBA per Microsoft Office Outlook

pdf – documento di Adobe Acrobat

swf – oggetto pacchetto di Shockwave® Flash

jpg, jpeg – formato grafico compresso per immagini

emf – formato di file Enhanced Metafile;

ico – oggetto file icona

Ov? – file eseguibili di Microsoft Office Word

xl* – documenti e file di Microsoft Office Excel, quali xla (estensione di Microsoft Office Excel), xlc per i diagrammi, xlt per i modelli di documento, xlsx per le cartelle di lavoro di Microsoft Office Excel 2007, xltm per le cartelle di lavoro di Microsoft Office Excel 2007 con supporto per le macro, xlsb per le cartelle di lavoro di Microsoft Office Excel 2007 in formato binario (non XML), xltx per i modelli di Microsoft Office Excel 2007, xlsm per i modelli di Microsoft Office Excel 2007 con supporto per le macro, xlam per i plug-in di Microsoft Office Excel 2007 con supporto per le macro

pp* – documenti e file di Microsoft Office PowerPoint®, quali pps per le diapositive di Microsoft Office PowerPoint, ppt per le presentazioni, pptx per le presentazioni di Microsoft Office PowerPoint 2007, pptm per le presentazioni di Microsoft Office PowerPoint 2007 con supporto per le macro, potx per i modelli di presentazione di Microsoft Office PowerPoint 2007, potm per i modelli di presentazione di Microsoft Office PowerPoint 2007 con supporto per le macro, ppsx per le presentazioni di Microsoft Office PowerPoint 2007, ppsm per le presentazioni di Microsoft Office PowerPoint 2007 con supporto per le macro, ppam per i plug-in di Microsoft Office PowerPoint 2007 con supporto per le macro

md* – documenti e file di Microsoft Office Access®, quali mda per i gruppi di lavoro di Microsoft Office Access e mdb per i database

sldx – diapositiva di Microsoft PowerPoint 2007

sldm – diapositiva di Microsoft PowerPoint 2007 con supporto per le macro

thmx – tema di Microsoft Office 2007

Appendice 5. Impostazioni di rete per l'interazione con servizi esterni

Kaspersky Endpoint Security e Kaspersky Security Center utilizzano un canale di comunicazione criptato con TLS (Transport Layer Security) per il funzionamento con i servizi esterni di Kaspersky.

Kaspersky Endpoint Security utilizza le seguenti impostazioni di rete per interagire con i servizi esterni.

Indirizzo	Descrizione
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocollo: `HTTPS` Porta: `443`	Attivazione dell'applicazione.

Indirizzo	Descrizione

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protocollo: `HTTPS`
Porta: `443`
	Aggiornamento di database e moduli software dell'applicazione.

`downloads.upd.kaspersky.com` Protocollo: `HTTPS` Porta: `443`	• Aggiornamento di database e moduli software dell'applicazione. • Verifica dell'accesso ai server Kaspersky. Se non è possibile accedere ai server che utilizzano il DNS di sistema, l'applicazione utilizza il DNS pubblico. Ciò è necessario per assicurarsi che i database antivirus siano aggiornati e che il livello di protezione del computer sia mantenuto. Kaspersky Endpoint Security utilizza il seguente elenco di server DNS pubblici nel seguente ordine: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Le richieste emesse dall'applicazione possono contenere indirizzi di domini e l'indirizzo IP pubblico dell'utente, poiché l'applicazione stabilisce una connessione TCP/UDP con il server DNS. Queste informazioni sono necessarie, ad esempio, per convalidare il certificato di una risorsa Web quando si utilizza HTTPS. Se Kaspersky Endpoint Security utilizza un server DNS pubblico, l'elaborazione dei dati è disciplinata dall'informativa sulla privacy del servizio in questione. Se si desidera impedire a Kaspersky Endpoint Security di utilizzare un server DNS pubblico, contattare l'Assistenza tecnica per ottenere una patch privata.
`touch.kaspersky.com` Protocollo: `HTTP`	• Ricezione dell'ora attendibile per il controllo del periodo di validità del certificato (connessione TLS). • Avviso relativo al negato accesso a una risorsa Web nel browser quando Protezione minacce Web è in esecuzione.

Indirizzo	Descrizione

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protocollo: `HTTP`
Porta: `80`
	Aggiornamento di database e moduli software dell'applicazione.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protocollo: `HTTPS`
Porta: `443`
	Utilizzo di Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protocollo: `KSN`
Porta: `443`, `1443`
	Utilizzo di Kaspersky Security Network.

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Protocollo: `HTTPS`
Porta: `443`
	Seguire i collegamenti presenti nell'interfaccia.

Impostazioni, utilizzate per il criptaggio

Indirizzo	Descrizione

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocollo: `HTTP`
Porta: `80`
	PKI (Public Key Infrastructure).

Appendice 6. Eventi applicativi

Nel registro eventi di Kaspersky Security Center e nel registro degli eventi di Windows, vengono registrate informazioni sull'esecuzione di ciascun componente di Kaspersky Endpoint Security, sugli eventi di criptaggio dei dati, sul completamento di ogni attività di scansione malware, attività di aggiornamento e attività di Controllo integrità, nonché sull'esecuzione complessiva dell'applicazione.

Kaspersky Endpoint Security genera eventi dei seguenti tipi: eventi generali ed eventi specifici. Gli eventi specifici vengono creati solo da Kaspersky Endpoint Security for Windows. Agli eventi specifici è associato un ID semplice, ad esempio `000000cb`. Gli eventi specifici contengono i seguenti parametri obbligatori:

- `GNRL_EA_DESCRIPTION` è il contenuto dell'evento.
- `GNRL_EA_ID` è l'ID del servizio dell'evento.
- `GNRL_EA_SEVERITY` è lo stato dell'evento. `1` – *Informazioni*, `2` – *Avviso*, `3` – *Errore funzionale*, `4` – *Critico*.
- `EVENT_TYPE_DISPLAY_NAME` è il titolo dell'evento.
- `TASK_DISPLAY_NAME` è il nome del componente dell'applicazione che ha avviato l'evento.

Gli eventi generali possono essere creati da Kaspersky Endpoint Security for Windows e da altre applicazioni Kaspersky (ad esempio, Kaspersky Security for Windows Server). Agli eventi generali è associato un ID più complesso, ad esempio `GNRL_EV_VIRUS_FOUND`. Oltre alle impostazioni obbligatorie, gli eventi generali contengono le impostazioni avanzate.

Durata dell'archiviazione degli eventi nel server

Critico

La licenza è scaduta

Stato	!
Componente	Audit sistema
ID evento di Windows	201
ID evento di Kaspersky Security Center	GNRL_EV_LICENSE_EXPIRATION
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

La licenza è quasi scaduta

Stato	!
Componente	Audit sistema
ID evento di Windows	203
ID evento di Kaspersky Security Center	000000cb

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Database mancanti o danneggiati

Stato	⚠
Componente	Audit sistema
ID evento di Windows	206
ID evento di Kaspersky Security Center	000000ce
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

I database non sono aggiornati da molto tempo

Stato	⚠
Componente	Audit sistema
ID evento di Windows	207
ID evento di Kaspersky Security Center	000000cf
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'esecuzione automatica dell'applicazione è disabilitata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	209
ID evento di Kaspersky Security Center	000000d1
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di attivazione

Stato	⚠
Componente	Audit sistema
ID evento di Windows	229
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

È stata rilevata una minaccia attiva. Si consiglia di avviare Disinfezione avanzata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	231
ID evento di Kaspersky Security Center	000000e7

Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Server KSN non disponibili

Stato	⚠
Componente	Audit sistema
ID evento di Windows	2023
ID evento di Kaspersky Security Center	000007e7
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Spazio insufficiente nell'archivio Quarantena

Stato	⚠
Componente	Audit sistema
ID evento di Windows	343
ID evento di Kaspersky Security Center	00000157
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto non ripristinato dalla Quarantena

Stato	⚠
Componente	Audit sistema
ID evento di Windows	346
ID evento di Kaspersky Security Center	0000015a
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto non eliminato dalla Quarantena

Stato	⚠
Componente	Audit sistema
ID evento di Windows	348
ID evento di Kaspersky Security Center	0000015c
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'applicazione ha stabilito una connessione a un sito Web con un certificato non attendibile

Stato	⚠
Componente	Audit sistema
ID evento di Windows	57
ID evento di Kaspersky Security Center	00000039

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile verificare una connessione criptata. Il dominio è stato aggiunto all'elenco delle esclusioni

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	`60`
ID evento di Kaspersky Security Center	`0000003c`
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rilevato un oggetto dannoso (database locali)

Stato	ⓘ
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Prevenzione Intrusioni Host Rilevamento del Comportamento Anti-Cryptor Prevenzione Exploit Scansione malware
ID evento di Windows	`302`
ID evento di Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parametri dell'evento	• `GNRL_EA_PARAM_1` è l'hash dell'oggetto (SHA256). • `GNRL_EA_PARAM_2` è il nome dell'oggetto. Quando viene rilevato il criptaggio esterno delle cartelle condivise, l'applicazione mostra il percorso del file di destinazione. • `GNRL_EA_PARAM_5` è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio `EICAR-Test-File`. • `GNRL_EA_PARAM_7` è il nome dell'utente della sessione. • `GNRL_EA_PARAM_8` è il tipo di minaccia (`type`). • `GNRL_EA_PARAM_9` sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (`engine`). Tecnologie di rilevamento delle minacce (`method`). Minaccia rilevata da Kaspersky Private Security Network (`blacklist`): `true` o `false`. Versione EDR. Identificatore della minaccia in EDR. Hash MD5 dell'oggetto.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rilevato un oggetto dannoso (KSN)

Stato	⚠
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Prevenzione Intrusioni Host Rilevamento del Comportamento Anti-Cryptor Prevenzione Exploit Scansione malware
ID evento di Windows	`302`
ID evento di Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parametri dell'evento	• `GNRL_EA_PARAM_1` è l'hash dell'oggetto (SHA256). • `GNRL_EA_PARAM_2` è il nome dell'oggetto. • `GNRL_EA_PARAM_5` è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio `EICAR-Test-File`. • `GNRL_EA_PARAM_7` è il nome dell'utente della sessione. • `GNRL_EA_PARAM_8` è il tipo di minaccia (`type`). • `GNRL_EA_PARAM_9` sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (`engine`). Tecnologie di rilevamento delle minacce (`method`). Minaccia rilevata da Kaspersky Private Security Network (`blacklist`): `true` o `false`. Versione EDR. Identificatore della minaccia in EDR. Hash MD5 dell'oggetto.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Disinfezione impossibile

Stato	⚠
Componente	Protezione minacce file Protezione minacce di posta Prevenzione Intrusioni Host Rilevamento del Comportamento Anti-Cryptor Scansione malware
ID evento di Windows	`312`
ID evento di Kaspersky Security Center	`GNRL_EV_OBJECT_NOTCURED`
Parametri dell'evento	• `GNRL_EA_PARAM_1` è l'hash dell'oggetto (SHA256). • `GNRL_EA_PARAM_2` è il nome dell'oggetto. • `GNRL_EA_PARAM_5` è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio `EICAR-Test-File`. • `GNRL_EA_PARAM_7` è il nome dell'utente della sessione. • `GNRL_EA_PARAM_8` è il tipo di minaccia (`type`). • `GNRL_EA_PARAM_9` sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (`engine`). Tecnologie di rilevamento delle minacce (`method`). Minaccia rilevata da Kaspersky Private Security Network (`blacklist`): `true` o `false`. Versione EDR. Identificatore della minaccia in EDR. Hash MD5 dell'oggetto.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile eliminare

Stato	⚠
Componente	Protezione minacce file Prevenzione Intrusioni Host Rilevamento del Comportamento Anti-Cryptor Scansione malware
ID evento di Windows	313
ID evento di Kaspersky Security Center	00000139
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di elaborazione

Stato	⚠
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Prevenzione Intrusioni Host Protezione AMSI Scansione malware
ID evento di Windows	317
ID evento di Kaspersky Security Center	0000013d
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Processo terminato

Stato	⚠
Componente	Protezione minacce file Prevenzione Intrusioni Host Rilevamento del Comportamento Scansione malware
ID evento di Windows	452
ID evento di Kaspersky Security Center	000001c4
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile terminare il processo

Stato	⚠
Componente	Protezione minacce file Prevenzione Intrusioni Host Rilevamento del Comportamento Scansione malware
ID evento di Windows	453
ID evento di Kaspersky Security Center	000001c5
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Collegamento pericoloso bloccato

Stato	ⓘ
Componente	Protezione minacce Web
ID evento di Windows	362
ID evento di Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Parametri dell'evento	• GNRL_EA_PARAM_2 è il percorso dell'oggetto. • GNRL_EA_PARAM_5 è il nome dell'oggetto secondo la classificazione di Kaspersky. • GNRL_EA_PARAM_7 è il nome dell'utente della sessione. • GNRL_EA_PARAM_8 è il tipo di minaccia (type). • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (engine). Tecnologie di rilevamento delle minacce (method). Minaccia rilevata da KSN Privato (blacklist): true o false.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Collegamento pericoloso aperto

Stato	ⓘ
Componente	Protezione minacce Web
ID evento di Windows	363
ID evento di Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Parametri dell'evento	• GNRL_EA_PARAM_2 è il percorso dell'oggetto. • GNRL_EA_PARAM_5 è il nome dell'oggetto secondo la classificazione di Kaspersky. • GNRL_EA_PARAM_7 è il nome dell'utente della sessione. • GNRL_EA_PARAM_8 è il tipo di minaccia (type). • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (engine). Tecnologie di rilevamento delle minacce (method). Minaccia rilevata da KSN Privato (blacklist): true o false.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rilevato collegamento pericoloso aperto in precedenza

Stato	ⓘ
Componente	Protezione minacce Web
ID evento di Windows	1201
ID evento di Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
Parametri dell'evento	• GNRL_EA_PARAM_2 è il percorso dell'oggetto. • GNRL_EA_PARAM_5 è il nome dell'oggetto secondo la classificazione di Kaspersky. • GNRL_EA_PARAM_7 è il nome dell'utente della sessione. • GNRL_EA_PARAM_8 è il tipo di minaccia (type). • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (engine). Tecnologie di rilevamento delle minacce (method). Minaccia rilevata da KSN Privato (blacklist): true o false.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Azione del processo bloccata

Stato	⚠
Componente	Controllo adattivo delle anomalie
ID evento di Windows	`2200`
ID evento di Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Parametri dell'evento	• `GNRL_EA_PARAM_1` è il nome della regola di Controllo adattivo delle anomalie. • `GNRL_EA_PARAM_2` è l'ID della regola euristica. • `GNRL_EA_PARAM_3` è il nome dell'utente della sessione. • `GNRL_EA_PARAM_4` è il processo di origine. • `GNRL_EA_PARAM_5` è l'oggetto di origine. • `GNRL_EA_PARAM_6` è il processo di destinazione. • `GNRL_EA_PARAM_7` è l'oggetto di destinazione. • `GNRL_EA_PARAM_8` sono informazioni aggiuntive sull'oggetto rilevato: Checksum del processo di origine/oggetto e processo di destinazione/oggetto. Processo bloccato (`verdict_type`): `true` o `false`. ID sicurezza utente (SID).
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Tastiera non autorizzata

Stato	⚠
Componente	Prevenzione Attacchi BadUSB
ID evento di Windows	`2051`
ID evento di Kaspersky Security Center	`00000803`
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

La richiesta AMSI è stata bloccata

Stato	⚠
Componente	Protezione AMSI
ID evento di Windows	`2200`
ID evento di Kaspersky Security Center	`00000898`
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Attività di rete bloccata

Stato	⚠
Componente	Firewall
ID evento di Windows	`602`
ID evento di Kaspersky Security Center	`00000329`
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Attacco di rete rilevato

Stato	!
Componente	Protezione minacce di rete
ID evento di Windows	651
ID evento di Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
Parametri dell'evento	• GNRL_EA_PARAM_1 è il nome dell'attacco. • GNRL_EA_PARAM_2 è il protocollo. • GNRL_EA_PARAM_3 è l'indirizzo IP del computer che funge da origine dell'attacco di rete. L'indirizzo IP è indicato nell'ordine di byte dell'host. Ad esempio, 2886729929 per 172.16.0.201. • GNRL_EA_PARAM_4 è il numero della porta. • GNRL_EA_PARAM_5 è un indirizzo IPv6, ad esempio 12B012B012B012B012B012B012B012B0. • GNRL_EA_PARAM_6 è l'indirizzo IP del computer obiettivo dell'attacco di rete. L'indirizzo IP è indicato nell'ordine di byte dell'host. Ad esempio, 2886729929 per 172.16.0.201.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avvio dell'applicazione non consentito

Stato	!
Componente	Controllo applicazioni
ID evento di Windows	702
ID evento di Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCH_DENIED
Parametri dell'evento	• GNRL_EA_PARAM_2 è il nome dell'utente della sessione. • GNRL_EA_PARAM_3 è l'identificatore della categoria creata manualmente. • GNRL_EA_PARAM_4 è l'ID della categoria dell'applicazione. • GNRL_EA_PARAM_5 si riferisce alle informazioni sulla firma digitale dell'applicazione. • GNRL_EA_PARAM_6 è il nome del file eseguibile dell'applicazione (ad esempio, chrome.exe). • GNRL_EA_PARAM_7 è il percorso del file eseguibile. • GNRL_EA_PARAM_8 è l'hash dell'oggetto (SHA256). • GNRL_EA_PARAM_9 è la versione dell'applicazione che l'utente tenta di eseguire.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Processo non consentito avviato prima dell'avvio di Kaspersky Endpoint Security

Stato	!
Componente	Controllo applicazioni
ID evento di Windows	710
ID evento di Kaspersky Security Center	000002c6
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Accesso negato (database locali)

Stato	!
Componente	Controllo Web

ID evento di Windows	752
ID evento di Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'URL. • GNRL_EA_PARAM_2 è il nome dell'utente della sessione. • GNRL_EA_PARAM_3 è il nome della regola di Controllo Web.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Accesso negato (KSN)

Stato	ⓘ
Componente	Controllo Web
ID evento di Windows	752
ID evento di Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'URL. • GNRL_EA_PARAM_2 è il nome dell'utente della sessione. • GNRL_EA_PARAM_3 è il nome della regola di Controllo Web.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Operazione con il dispositivo non consentita

Stato	ⓘ
Componente	Controllo dispositivi
ID evento di Windows	802
ID evento di Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'ID hardware (HWID). • GNRL_EA_PARAM_2 è il nome dell'utente della sessione.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione di rete bloccata

Stato	ⓘ
Componente	Controllo dispositivi
ID evento di Windows	809
ID evento di Kaspersky Security Center	00000329
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'utilizzo del dispositivo è vietato fino all'avvio di Kaspersky Endpoint Security

Stato	ⓘ
Componente	Controllo dispositivi
ID evento di Windows	816
ID evento di Kaspersky Security Center	00000330

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

La connessione del dispositivo è vietata fino all'avvio di Kaspersky Endpoint Security

Stato	ⓘ
Componente	Controllo dispositivi
ID evento di Windows	817
ID evento di Kaspersky Security Center	00000331
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di aggiornamento del componente

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1011
ID evento di Kaspersky Security Center	000003f3
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di distribuzione degli aggiornamenti dei componenti

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1012
ID evento di Kaspersky Security Center	000003f4
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Errore di aggiornamento locale

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1014
ID evento di Kaspersky Security Center	000003f6
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Errore di aggiornamento in rete

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1015
ID evento di Kaspersky Security Center	000003f7

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Impossibile avviare due attività contemporaneamente

Stato	⚠
Componente	Aggiornamento
ID evento di Windows	1017
ID evento di Kaspersky Security Center	000003f9
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore durante la verifica dei database e dei moduli dell'applicazione

Stato	⚠
Componente	Aggiornamento
ID evento di Windows	1018
ID evento di Kaspersky Security Center	000003fa
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore durante l'interazione con Kaspersky Security Center

Stato	⚠
Componente	Aggiornamento
ID evento di Windows	1019
ID evento di Kaspersky Security Center	000003fb
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Non tutti i componenti sono stati aggiornati

Stato	⚠
Componente	Aggiornamento
ID evento di Windows	1021
ID evento di Kaspersky Security Center	000003fd
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Aggiornamento completato correttamente, distribuzione aggiornamenti non riuscita

Stato	⚠
Componente	Aggiornamento
ID evento di Windows	1023
ID evento di Kaspersky Security Center	000003ff

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Errore interno dell'attività

Stato	⊗
Componente	Audit sistema
ID evento di Windows	101
ID evento di Kaspersky Security Center	00000065
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Installazione patch non riuscita

Stato	⊗
Componente	Aggiornamento
ID evento di Windows	2153
ID evento di Kaspersky Security Center	00000869
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rollback della patch non riuscito

Stato	⊗
Componente	Aggiornamento
ID evento di Windows	2156
ID evento di Kaspersky Security Center	0000086c
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore durante l'applicazione delle regole di criptaggio/decriptaggio dei file

Stato	⊗
Componente	Criptaggio dei dati
ID evento di Windows	904
ID evento di Kaspersky Security Center	00000388
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di criptaggio/decriptaggio dei file

Stato	⊗
Componente	Criptaggio dei dati
ID evento di Windows	912

ID evento di Kaspersky Security Center	GNRL_EV_ENCRYPTION_ERROR
Parametri dell'evento	• GNRL_EA_PARAM_1 è il percorso del file. • GNRL_EA_PARAM_2 è la causa dell'errore. • GNRL_EA_PARAM_3 è il tipo di dispositivo.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Accesso al file bloccato

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	940
ID evento di Kaspersky Security Center	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'oggetto di destinazione. • GNRL_EA_PARAM_2 è il nome dell'utente della sessione. • GNRL_EA_PARAM_3 è il nome del file eseguibile dell'applicazione, ad esempio Chrome.exe, che tenta di accedere al file.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Errore durante l'abilitazione della modalità portatile

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	951
ID evento di Kaspersky Security Center	000003b7
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore durante la disabilitazione della modalità portatile

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	953
ID evento di Kaspersky Security Center	000003b9
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore durante la creazione del pacchetto criptato

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	931
ID evento di Kaspersky Security Center	000003a3
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore durante il criptaggio/decriptaggio del dispositivo

Stato	⊗
Componente	Criptaggio dei dati
ID evento di Windows	1305
ID evento di Kaspersky Security Center	00000519
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile caricare il modulo di criptaggio

Stato	⊗
Componente	Criptaggio dei dati
ID evento di Windows	1311
ID evento di Kaspersky Security Center	0000051f
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'attività per la gestione degli account per l'Agente di Autenticazione si è conclusa con un errore

Stato	⊗
Componente	Criptaggio dei dati
ID evento di Windows	1340
ID evento di Kaspersky Security Center	0000053c
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il criterio non può essere applicato

Stato	⊗
Componente	Audit sistema
ID evento di Windows	1312
ID evento di Kaspersky Security Center	00000520
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Upgrade FDE non riuscito

Stato	⊗
Componente	Criptaggio dei dati
ID evento di Windows	1342
ID evento di Kaspersky Security Center	0000053e
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rollback dell'upgrade FDE non riuscito (per informazioni, vedere la Guida in linea di Kaspersky Endpoint Security for Windows)

Stato	⚠
Componente	Criptaggio dei dati
ID evento di Windows	1344
ID evento di Kaspersky Security Center	00000540
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Server Kaspersky Anti Targeted Attack Platform non disponibile

Stato	⚠
Componente	Sensore Endpoint
ID evento di Windows	2100
ID evento di Kaspersky Security Center	00000834
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile eliminare l'oggetto

Stato	⚠
Componente	Sandbox
ID evento di Windows	2252
ID evento di Kaspersky Security Center	000008cc
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto non inserito in Quarantena (Sandbox)

Stato	⚠
Componente	Sandbox
ID evento di Windows	2603
ID evento di Kaspersky Security Center	00000a2b
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Si è verificato un errore interno

Stato	⚠
Componente	Sandbox
ID evento di Windows	2607
ID evento di Kaspersky Security Center	00000a2f
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato server Sandbox non valido

Stato	!
Componente	Sandbox
ID evento di Windows	2613
ID evento di Kaspersky Security Center	00000a35
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il nodo Sandbox non è disponibile

Stato	!
Componente	Sandbox
ID evento di Windows	2614
ID evento di Kaspersky Security Center	00000a36
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile elaborare un oggetto in Sandbox

Stato	!
Componente	Sandbox
ID evento di Windows	2617
ID evento di Kaspersky Security Center	00000a39
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Carico massimo su Sandbox superato

Stato	!
Componente	Sandbox
ID evento di Windows	2618
ID evento di Kaspersky Security Center	00000a3a
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Rilevato oggetto IOC

Stato	!
Componente	Endpoint Detection and Response
ID evento di Windows	2651
ID evento di Kaspersky Security Center	00000a5b
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Verifica della licenza di Sandbox non riuscita

Stato	⚠
Componente	Sandbox
ID evento di Windows	2620
ID evento di Kaspersky Security Center	00000a3c
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile inviare l'attività di scansione a Sandbox in base a un utente

Stato	⚠
Componente	Sandbox
ID evento di Windows	2623
ID evento di Kaspersky Security Center	00000a3e
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore durante la creazione dell'attività Sandbox

Stato	⚠
Componente	Sandbox
ID evento di Windows	2621
ID evento di Kaspersky Security Center	00000a3d
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avvio dell'oggetto bloccato

Stato	⚠
Componente	Endpoint Detection and Response
ID evento di Windows	2553
ID evento di Kaspersky Security Center	000009f9
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avvio del processo bloccato

Stato	⚠
Componente	Endpoint Detection and Response
ID evento di Windows	2551
ID evento di Kaspersky Security Center	000009f7
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Esecuzione script bloccata

Stato	ⓘ
Componente	Endpoint Detection and Response
ID evento di Windows	2559
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto non inserito in Quarantena (Endpoint Detection and Response)

Stato	ⓘ
Componente	Endpoint Detection and Response
ID evento di Windows	2556
ID evento di Kaspersky Security Center	000009fc
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avvio del processo non bloccato

Stato	ⓘ
Componente	Endpoint Detection and Response
ID evento di Windows	2561
ID evento di Kaspersky Security Center	00000a01
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'oggetto non è bloccato

Stato	ⓘ
Componente	Endpoint Detection and Response
ID evento di Windows	2562
ID evento di Kaspersky Security Center	00000a02
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Esecuzione script non bloccata

Stato	ⓘ
Componente	Endpoint Detection and Response
ID evento di Windows	2563
ID evento di Kaspersky Security Center	00000a03
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore durante la modifica dei componenti dell'applicazione

Stato	⚠
Componente	Audit sistema
ID evento di Windows	1401
ID evento di Kaspersky Security Center	00000579
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Sono stati rilevati schemi di un possibile attacco di forza bruta nel sistema

Stato	⚠
Componente	Log Inspection
ID evento di Windows	2800
ID evento di Kaspersky Security Center	00000af0
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Sono stati rilevati schemi di un possibile abuso del Registro eventi di Windows

Stato	⚠
Componente	Log Inspection
ID evento di Windows	2801
ID evento di Kaspersky Security Center	00000af1
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rilevate azioni atipiche per conto di un nuovo servizio installato

Stato	⚠
Componente	Log Inspection
ID evento di Windows	2802
ID evento di Kaspersky Security Center	00000af2
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rilevato un accesso atipico che utilizza credenziali esplicite

Stato	⚠
Componente	Log Inspection
ID evento di Windows	2803
ID evento di Kaspersky Security Center	00000af3
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Sono stati rilevati schemi di un possibile attacco PAC falsificato con Kerberos (MS14-068) nel sistema

Stato	ⓘ
Componente	Log Inspection
ID evento di Windows	2804
ID evento di Kaspersky Security Center	00000af4
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rilevate modifiche sospette nel gruppo Amministratori integrato con privilegi

Stato	ⓘ
Componente	Log Inspection
ID evento di Windows	2805
ID evento di Kaspersky Security Center	00000af5
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Sono state rilevate attività atipiche durante una sessione di accesso alla rete

Stato	ⓘ
Componente	Log Inspection
ID evento di Windows	2806
ID evento di Kaspersky Security Center	00000af6
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Regola Log Inspection attivata

Stato	ⓘ
Componente	Log Inspection
ID evento di Windows	2807
ID evento di Kaspersky Security Center	00000af7
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Si sta verificando un evento atipico con una certa frequenza. Aggregazione degli eventi avviata

Stato	ⓘ
Componente	Log Inspection
ID evento di Windows	2808
ID evento di Kaspersky Security Center	00000af8
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rapporto su un evento atipico per il periodo di aggregazione

Stato	ⓘ
Componente	Log Inspection
ID evento di Windows	2809
ID evento di Kaspersky Security Center	00000af9
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di connessione al server di EDR Expert

Stato	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID evento di Windows	2850
ID evento di Kaspersky Security Center	00000b22
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido del server di EDR Expert

Stato	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID evento di Windows	2851
ID evento di Kaspersky Security Center	00000b23
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido dell'agente sul server di EDR Expert

Stato	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID evento di Windows	2852
ID evento di Kaspersky Security Center	00000b24
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di connessione al server di risposta di EDR Expert

Stato	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID evento di Windows	2858
ID evento di Kaspersky Security Center	00000b22
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido del server di risposta di EDR Expert

Stato	⊗
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID evento di Windows	2859
ID evento di Kaspersky Security Center	00000b23
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido dell'agente sul server di risposta di EDR Expert

Stato	⊗
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID evento di Windows	2860
ID evento di Kaspersky Security Center	00000b24
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di connessione al server di raccolta della telemetria di EDR Expert

Stato	⊗
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID evento di Windows	2854
ID evento di Kaspersky Security Center	00000b22
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido del server di raccolta della telemetria di EDR Expert

Stato	⊗
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID evento di Windows	2855
ID evento di Kaspersky Security Center	00000b23
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido dell'agente sul server di raccolta della telemetria di EDR Expert

Stato	⊗
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID evento di Windows	2856
ID evento di Kaspersky Security Center	00000b24

Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di connessione al server NDR

Stato	⊗
Componente	Network Detection and Response (KATA)
ID evento di Windows	3080
ID evento di Kaspersky Security Center	00000c08
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido del server NDR

Stato	⊗
Componente	Network Detection and Response (KATA)
ID evento di Windows	3081
ID evento di Kaspersky Security Center	00000c09
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido dell'agente sul server NDR

Stato	⊗
Componente	Network Detection and Response (KATA)
ID evento di Windows	3082
ID evento di Kaspersky Security Center	00000c0a
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il dispositivo è connesso a un Administration Server non attendibile. Contattare l'amministratore

Stato	⊗
Componente	Protezione della connessione ad Administration Server
ID evento di Windows	3301
ID evento di Kaspersky Security Center	00000ce5
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

È stata rilevata la modifica di un file o di una cartella

Stato	ⓘ / ⚠ / ⊗
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2950
ID evento di Kaspersky Security Center	00000b86
Registro eventi di Windows (predefinito)	–

Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

L'oggetto cambia troppo spesso. Aggregazione degli eventi avviata

Stato	ⓘ / ⚠ / ⓔ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2955
ID evento di Kaspersky Security Center	00000b8b
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rapporto sulla modifica degli oggetti per il periodo di aggregazione

Stato	ⓔ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2953
ID evento di Kaspersky Security Center	00000b89
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Stato	ⓘ / ⚠ / ⓔ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2956
ID evento di Kaspersky Security Center	00000b8c
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

È stata rilevata la modifica del Registro di sistema

Stato	ⓘ / ⚠ / ⓔ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2951
ID evento di Kaspersky Security Center	00000b87
Registro eventi di Windows (predefinito)	–

Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

È stata rilevata la connessione/disconnessione del dispositivo

Stato	ⓘ / ⚠ / ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2952
ID evento di Kaspersky Security Center	00000b88
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

L'ambito del monitoraggio include oggetti errati

Stato	ⓘ / ⚠ / ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2903
ID evento di Kaspersky Security Center	00000b89
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

Troppi tentativi di eseguire le operazioni limitate con l'oggetto. Aggregazione degli eventi avviata

Stato	ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2963
ID evento di Kaspersky Security Center	00000b93
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Un'operazione con i file dell'ambito del monitoraggio è stata bloccata

Stato	ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2959
ID evento di Kaspersky Security Center	00000b8f

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

Modifica del Registro di sistema bloccata

Stato	ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2960
ID evento di Kaspersky Security Center	00000b90
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

Errore di elaborazione

Stato	ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2954
ID evento di Kaspersky Security Center	00000b8a
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Monitoraggio integrità di sistema: attivazione delle regole disabilitata per gli account utente senza corrispondenza dell'identificativo di sicurezza (SID)

Stato	ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2964
ID evento di Kaspersky Security Center	00000b94
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Controllo applicazioni: attivazione delle regole disabilitata per gli account utente senza corrispondenza dell'identificativo di sicurezza (SID)

Stato	ⓘ
Componente	Controllo applicazioni
ID evento di Windows	711
ID evento di Kaspersky Security Center	000002c7

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Controllo dispositivi: attivazione delle regole disabilitata per gli account utente senza corrispondenza dell'identificativo di sicurezza (SID)

Stato	⚠
Componente	Controllo dispositivi
ID evento di Windows	810
ID evento di Kaspersky Security Center	0000032a
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Controllo Web: attivazione delle regole disabilitata per gli account utente senza corrispondenza dell'identificativo di sicurezza (SID)

Stato	⚠
Componente	Controllo Web
ID evento di Windows	757
ID evento di Kaspersky Security Center	000002f5
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Controllo adattivo delle anomalie: attivazione delle regole disabilitata per gli account utente senza corrispondenza dell'identificativo di sicurezza (SID)

Stato	⚠
Componente	Controllo adattivo delle anomalie
ID evento di Windows	504
ID evento di Kaspersky Security Center	000001f8
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Log Inspection: attivazione delle regole disabilitata per gli account utente senza corrispondenza dell'identificativo di sicurezza (SID)

Stato	⚠
Componente	Log Inspection
ID evento di Windows	2810
ID evento di Kaspersky Security Center	00000afa
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

SVM non disponibile

Stato	⚠
Componente	Light Agent

ID evento di Windows	3151
ID evento di Kaspersky Security Center	00000c4f
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto dannoso rilevato. È necessario avviare la disinfezione avanzata su un modello di macchina virtuale

Stato	ⓘ
Componente	Light Agent
ID evento di Windows	3182
ID evento di Kaspersky Security Center	00000c6e
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

La connessione di rete stabilita tramite il protocollo obsoleto è stata bloccata

Stato	ⓘ
Componente	Protezione
ID evento di Windows	75
ID evento di Kaspersky Security Center	0000004b
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di connessione al server KUMA

Stato	ⓘ
Componente	Integrazione KUMA
ID evento di Windows	2854
ID evento di Kaspersky Security Center	00000b26
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido del server KUMA

Stato	ⓘ
Componente	Integrazione KUMA
ID evento di Windows	2855
ID evento di Kaspersky Security Center	00000b27
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido dell'agente sul server KUMA

Stato	ⓘ
Componente	Integrazione KUMA

ID evento di Windows	2856
ID evento di Kaspersky Security Center	00000b28
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di connessione al server SIEM

Stato	⚠
Componente	Integrazione KUMA
ID evento di Windows	3250
ID evento di Kaspersky Security Center	00000cb2
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido del server SIEM

Stato	⚠
Componente	Integrazione KUMA
ID evento di Windows	3251
ID evento di Kaspersky Security Center	00000cb3
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Certificato non valido dell'agente sul server SIEM

Stato	⚠
Componente	Integrazione KUMA
ID evento di Windows	3252
ID evento di Kaspersky Security Center	00000cb4
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore funzionale

Impossibile eseguire l'attività

Stato	⚠
Componente	Audit sistema
ID evento di Windows	212
ID evento di Kaspersky Security Center	000000d4
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impostazioni attività non valide. Impostazioni non applicate

Stato	⊗
Componente	Audit sistema
ID evento di Windows	707
ID evento di Kaspersky Security Center	000002c3
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avviso

Arresto anomalo dell'applicazione durante la sessione precedente

Stato	⚠
Componente	Audit sistema
ID evento di Windows	237
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

La licenza sta per scadere

Stato	⚠
Componente	Audit sistema
ID evento di Windows	204
ID evento di Kaspersky Security Center	000000cc
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

I database non sono aggiornati

Stato	⚠
Componente	Audit sistema
ID evento di Windows	208
ID evento di Kaspersky Security Center	000000d0
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Gli aggiornamenti automatici sono disabilitati

Stato	⚠
Componente	Audit sistema
ID evento di Windows	210
ID evento di Kaspersky Security Center	000000d2

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'Auto-difesa è disabilitata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	211
ID evento di Kaspersky Security Center	000000d3
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

I componenti della protezione sono disabilitati

Stato	⚠
Componente	Audit sistema
ID evento di Windows	214
ID evento di Kaspersky Security Center	000000d6
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il computer è in esecuzione in modalità provvisoria

Stato	⚠
Componente	Audit sistema
ID evento di Windows	215
ID evento di Kaspersky Security Center	000000d7
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Sono presenti file non elaborati

Stato	⚠
Componente	Audit sistema
ID evento di Windows	216
ID evento di Kaspersky Security Center	000000d8
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Criterio di gruppo applicato

Stato	⚠
Componente	Audit sistema
ID evento di Windows	219
ID evento di Kaspersky Security Center	000000db

Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Attività interrotta

Stato	⚠
Componente	Audit sistema
ID evento di Windows	222
ID evento di Kaspersky Security Center	000000de
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Chiudere e riaprire l'applicazione per completare l'aggiornamento

Stato	⚠
Componente	Audit sistema
ID evento di Windows	224
ID evento di Kaspersky Security Center	0000057b
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

È necessario riavviare il computer

Stato	⚠
Componente	Audit sistema
ID evento di Windows	225
ID evento di Kaspersky Security Center	000000e1
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

La licenza consente l'utilizzo di componenti che non sono stati installati

Stato	⚠
Componente	Audit sistema
ID evento di Windows	226
ID evento di Kaspersky Security Center	000000e2
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Disinfezione avanzata avviata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	232
ID evento di Kaspersky Security Center	000000e8

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Disinfezione avanzata completata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	233
ID evento di Kaspersky Security Center	000000e9
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Chiave di riserva errata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	230
ID evento di Kaspersky Security Center	000000e6
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'abbonamento scadrà a breve

Stato	⚠
Componente	Audit sistema
ID evento di Windows	240
ID evento di Kaspersky Security Center	000000f0
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Bloccato

Stato	⚠
Componente	Rilevamento del Comportamento Anti-Cryptor Prevenzione Exploit Protezione minacce Web
ID evento di Windows	331

ID evento di Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'hash dell'oggetto (SHA256). • GNRL_EA_PARAM_2 è il nome dell'oggetto. Quando viene rilevato il criptaggio esterno delle cartelle condivise, l'applicazione mostra il percorso del file di destinazione. • GNRL_EA_PARAM_5 è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio EICAR-Test-File. • GNRL_EA_PARAM_7 è il nome dell'utente della sessione. • GNRL_EA_PARAM_8 è il tipo di minaccia (type). • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (engine). Tecnologie di rilevamento delle minacce (method). Minaccia rilevata da Kaspersky Private Security Network (blacklist): true o false. Versione EDR. Identificatore della minaccia in EDR. Hash MD5 dell'oggetto.
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Le impostazioni del sistema operativo non consentono di controllare l'accesso alle reti Wi-Fi

Stato	⚠
Componente	Controllo dispositivi
ID evento di Windows	249
ID evento di Kaspersky Security Center	000000f9
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Oggetto non ripristinato dal backup

Stato	⚠
Componente	Audit sistema
ID evento di Windows	336
ID evento di Kaspersky Security Center	00000150
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Rilevata attività di rete sospetta

Stato	⚠
Componente	Audit sistema
ID evento di Windows	2001
ID evento di Kaspersky Security Center	000007d1
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione criptata terminata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	250
ID evento di Kaspersky Security Center	000007d3
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Partecipazione a KSN disabilitata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	2021
ID evento di Kaspersky Security Center	000007e5
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'elaborazione di alcune funzioni del sistema operativo è disabilitata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	245
ID evento di Kaspersky Security Center	000000f5
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Spazio nell'archivio Quarantena quasi esaurito

Stato	⚠
Componente	Audit sistema
ID evento di Windows	344
ID evento di Kaspersky Security Center	00000158
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione di rete bloccata

Stato	⚠
Componente	Audit sistema
ID evento di Windows	809
ID evento di Kaspersky Security Center	00000abe
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile creare una copia di backup

Stato	⚠
Componente	Protezione minacce file Rilevamento del Comportamento Anti-Cryptor Prevenzione Intrusioni Host Scansione malware
ID evento di Windows	310
ID evento di Kaspersky Security Center	00000136
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto non elaborato

Stato	⚠
Componente	Protezione minacce file Protezione minacce di posta Prevenzione Intrusioni Host Protezione AMSI Scansione malware
ID evento di Windows	314
ID evento di Kaspersky Security Center	0000013a
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto criptato

Stato	⚠
Componente	Prevenzione Intrusioni Host
ID evento di Windows	320
ID evento di Kaspersky Security Center	00000140
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Oggetto danneggiato

Stato	⚠
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Prevenzione Intrusioni Host Scansione malware
ID evento di Windows	321
ID evento di Kaspersky Security Center	00000141
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

È stato rilevato software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali (basi locali)

Stato	⚠
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Prevenzione Intrusioni Host Protezione AMSI Rilevamento del Comportamento Anti-Cryptor Anti-Cryptor Scansione malware
ID evento di Windows	`303`
ID evento di Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parametri dell'evento	• `GNRL_EA_PARAM_1` è l'hash dell'oggetto (SHA256). • `GNRL_EA_PARAM_2` è il nome dell'oggetto. • `GNRL_EA_PARAM_5` è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio `EICAR-Test-File`. • `GNRL_EA_PARAM_7` è il nome dell'utente della sessione. • `GNRL_EA_PARAM_8` è il tipo di minaccia (`type`).
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

È stato rilevato software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali (KSN)

Stato	⚠
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Prevenzione Intrusioni Host Protezione AMSI Rilevamento del Comportamento Anti-Cryptor Anti-Cryptor Scansione malware
ID evento di Windows	`303`
ID evento di Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parametri dell'evento	• `GNRL_EA_PARAM_1` è l'hash dell'oggetto (SHA256). • `GNRL_EA_PARAM_2` è il nome dell'oggetto. • `GNRL_EA_PARAM_5` è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio `EICAR-Test-File`. • `GNRL_EA_PARAM_7` è il nome dell'utente della sessione. • `GNRL_EA_PARAM_8` è il tipo di minaccia (`type`).
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto eliminato

Stato	⚠
Componente	Protezione minacce file Protezione minacce di posta Prevenzione Intrusioni Host Prevenzione Exploit Rilevamento del Comportamento Anti-Cryptor Scansione malware

ID evento di Windows	307
ID evento di Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'hash dell'oggetto (SHA256). • GNRL_EA_PARAM_2 è il nome dell'oggetto. • GNRL_EA_PARAM_5 è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio EICAR-Test-File. • GNRL_EA_PARAM_7 è il nome dell'utente della sessione. • GNRL_EA_PARAM_8 è il tipo di minaccia (type). • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (engine). Tecnologie di rilevamento delle minacce (method). Minaccia rilevata da Kaspersky Private Security Network (blacklist): true o false. Versione EDR. Identificatore della minaccia in EDR. Hash MD5 dell'oggetto.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto disinfettato

Stato	⚠
Componente	Protezione minacce file Protezione minacce di posta Prevenzione Intrusioni Host Scansione malware
ID evento di Windows	306
ID evento di Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'hash dell'oggetto (SHA256). • GNRL_EA_PARAM_2 è il nome dell'oggetto. • GNRL_EA_PARAM_5 è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio EICAR-Test-File. • GNRL_EA_PARAM_7 è il nome dell'utente della sessione. • GNRL_EA_PARAM_8 è il tipo di minaccia (type). • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (engine). Tecnologie di rilevamento delle minacce (method). Minaccia rilevata da Kaspersky Private Security Network (blacklist): true o false. Versione EDR. Identificatore della minaccia in EDR. Hash MD5 dell'oggetto.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto da disinfettare al riavvio

Stato	⚠
Componente	Prevenzione Intrusioni Host Protezione minacce file Scansione malware
ID evento di Windows	324
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Oggetto da eliminare al riavvio

Stato	⚠
Componente	Rilevamento del Comportamento Anti-Cryptor Prevenzione Exploit Prevenzione Intrusioni Host Protezione minacce file Scansione malware
ID evento di Windows	323
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Oggetto eliminato in base alle impostazioni

Stato	⚠
Componente	Protezione minacce di posta
ID evento di Windows	342
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Rollback completato

Stato	⚠
Componente	Protezione minacce file Rilevamento del Comportamento Anti-Cryptor Prevenzione Exploit Scansione malware
ID evento di Windows	455
ID evento di Kaspersky Security Center	000001c7
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore durante la rimozione della versione precedente dell'applicazione

Stato	⚠
Componente	Audit sistema
ID evento di Windows	246
ID evento di Kaspersky Security Center	000000f6
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Download dell'oggetto bloccato

Stato	⚠
Componente	Protezione minacce Web

ID evento di Windows	341
ID evento di Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'hash dell'oggetto (SHA256). • GNRL_EA_PARAM_2 è il nome dell'oggetto. • GNRL_EA_PARAM_5 è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio EICAR-Test-File. • GNRL_EA_PARAM_7 è il nome dell'utente della sessione. • GNRL_EA_PARAM_8 è il tipo di minaccia (type). • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (engine). Tecnologie di rilevamento delle minacce (method). Minaccia rilevata da Kaspersky Private Security Network (blacklist): true o false. Versione EDR. Identificatore della minaccia in EDR. Hash MD5 dell'oggetto.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Errore di autorizzazione tastiera

Stato	⚠
Componente	Prevenzione Attacchi BadUSB
ID evento di Windows	2052
ID evento di Kaspersky Security Center	00000804
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il risultato della scansione dell'oggetto è stato inviato a un'applicazione di terze parti

Stato	⚠
Componente	Protezione AMSI
ID evento di Windows	1512
ID evento di Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'hash dell'oggetto (SHA256). • GNRL_EA_PARAM_2 è il nome dell'oggetto. • GNRL_EA_PARAM_5 è il nome della minaccia in conformità con la classificazione di Kaspersky, ad esempio EICAR-Test-File. • GNRL_EA_PARAM_7 è il nome dell'utente della sessione. • GNRL_EA_PARAM_8 è il tipo di minaccia (type). • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (engine). Tecnologie di rilevamento delle minacce (method). Minaccia rilevata da Kaspersky Private Security Network (blacklist): true o false. Versione EDR. Identificatore della minaccia in EDR. Hash MD5 dell'oggetto.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Applicazione delle impostazioni dell'attività completata

Stato	⚠
Componente	Controllo applicazioni

ID evento di Windows	708
ID evento di Kaspersky Security Center	000002c4
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avviso su contenuti indesiderati (database locali)

Stato	⚠
Componente	Controllo Web
ID evento di Windows	708
ID evento di Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'URL. • GNRL_EA_PARAM_2 è il nome dell'utente della sessione. • GNRL_EA_PARAM_3 è il nome della regola di Controllo Web.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avviso su contenuti indesiderati (KSN)

Stato	⚠
Componente	Controllo Web
ID evento di Windows	708
ID evento di Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'URL. • GNRL_EA_PARAM_2 è il nome dell'utente della sessione. • GNRL_EA_PARAM_3 è il nome della regola di Controllo Web.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Accesso ai contenuti indesiderati eseguito dopo un avviso

Stato	⚠
Componente	Controllo Web
ID evento di Windows	754
ID evento di Kaspersky Security Center	000002f2
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Accesso temporaneo al dispositivo attivato

Stato	⚠
Componente	Controllo dispositivi
ID evento di Windows	803
ID evento di Kaspersky Security Center	000002f2
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Operazione annullata dall'utente

Stato	⚠
Componente	Aggiornamento
ID evento di Windows	1016
ID evento di Kaspersky Security Center	000003f8
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'utente ha scelto di non applicare il criterio di criptaggio

Stato	⚠
Componente	Criptaggio dei dati
ID evento di Windows	1306
ID evento di Kaspersky Security Center	0000051a
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Applicazione delle regole di criptaggio/decriptaggio dei file interrotta

Stato	⚠
Componente	Criptaggio dei dati
ID evento di Windows	903
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Criptaggio/decriptaggio dei file interrotto

Stato	⚠
Componente	Criptaggio dei dati
ID evento di Windows	914
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Criptaggio/decriptaggio del dispositivo interrotto

Stato	⚠
Componente	Criptaggio dei dati
ID evento di Windows	1303
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Impossibile installare o eseguire l'upgrade dei driver di Criptaggio disco Kaspersky nell'immagine WinRE

Stato	⚠
Componente	Criptaggio dei dati
ID evento di Windows	1345
ID evento di Kaspersky Security Center	00000541
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Controllo firma del modulo non riuscito

Stato	⚠
Componente	Controllo integrità di sistema
ID evento di Windows	2002
ID evento di Kaspersky Security Center	000007d2
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avvio dell'applicazione bloccato

Stato	⚠
Componente	Sensore Endpoint
ID evento di Windows	2105
ID evento di Kaspersky Security Center	00000839
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Apertura del documento bloccata

Stato	⚠
Componente	Endpoint Sensor
ID evento di Windows	2106
ID evento di Kaspersky Security Center	0000083a
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il processo è stato terminato dall'amministratore del server Kaspersky Anti Targeted Attack Platform

Stato	⚠
Componente	Endpoint Sensor
ID evento di Windows	2112
ID evento di Kaspersky Security Center	00000840
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'applicazione è stata terminata dall'amministratore del server Kaspersky Anti Targeted Attack Platform

Stato	⚠
Componente	Sensore Endpoint
ID evento di Windows	2113
ID evento di Kaspersky Security Center	00000841
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il file o il flusso è stato eliminato dall'amministratore del server Kaspersky Anti Targeted Attack Platform

Stato	⚠
Componente	Sensore Endpoint
ID evento di Windows	2111
ID evento di Kaspersky Security Center	0000083f
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il file è stato ripristinato dalla Quarantena nel server Kaspersky Anti Targeted Attack Platform dall'amministratore

Stato	⚠
Componente	Sensore Endpoint
ID evento di Windows	2110
ID evento di Kaspersky Security Center	0000083e
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il file è stato messo in quarantena nel server di Kaspersky Anti Targeted Attack Platform dall'amministratore

Stato	⚠
Componente	Endpoint Sensor
ID evento di Windows	2109
ID evento di Kaspersky Security Center	0000083d
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Le attività di rete di tutte le applicazioni di terze parti sono bloccate

Stato	⚠
Componente	Endpoint Sensor
ID evento di Windows	2107
ID evento di Kaspersky Security Center	0000083b
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Le attività di rete di tutte le applicazioni di terze parti sono sbloccate

Stato	⚠
Componente	Endpoint Sensor
ID evento di Windows	2108
ID evento di Kaspersky Security Center	0000083c
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'oggetto verrà eliminato dopo il riavvio (Sandbox)

Stato	⚠
Componente	Sandbox
ID evento di Windows	2605
ID evento di Kaspersky Security Center	00000a2d
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Le dimensioni totali delle attività di scansione hanno superato il limite

Stato	⚠
Componente	Sandbox
ID evento di Windows	2612
ID evento di Kaspersky Security Center	00000a34
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avvio oggetto consentito, evento registrato

Stato	⚠
Componente	Endpoint Detection and Response
ID evento di Windows	2553
ID evento di Kaspersky Security Center	000009fa
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avvio processi consentito, evento registrato

Stato	⚠
Componente	Endpoint Detection and Response
ID evento di Windows	2554
ID evento di Kaspersky Security Center	000009f8
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'oggetto verrà eliminato dopo il riavvio (Endpoint Detection and Response)

Stato	⚠
Componente	Endpoint Detection and Response
ID evento di Windows	2558
ID evento di Kaspersky Security Center	000009fe
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Isolamento di rete

Stato	⚠
Componente	Endpoint Detection and Response
ID evento di Windows	2700
ID evento di Kaspersky Security Center	00000a8c
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Fine dell'isolamento di rete

Stato	⚠
Componente	Endpoint Detection and Response
ID evento di Windows	2701
ID evento di Kaspersky Security Center	00000a8d
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

È necessario riavviare il sistema per completare l'attività

Stato	⚠
Componente	Audit sistema
ID evento di Windows	225
ID evento di Kaspersky Security Center	0000057b
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

La connessione a un sito Web con un certificato non attendibile viene stabilita dalla decisione dell'utente

Stato	⚠
Componente	Network Detection and Response (KATA)
ID evento di Windows	70
ID evento di Kaspersky Security Center	00000046
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Messaggio all'amministratore per il blocco dell'avvio di un'applicazione

Stato	⚠
Componente	Controllo applicazioni
ID evento di Windows	503
ID evento di Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Parametri dell'evento	• GNRL_EA_DESCRIPTION è il messaggio per l'utente. • GNRL_EA_PARAM_2 è il nome dell'utente della sessione. • GNRL_EA_PARAM_6 è il nome del file eseguibile dell'applicazione (ad esempio, chrome.exe). • GNRL_EA_PARAM_7 è il percorso del file eseguibile. • GNRL_EA_PARAM_8 è l'hash dell'oggetto (SHA256). • GNRL_EA_PARAM_9 è la versione dell'applicazione che l'utente tenta di eseguire.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Messaggio all'amministratore per il blocco dell'accesso a un dispositivo

Stato	⚠
Componente	Controllo dispositivi
ID evento di Windows	804
ID evento di Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Parametri dell'evento	• c_er_descr è il messaggio per l'utente. • GNRL_EA_PARAM_1 è l'ID hardware (HWID). • GNRL_EA_PARAM_2 è il nome dell'utente della sessione.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Messaggio all'amministratore per il blocco dell'accesso a una pagina Web

Stato	⚠
Componente	Controllo Web
ID evento di Windows	755
ID evento di Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Parametri dell'evento	• GNRL_EA_DESCRIPTION è il messaggio per l'utente. • GNRL_EA_PARAM_1 è l'URL. • GNRL_EA_PARAM_2 è il nome dell'utente della sessione.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione dispositivo bloccata

Stato	⚠
Componente	Controllo dispositivi
ID evento di Windows	807
ID evento di Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'ID hardware (HWID). • GNRL_EA_PARAM_2 è il nome dell'utente della sessione.

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Messaggio all'amministratore per il blocco dell'attività di un'applicazione

Stato	⚠
Componente	Controllo adattivo delle anomalie
ID evento di Windows	`503`
ID evento di Kaspersky Security Center	`GNRL_EV_ADSEC_USER_REQUEST`
Parametri dell'evento	• `GNRL_EA_DESCRIPTION` è il messaggio per l'utente. • `GNRL_EA_PARAM_1` è il nome della regola di Controllo adattivo delle anomalie. • `GNRL_EA_PARAM_2` è l'ID della regola euristica. • `GNRL_EA_PARAM_3` è il nome dell'utente della sessione. • `GNRL_EA_PARAM_4` è il processo di origine. • `GNRL_EA_PARAM_5` è l'oggetto di origine. • `GNRL_EA_PARAM_6` è il processo di destinazione. • `GNRL_EA_PARAM_7` è l'oggetto di destinazione. • `GNRL_EA_PARAM_8` sono informazioni aggiuntive sull'oggetto rilevato: Hash del processo di origine/oggetto e processo di destinazione/oggetto. Processo bloccato (`verdict_type`): `true` o `false`. ID sicurezza utente (SID).
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'avvio dell'applicazione client del servizio cloud è bloccato

Stato	⚠
Componente	Cloud Discovery
ID evento di Windows	`2212`
ID evento di Kaspersky Security Center	`000008a4`
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'accesso al servizio cloud è bloccato

Stato	⚠
Componente	Cloud Discovery
ID evento di Windows	`2213`
ID evento di Kaspersky Security Center	`000008a5`
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

È stata rilevata la modifica di un file o di una cartella

Stato	ⓘ / ⚠ / ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	`2950`
ID evento di Kaspersky Security Center	`00000b86`
Registro eventi di Windows (predefinito)	–

Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

L'oggetto cambia troppo spesso. Aggregazione degli eventi avviata

Stato	ⓘ / ⚠ / ⓧ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2955
ID evento di Kaspersky Security Center	00000b8b
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rapporto sulla modifica degli oggetti per il periodo di aggregazione

Stato	ⓘ / ⚠ / ⓧ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2956
ID evento di Kaspersky Security Center	00000b8c
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

È stata rilevata la modifica del Registro di sistema

Stato	ⓘ / ⚠ / ⓧ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2951
ID evento di Kaspersky Security Center	00000b87
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

È stata rilevata la connessione/disconnessione del dispositivo

Stato	ⓘ / ⚠ / ⓧ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2952
ID evento di Kaspersky Security Center	00000b88

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

L'ambito del monitoraggio include oggetti errati

Stato	ⓘ / ⚠ / ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2903
ID evento di Kaspersky Security Center	00000b89
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

L'operazione vietata è stata consentita in modalità di test

Stato	⚠
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2961
ID evento di Kaspersky Security Center	00000b91
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile connettersi al server di integrazione per più di 30 minuti. Verificare lo stato del server di integrazione e le impostazioni di rete

Stato	⚠
Componente	Light Agent
ID evento di Windows	3102
ID evento di Kaspersky Security Center	00000c1e
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile connettersi al server di integrazione per più di 6 ore. Verificare lo stato del server di integrazione e le impostazioni di rete

Stato	⚠
Componente	Light Agent
ID evento di Windows	3103
ID evento di Kaspersky Security Center	00000c1f

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile connettersi al server di integrazione. Verificare lo stato del server di integrazione e le impostazioni di rete

Stato	⚠
Componente	Light Agent
ID evento di Windows	3101
ID evento di Kaspersky Security Center	00000c1d
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il modello della macchina virtuale deve essere aggiornato

Stato	⚠
Componente	Light Agent
ID evento di Windows	3181
ID evento di Kaspersky Security Center	00000c6d
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

La licenza Standard è terminata. L'applicazione è in esecuzione con la licenza Enterprise

Stato	⚠
Componente	Light Agent
ID evento di Windows	3171
ID evento di Kaspersky Security Center	00000c64
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Stato	⚠
Componente	Monitoraggio integrità file
ID evento di Windows	2901
ID evento di Kaspersky Security Center	00000b55
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Stato	⚠
Componente	Monitoraggio integrità file
ID evento di Windows	2900
ID evento di Kaspersky Security Center	00000b54
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Messaggio informativo

Applicazione avviata

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	235
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Applicazione arrestata

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	236
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Auto-difesa ha limitato l'accesso alla risorsa protetta

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	213
ID evento di Kaspersky Security Center	000000d5
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rapporto cancellato

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	217
ID evento di Kaspersky Security Center	000000d9
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Criterio di gruppo disabilitato

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	220

ID evento di Kaspersky Security Center	000000dc
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Impostazioni dell'applicazione modificate

Stato	
Componente	Audit sistema
ID evento di Windows	218
ID evento di Kaspersky Security Center	000000da
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Attività avviata

Stato	
Componente	Audit sistema
ID evento di Windows	221
ID evento di Kaspersky Security Center	000000dd
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Attività completata

Stato	
Componente	Audit sistema
ID evento di Windows	223
ID evento di Kaspersky Security Center	000000df
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Tutti i componenti dell'applicazione definiti dalla licenza sono stati installati e vengono eseguiti in modalità normale

Stato	
Componente	Audit sistema
ID evento di Windows	227
ID evento di Kaspersky Security Center	000000e3
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Le impostazioni dell'abbonamento sono state modificate

Stato	
Componente	Audit sistema
ID evento di Windows	238

ID evento di Kaspersky Security Center	000000ee
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'abbonamento è stato rinnovato

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	239
ID evento di Kaspersky Security Center	000000ef
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto ripristinato dal backup

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	335
ID evento di Kaspersky Security Center	0000014f
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Immissione nome utente e password

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	2000
ID evento di Kaspersky Security Center	000007d0
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Partecipazione a KSN abilitata

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	2020
ID evento di Kaspersky Security Center	000007e4
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Server KSN disponibili

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	2022

ID evento di Kaspersky Security Center	000007e6
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'applicazione gestisce ed elabora i dati in base alle leggi vigenti e utilizza l'infrastruttura appropriata

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	2024
ID evento di Kaspersky Security Center	000007e8
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto ripristinato dalla Quarantena

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	345
ID evento di Kaspersky Security Center	00000159
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto eliminato dalla Quarantena

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	347
ID evento di Kaspersky Security Center	0000015b
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

È stata creata una copia di backup dell'oggetto

Stato	ⓘ
Componente	Protezione minacce file Protezione minacce di posta Rilevamento del Comportamento Anti-Cryptor Prevenzione Intrusioni Host Sandbox Scansione malware
ID evento di Windows	308
ID evento di Kaspersky Security Center	00000134
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Sovrascritto da una copia disinfettata in precedenza

Stato	ⓘ
Componente	Protezione minacce file Prevenzione Intrusioni Host Scansione malware
ID evento di Windows	327
ID evento di Kaspersky Security Center	00000147
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Rilevato un archivio protetto da password

Stato	ⓘ
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Prevenzione Intrusioni Host Scansione malware
ID evento di Windows	322
ID evento di Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Parametri dell'evento	• GNRL_EA_PARAM_2 è il nome dell'oggetto. • GNRL_EA_PARAM_3 è la data di creazione dell'oggetto (opzionale). • GNRL_EA_PARAM_7 è il nome dell'utente della sessione. • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (engine). Tecnologie di rilevamento delle minacce (method). Minaccia rilevata dall'istanza privata di KSN (lista vietati): true o false.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Informazioni sull'oggetto rilevato

Stato	ⓘ
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Prevenzione Intrusioni Host Scansione malware
ID evento di Windows	332
ID evento di Kaspersky Security Center	0000014c
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'oggetto è presente nella lista consentiti di Kaspersky Private Security Network

Stato	ⓘ
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Prevenzione Intrusioni Host Scansione malware
ID evento di Windows	340

ID evento di Kaspersky Security Center	00000154
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto rinominato

Stato	ⓘ
Componente	Protezione minacce di posta Prevenzione Exploit Rilevamento del Comportamento Anti-Cryptor Scansione malware
ID evento di Windows	329
ID evento di Kaspersky Security Center	00000149
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto elaborato

Stato	ⓘ
Componente	Prevenzione Intrusioni Host Protezione minacce file Protezione minacce Web Protezione minacce di posta Scansione malware
ID evento di Windows	301
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Oggetto ignorato

Stato	ⓘ
Componente	Prevenzione Intrusioni Host Protezione minacce file Protezione AMSI Scansione malware
ID evento di Windows	315
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Archivio rilevato

Stato	ⓘ
Componente	Prevenzione Intrusioni Host Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Scansione malware
ID evento di Windows	318

ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Rilevato oggetto compresso

Stato	ⓘ
Componente	Prevenzione Intrusioni Host Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Scansione malware
ID evento di Windows	319
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Collegamento elaborato

Stato	ⓘ
Componente	Protezione minacce Web
ID evento di Windows	361
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Avvio dell'applicazione consentito

Stato	ⓘ
Componente	Controllo applicazioni
ID evento di Windows	701
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Sorgente degli aggiornamenti selezionata

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1001
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Server proxy selezionato

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1002
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Il collegamento è presente nella lista consentiti di Kaspersky Private Security Network

Stato	ⓘ
Componente	Protezione minacce Web
ID evento di Windows	370
ID evento di Kaspersky Security Center	00000172
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Applicazione inserita nel gruppo Attendibili

Stato	ⓘ
Componente	Prevenzione Intrusioni Host
ID evento di Windows	401
ID evento di Kaspersky Security Center	00000191
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Applicazione inserita in un gruppo con restrizioni

Stato	ⓘ
Componente	Prevenzione Intrusioni Host
ID evento di Windows	402
ID evento di Kaspersky Security Center	00000192
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

È stato attivato Prevenzione Intrusioni Host

Stato	ⓘ
Componente	Prevenzione Intrusioni Host
ID evento di Windows	403
ID evento di Kaspersky Security Center	00000193
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

File ripristinato

Stato	ⓘ
Componente	Rilevamento del Comportamento Anti-Cryptor Prevenzione Exploit Prevenzione Intrusioni Host
ID evento di Windows	457
ID evento di Kaspersky Security Center	000001c9
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Valore del Registro di sistema ripristinato

Stato	ⓘ
Componente	Rilevamento del Comportamento Prevenzione Exploit
ID evento di Windows	458
ID evento di Kaspersky Security Center	000001ca
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Valore del Registro di sistema eliminato

Stato	ⓘ
Componente	Rilevamento del Comportamento Prevenzione Exploit
ID evento di Windows	459
ID evento di Kaspersky Security Center	000001cb
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Azione del processo ignorata

Stato	ⓘ
Componente	Controllo adattivo delle anomalie
ID evento di Windows	2201
ID evento di Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
Parametri dell'evento	• GNRL_EA_PARAM_1 è il nome della regola di Controllo adattivo delle anomalie. • GNRL_EA_PARAM_2 è l'ID della regola euristica. • GNRL_EA_PARAM_3 è il nome dell'utente della sessione. • GNRL_EA_PARAM_4 è il processo di origine. • GNRL_EA_PARAM_5 è l'oggetto di origine. • GNRL_EA_PARAM_6 è il processo di destinazione. • GNRL_EA_PARAM_7 è l'oggetto di destinazione. • GNRL_EA_PARAM_8 sono informazioni aggiuntive sull'oggetto rilevato: Hash del processo di origine/oggetto e processo di destinazione/oggetto. Processo bloccato (verdict_type): true o false. ID sicurezza utente (SID).
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Tastiera autorizzata

Stato	ⓘ
Componente	Prevenzione Attacchi BadUSB
ID evento di Windows	2050
ID evento di Kaspersky Security Center	00000802
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Attività di rete consentita

Stato	ⓘ
Componente	Firewall
ID evento di Windows	601
ID evento di Kaspersky Security Center	00000259
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Avvio dell'applicazione non consentito in modalità di test

Stato	ⓘ
Componente	Controllo applicazioni
ID evento di Windows	703
ID evento di Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Parametri dell'evento	• GNRL_EA_PARAM_2 è il nome dell'utente della sessione. • GNRL_EA_PARAM_3 è l'identificatore della categoria creata manualmente. • GNRL_EA_PARAM_4 è l'identificatore di sicurezza dell'account (SID). • GNRL_EA_PARAM_5 si riferisce alle informazioni sulla firma digitale dell'applicazione. • GNRL_EA_PARAM_6 è il nome del file eseguibile dell'applicazione (ad esempio, chrome.exe). • GNRL_EA_PARAM_7 è il percorso del file eseguibile. • GNRL_EA_PARAM_8 è l'hash dell'oggetto (SHA256). • GNRL_EA_PARAM_9 è la versione dell'applicazione che l'utente tenta di eseguire.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Avvio dell'applicazione consentito in modalità di test

Stato	ⓘ
Componente	Controllo applicazioni
ID evento di Windows	704
ID evento di Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Parametri dell'evento	• GNRL_EA_PARAM_2 è il nome dell'utente della sessione. • GNRL_EA_PARAM_3 è l'identificatore della categoria creata manualmente. • GNRL_EA_PARAM_4 è l'identificatore di sicurezza dell'account (SID). • GNRL_EA_PARAM_5 si riferisce alle informazioni sulla firma digitale dell'applicazione.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Pagina consentita aperta

Stato	
Componente	Controllo Web
ID evento di Windows	751
ID evento di Kaspersky Security Center	000002f4
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Operazione con il dispositivo consentita

Stato	
Componente	Controllo dispositivi
ID evento di Windows	801
ID evento di Kaspersky Security Center	00000321
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Operazione sul file eseguita

Stato	
Componente	Controllo dispositivi
ID evento di Windows	808
ID evento di Kaspersky Security Center	GNRL_EV_USB_FILE_OPERATION
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'operazione sul file (scrittura o eliminazione). • GNRL_EA_PARAM_2 è il percorso del file. • GNRL_EA_PARAM_3 è il nome del dispositivo. • GNRL_EA_PARAM_4 è il nome dell'utente della sessione. • GNRL_EA_PARAM_5 è l'ID hardware (HWID).
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Nessun aggiornamento disponibile

Stato	
Componente	Aggiornamento
ID evento di Windows	1020
ID evento di Kaspersky Security Center	000003fc
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Distribuzione aggiornamenti completata correttamente

Stato	
Componente	Aggiornamento
ID evento di Windows	1022
ID evento di Kaspersky Security Center	000003fe

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Download dei file in corso...

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1003
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

File scaricato

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1004
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

File installato

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1005
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

File aggiornato

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1006
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Rollback del file a causa di un errore di aggiornamento

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1007
ID evento di Kaspersky Security Center	–

Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Aggiornamento dei file in corso...

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1008
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Distribuzione degli aggiornamenti...

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1009
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Rollback dei file in corso...

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1010
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Creazione dell'elenco dei file da scaricare...

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	1013
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Download delle patch in corso...

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	2150
ID evento di Kaspersky Security Center	–

Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Installazione della patch in corso...

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	2151
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Patch installata

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	2152
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Rollback della patch in corso...

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	2154
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Rollback della patch eseguito

Stato	ⓘ
Componente	Aggiornamento
ID evento di Windows	2155
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Applicazione delle regole di criptaggio/decriptaggio dei file avviata

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	901
ID evento di Kaspersky Security Center	00000385

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Applicazione delle regole di criptaggio/decriptaggio dei file completata

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	902
ID evento di Kaspersky Security Center	00000386
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Applicazione delle regole di criptaggio/decriptaggio dei file ripresa

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	905
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Criptaggio/decriptaggio dei file avviato

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	910
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Criptaggio/decriptaggio dei file completato

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	911
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Il file non è stato criptato perché è specificato come esclusione

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	913
ID evento di Kaspersky Security Center	–

Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Modalità portatile abilitata

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	950
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Modalità portatile disabilitata

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	952
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Criptaggio/decriptaggio del dispositivo avviato

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1301
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Criptaggio/decriptaggio del dispositivo completato

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1302
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Criptaggio/decriptaggio del dispositivo ripreso

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1304
ID evento di Kaspersky Security Center	–

Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Il dispositivo non è criptato

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1307
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Il processo di criptaggio/decriptaggio del dispositivo è passato in modalità attiva

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1308
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Il processo di criptaggio/decriptaggio del dispositivo è passato in modalità passiva

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1309
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Modulo di criptaggio caricato

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1310
ID evento di Kaspersky Security Center	0000051e
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Creazione nuovo account Agente di Autenticazione completata

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1330
ID evento di Kaspersky Security Center	00000532

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Account per l'Agente di Autenticazione eliminato

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1331
ID evento di Kaspersky Security Center	00000533
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Password dell'account per l'Agente di Autenticazione modificata

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1332
ID evento di Kaspersky Security Center	00000534
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Accesso all'Agente di Autenticazione completato

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1333
ID evento di Kaspersky Security Center	00000535
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Tentativo non riuscito di accesso all'Agente di Autenticazione

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1334
ID evento di Kaspersky Security Center	00000536
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Accesso al disco rigido eseguito mediante la procedura di richiesta di accesso ai dispositivi criptati

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1335
ID evento di Kaspersky Security Center	00000537

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Tentativo non riuscito di accesso al disco rigido mediante la procedura di richiesta di accesso ai dispositivi criptati

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1336
ID evento di Kaspersky Security Center	00000538
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

L'account non è stato aggiunto. Questo account esiste già

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1337
ID evento di Kaspersky Security Center	00000539
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

L'account non è stato modificato. Questo account non esiste

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1338
ID evento di Kaspersky Security Center	0000053a
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

L'account non è stato eliminato. Questo account non esiste

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1339
ID evento di Kaspersky Security Center	0000053b
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Upgrade FDE completato

Stato	
Componente	Criptaggio dei dati
ID evento di Windows	1341
ID evento di Kaspersky Security Center	0000053d

Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rollback dell'upgrade FDE completato

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1343
ID evento di Kaspersky Security Center	0000053f
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Impossibile disinstallare i driver di Criptaggio disco Kaspersky dall'immagine WinRE

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1346
ID evento di Kaspersky Security Center	00000542
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Chiave di ripristino di BitLocker modificata

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1370
ID evento di Kaspersky Security Center	0000055a
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Password / PIN BitLocker modificati

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1371
ID evento di Kaspersky Security Center	0000055b
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

La chiave di ripristino di BitLocker è stata salvata in un'unità rimovibile

Stato	ⓘ
Componente	Criptaggio dei dati
ID evento di Windows	1372
ID evento di Kaspersky Security Center	0000055c

Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'elaborazione delle attività del server Kaspersky Anti Targeted Attack Platform non è attiva

Stato	ⓘ
Componente	Sensore Endpoint
ID evento di Windows	2103
ID evento di Kaspersky Security Center	00000837
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Endpoint Sensor connesso al server

Stato	ⓘ
Componente	Endpoint Sensor
ID evento di Windows	2101
ID evento di Kaspersky Security Center	00000835
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione al server Kaspersky Anti Targeted Attack Platform ripristinata

Stato	ⓘ
Componente	Sensore Endpoint
ID evento di Windows	2102
ID evento di Kaspersky Security Center	00000836
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Le attività del server Kaspersky Anti Targeted Attack Platform sono in fase di elaborazione

Stato	ⓘ
Componente	Sensore Endpoint
ID evento di Windows	2104
ID evento di Kaspersky Security Center	00000838
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto eliminato

Stato	ⓘ
Componente	Cancella dati
ID evento di Windows	2251
ID evento di Kaspersky Security Center	000008cb

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	–

Statistiche attività di cancellazione

Stato	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID evento di Windows	2853
ID evento di Kaspersky Security Center	00000b25
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Stato	ⓘ
Componente	Cancella dati
ID evento di Windows	2253
ID evento di Kaspersky Security Center	000008cd
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto inserito in Quarantena (Sandbox)

Stato	ⓘ
Componente	Sandbox
ID evento di Windows	2602
ID evento di Kaspersky Security Center	00000a2a
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto eliminato (Sandbox)

Stato	ⓘ
Componente	Sandbox
ID evento di Windows	2604
ID evento di Kaspersky Security Center	00000a2c
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Scansione IOC avviata

Stato	ⓘ
Componente	Endpoint Detection and Response
ID evento di Windows	2652
ID evento di Kaspersky Security Center	00000a5c
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Scansione IOC completata

Stato	ⓘ
Componente	Endpoint Detection and Response
ID evento di Windows	2653
ID evento di Kaspersky Security Center	00000a5d
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto inserito in Quarantena (Endpoint Detection and Response)

Stato	ⓘ
Componente	Endpoint Detection and Response
ID evento di Windows	2555
ID evento di Kaspersky Security Center	000009fb
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Oggetto eliminato (Endpoint Detection and Response)

Stato	ⓘ
Componente	Endpoint Detection and Response
ID evento di Windows	2557
ID evento di Kaspersky Security Center	000009fd
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Componenti dell'applicazione modificati

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	1402
ID evento di Kaspersky Security Center	0000057a
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Stato	ⓘ
Componente	Sandbox
ID evento di Windows	2606
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Stato	ⓘ
Componente	Sandbox
ID evento di Windows	2609
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Stato	ⓘ
Componente	Sandbox
ID evento di Windows	2610
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

Stato	ⓘ
Componente	Sandbox
ID evento di Windows	2616
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	–

L'Administration Server a cui è connesso il dispositivo è impostato come attendibile

Stato	ⓘ
Componente	Protezione della connessione ad Administration Server
ID evento di Windows	3300
ID evento di Kaspersky Security Center	00000ce4
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il dispositivo è connesso a un nuovo Administration Server attendibile

Stato	ⓘ
Componente	Protezione della connessione ad Administration Server
ID evento di Windows	3302
ID evento di Kaspersky Security Center	00000ce6
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'Administration Server a cui è connesso il dispositivo non è più impostato come attendibile

Stato	ⓘ
Componente	Protezione della connessione ad Administration Server
ID evento di Windows	3303

ID evento di Kaspersky Security Center	00000ce7
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rilevamento Sandbox asincrono

Stato	ⓘ
Componente	Sandbox
ID evento di Windows	2619
ID evento di Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
Parametri dell'evento	• GNRL_EA_PARAM_1 sono i parametri dei componenti di Sandbox. • GNRL_EA_PARAM_2 è il percorso dell'oggetto. • GNRL_EA_PARAM_3 è l'ID dell'incidente. • GNRL_EA_PARAM_4 è l'hash dell'oggetto (SHA256).
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'attività di scansione è stata inviata correttamente a Sandbox da parte di un utente

Stato	ⓘ
Componente	Sandbox
ID evento di Windows	2622
ID evento di Kaspersky Security Center	00000a3e
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il dispositivo è connesso

Stato	ⓘ
Componente	Controllo dispositivi
ID evento di Windows	805
ID evento di Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'ID hardware (HWID). • GNRL_EA_PARAM_2 è il nome dell'utente della sessione.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Il dispositivo è disconnesso

Stato	ⓘ
Componente	Controllo dispositivi
ID evento di Windows	806
ID evento di Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Parametri dell'evento	• GNRL_EA_PARAM_1 è l'ID hardware (HWID). • GNRL_EA_PARAM_2 è il nome dell'utente della sessione.
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione al server di EDR Expert riuscita

Stato	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises)
ID evento di Windows	2853
ID evento di Kaspersky Security Center	00000b25
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione al server di risposta di EDR Expert riuscita

Stato	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID evento di Windows	2853
ID evento di Kaspersky Security Center	00000b25
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione al server di raccolta della telemetria di EDR Expert riuscita

Stato	ⓘ
Componente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
ID evento di Windows	2857
ID evento di Kaspersky Security Center	00000b26
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione al server NDR riuscita

Stato	ⓘ
Componente	Network Detection and Response (KATA)
ID evento di Windows	3083
ID evento di Kaspersky Security Center	00000c0b
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'avvio dell'applicazione client del servizio cloud è consentito

Stato	ⓘ
Componente	Cloud Discovery
ID evento di Windows	2210
ID evento di Kaspersky Security Center	000008a2

Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

L'accesso al servizio cloud è consentito

Stato	ⓘ
Componente	Cloud Discovery
ID evento di Windows	2211
ID evento di Kaspersky Security Center	000008a3
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Accesso all'area protetta

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	2004
ID evento di Kaspersky Security Center	000007d4
Registro eventi di Windows (predefinito)	✓
Registro eventi di Kaspersky Security Center (predefinito)	✓

È stata rilevata la modifica di un file o di una cartella

Stato	ⓘ / ⚠ / ⓔ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2950
ID evento di Kaspersky Security Center	00000b86
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

L'oggetto cambia troppo spesso. Aggregazione degli eventi avviata

Stato	ⓘ / ⚠ / ⓔ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2955
ID evento di Kaspersky Security Center	00000b8b
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Rapporto sulla modifica degli oggetti per il periodo di aggregazione

Stato	ⓘ / ⚠ / ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2956
ID evento di Kaspersky Security Center	00000b8c
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

È stata rilevata la modifica del Registro di sistema

Stato	ⓘ / ⚠ / ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2951
ID evento di Kaspersky Security Center	00000b87
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

È stata rilevata la connessione/disconnessione del dispositivo

Stato	ⓘ / ⚠ / ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2952
ID evento di Kaspersky Security Center	00000b88
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

L'ambito del monitoraggio include oggetti errati

Stato	ⓘ / ⚠ / ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2903
ID evento di Kaspersky Security Center	00000b89
Registro eventi di Windows (predefinito)	–

Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

Riferimento creato

Stato	ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2957
ID evento di Kaspersky Security Center	00000b8d
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Riferimento aggiornato

Stato	ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2958
ID evento di Kaspersky Security Center	00000b8e
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Un'operazione viene eseguita dall'utente attendibile

Stato	ⓘ
Componente	Monitoraggio integrità di sistema
ID evento di Windows	2962
ID evento di Kaspersky Security Center	00000b92
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Per configurare il periodo di conservazione per questo evento, passare alla sezione **Configurazione eventi** del criterio e impostare il periodo di conservazione per l'evento generale Monitoraggio dell'integrità del sistema - *È stata rilevata la modifica di un file o di una cartella*.

Connesso a SVM

Stato	ⓘ
Componente	Light Agent
ID evento di Windows	3152
ID evento di Kaspersky Security Center	00000c50
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

È stata creata una nuova password temporanea

Stato	ⓘ
Componente	Audit sistema
ID evento di Windows	265
ID evento di Kaspersky Security Center	00000109
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connesso al server di integrazione

Stato	ⓘ
Componente	Light Agent
ID evento di Windows	3105
ID evento di Kaspersky Security Center	00000c21
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Ripristino della connessione al server di integrazione...

Stato	ⓘ
Componente	Light Agent
ID evento di Windows	3104
ID evento di Kaspersky Security Center	00000c20
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Connessione al server KUMA riuscita

Stato	ⓘ
Componente	Integrazione KUMA
ID evento di Windows	2857
ID evento di Kaspersky Security Center	00000b29
Registro eventi di Windows (predefinito)	–
Registro eventi di Kaspersky Security Center (predefinito)	✓

Appendice 7. Estensioni di file supportate per Prevenzione dell'esecuzione

Kaspersky Endpoint Security supporta la prevenzione dell'apertura dei file in formato Office in alcune applicazioni. Le informazioni sulle applicazioni ed estensioni di file supportate sono riportate nella seguente tabella.

Estensioni di file supportate per Prevenzione dell'esecuzione

Nome dell'applicazione	File eseguibile	Estensione file
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

Appendice 8. Interpreti di script supportati per la prevenzione dell'esecuzione

Prevenzione dell'esecuzione supporta i seguenti interpreti di script:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe

- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Prevenzione dell'esecuzione supporta l'esecuzione delle applicazioni Java nell'ambiente di runtime Java (processi java.exe e javaw.exe).

Appendice 9. Ambito della scansione IOC nel Registro di sistema (RegistryItem)

Quando si aggiunge il tipo di dati **Registro di sistema di Windows - RegistryItem** all'ambito della scansione IOC, per impostazione predefinita Kaspersky Endpoint Security esamina le seguenti chiavi del Registro di sistema:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile
```

```
HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

Appendice 10. Requisiti del file IOC

Quando si creano attività Scansione IOC, è necessario tenere conto dei seguenti requisiti e limitazioni dei file IOC :

- L'applicazione supporta i file con estensioni IOC e XML nello standard aperto OpenIOC versioni 1.0 e 1.1 per la descrizione degli indicatori di compromissione.
- Dopo il caricamento dei file IOC, è possibile modificare manualmente i file nell'editor integrato direttamente nelle proprietà dell'attività. Kaspersky Endpoint Security supporta la modifica di file IOC conformi allo standard OpenIOC 1.1. Non è possibile modificare il contenuto dei file IOC compatibili con OpenIOC versione 1.0.
- Se, durante la creazione di un'attività *Scansione IOC* nella riga di comando, si caricano file IOC, alcuni dei quali non supportati, quando l'attività viene eseguita, l'applicazione utilizza solo i file IOC supportati. Se, durante la creazione di un'attività *Scansione IOC* sulla riga di comando, tutti i file IOC caricati risultano non supportati, l'attività può essere comunque eseguita, ma non rileverà alcun indicatore di compromissione. Non è possibile caricare file IOC non supportati utilizzando Web Console o Cloud Console.
- Gli errori semantici e i termini e i tag IOC non supportati nei file IOC non causano la mancata riuscita dell'esecuzione dell'attività. In tali sezioni dei file IOC, l'applicazione non rileva alcuna corrispondenza.
- Gli identificatori di tutti i file IOC utilizzati in una singola attività Scansione IOC devono essere univoci. Se sono presenti file IOC con lo stesso identificatore, potrebbe influire sui risultati dell'esecuzione dell'attività.
- Un singolo file IOC non deve avere dimensioni superiori a 2 MB. L'utilizzo di file più grandi causerà l'interruzione delle attività Scansione IOC con un errore. La dimensione finale di tutti i file aggiunti alla raccolta IOC non deve superare i 10 MB. Se la dimensione totale di tutti i file supera i 10 MB, è necessario suddividere la raccolta IOC e creare diverse attività *Scansione IOC*.

- È consigliabile creare un unico file IOC per minaccia. In questo modo, l'analisi dei risultati dell'attività *Scansione IOC* viene semplificata.

Il file che è possibile scaricare facendo clic sul collegamento sottostante contiene una tabella con l'elenco completo dei termini IOC dello standard OpenIOC.

SCARICA IL FILE IOC_TERMS.XLSX

Le funzionalità e le limitazioni del supporto dell'applicazione dello standard OpenIOC sono mostrate nella seguente tabella.

Funzionalità e limitazioni del supporto di OpenIOC versioni 1.0 e 1.1.

Condizioni supportate	OpenIOC 1.0:
	
	`is`
	`isnot` (come eccezione dal set)
	`contains`
	`containsnot` (come eccezione dal set)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Per i termini Email/*, sono supportate solo le condizioni `contains` e `is`. Per il corretto funzionamento di Scansione IOC retrospettiva, quando si utilizza la condizione `is`, gli indirizzi e-mail nei file IOC devono essere specificati nel seguente formato: `"name@example.org" <SMTP:name@example.org>`. Quando si esegue l'attività *Scansione IOC* normalmente, è sufficiente specificare l'indirizzo e-mail nel seguente formato: `name@example.org`.

Attributi di condizioni supportate	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Operatori supportati	`AND` `OR`
Tipi di dati supportati	`"date"`: data (condizioni applicabili: `is`, `greater-than`, `less-than`) `"int"`: numero intero (condizioni applicabili: `is`, `greater-than`, `less-than`) `"string"`: stringa (condizioni applicabili: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: durata in secondi (condizioni applicabili: `is`, `greater-than`, `less-than`)

Funzionalità dell'interpretazione dei tipi di dati	I tipi di dati `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` e `"base64Binary"` sono interpretati come stringa.
	
	L'applicazione supporta l'interpretazione dell'impostazione `Content` per i tipi di dati `int` e `date` quando è impostata in formato di intervalli:
	
	OpenIOC 1.0:
	Utilizzo dell'operatore `TO` nel campo `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Utilizzo delle condizioni `greater-than` e `less-than`
	Utilizzo dell'operatore `TO` nel campo `Content`:
	L'applicazione supporta l'interpretazione dei tipi di dati `date` e `duration` se gli indicatori sono impostati nel formato `ISO 8601, Zulu time zone, UTC`.

Appendice 11. API per la risposta alle minacce EDR

Kaspersky Endpoint Security 12.9 for Windows introduce il supporto per le azioni di EDR Threat Response (EDR responses) utilizzando Kaspersky Security Center OpenAPI. In altre parole, è possibile chiamare i metodi OpenAPI per automatizzare la risposta alle minacce EDR utilizzando Python. È possibile chiamare questi metodi durante l'integrazione con le soluzioni SIEM. *Kaspersky Unified Monitoring and Analysis Platform*, la soluzione Kaspersky SIEM, supporta EDR Threat Response OpenAPI a partire dalla versione 3.4.1. Per script di esempio, fare riferimento alla documentazione di KUMA.

Per eseguire le azioni di EDR Threat Response, è necessario creare una richiesta e inviarla utilizzando KSC Open API (`AddIncident`). Dopo l'elaborazione della richiesta, viene creata un'attività speciale nella console di Kaspersky Security Center.

Per creare attività durante la risposta alle minacce EDR, è necessario stabilire una connessione in background tra Administration Server e Kaspersky Security Center Web Console. Il servizio di connessione in background è disponibile in Kaspersky Security Center Windows 14.2 o versioni successive e in Kaspersky Security Center Linux 15.2 o versioni successive. Le altre console, incluse le console delle soluzioni Kaspersky Detection and Response, non sono supportate.

Per EDR Threat Response, è necessario specificare i parametri di base della richiesta, ad esempio in formato JSON:

- `task` è il tipo di attività (vedere di seguito).
- `targetHost` è l'ID del computer in cui è necessario eseguire lo script. Argomento richiesto. Lo script ottiene questo argomento dall'evento.
- `responseEventIncidentArea` è il nome dell'applicazione che ha eseguito lo script (ad esempio `KUMA`). Questo parametro viene aggiunto al nome dell'attività creata.

Per configurare EDR Threat Response, è necessario specificare le impostazioni dell'attività in formato JSON nel parametro `"KLINCDT_BODY": json.dumps(data)`. In seguito a questa operazione, l'applicazione crea `[Response][KUMA] <task type> - <Date> <Time> - <ID>` nella console di Kaspersky Security Center.

Connessione a Kaspersky Security Center OpenAPI

Nell'ambito di EDR Threat Response, l'applicazione crea attività speciali nella console di Kaspersky Security Center. La creazione di queste attività richiede la creazione di una connessione tra il computer e Kaspersky Security Center. A tale scopo, è necessario specificare i parametri di connessione di Kaspersky Security Center nella richiesta.

In Kaspersky XDR versione 2.1, il metodo di autorizzazione delle richieste è cambiato. Kaspersky XDR utilizza i token PAT anziché l'autenticazione di nome utente e password. Pertanto, non è possibile eseguire script in Kaspersky XDR. Per ulteriori informazioni sulla richiesta di autorizzazione, consultare la Guida di Kaspersky XDR.

Parametri di connessione di Kaspersky Security Center

Parametro	Tipo	Descrizione
`kscHost`	`string`	Indirizzo del server di Kaspersky Security Center Administration. Parametro richiesto.
`kscPort`	`int`	Porta di connessione ad Administration Server. Parametro richiesto.
`kscCert`	`string`	Percorso di un file di certificato per la connessione a Kaspersky Security Center Administration Server. Per impostazione predefinita, il parametro è impostato su `False`.
`kscUser`	`string`	Nome dell'account utente. Parametro richiesto.
`kscPassword`	`string`	Password dell'account utente. Parametro richiesto.

Esempio

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

I dati dell'account utente non sono protetti, pertanto è necessario dedicare un utente separato che verrà utilizzato solo per eseguire queste azioni.

Ottieni file – getFile

Impostazioni attività di Ottieni file

Parametro	Tipo	Descrizione
`md5hash`	`string`	Hash MD5 del file che si desidera ottenere.
`sha256hash`	`string`	Hash SHA256 del file che si desidera ottenere.
`path`	`string`	Percorso del file che si desidera ottenere.

Esempio

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Elimina il file – deleteFile

Impostazioni attività di Elimina il file

Parametro	Tipo	Descrizione
`md5hash`	`string`	Hash MD5 del file che si desidera eliminare.
`sha256hash`	`string`	Hash SHA256 del file che si desidera eliminare.
`path`	`string`	Percorso del file che si desidera eliminare.
`searchInSubfolders?`	`boolean`	Cercare il file che si desidera eliminare nelle sottocartelle.

Esempio

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Sposta file in Quarantena – quarantineFile

Impostazioni attività di Sposta file in Quarantena

Parametro	Tipo	Descrizione
`md5hash`	`string`	Hash MD5 del file che si desidera mettere in quarantena.
`sha256hash`	`string`	Hash SHA256 del file che si desidera mettere in quarantena.
`path`	`string`	Percorso del file che si desidera mettere in quarantena.

Esempio

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Scansione IOC – iocScan

Impostazioni attività di Scansione IOC

Parametro	Tipo	Descrizione
`ioc`	`string`	Percorso all'archivio ZIP con un file IOC che si desidera utilizzare per la scansione.
`isolateHost`	`boolean`	Isolare il computer dalla rete quando viene rilevato un indicatore di compromissione per prevenire la diffusione della minaccia.
`scanCriticalAreas`	`boolean`	Eseguire l'attività *Scansione delle aree critiche* quando viene rilevato un indicatore di compromissione.
`quarantineObject`	`boolean`	Eliminare l'oggetto dannoso quando viene rilevato un indicatore di compromissione. Prima di eliminare l'oggetto, Kaspersky Endpoint Security crea una copia di backup nel caso in cui sia necessario ripristinare l'oggetto in un secondo momento. Kaspersky Endpoint Security sposta la copia di backup in Quarantena.

Esempio

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Avvia processo – startProcess

Impostazioni attività di Avvia processo

Parametro	Tipo	Descrizione
executablePath	string	Percorso del file eseguibile utilizzato per avviare il processo.
arguments?	string	Argomenti della riga di comando aggiuntivi per l'avvio del processo.
workingFolder?	string	Percorso della cartella di lavoro del processo.

Esempio

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Termina processo – terminateProcess

Impostazioni attività di Termina processo

Parametro	Tipo	Descrizione
md5hash	string	Hash MD5 del file per cui si desidera arrestare il processo.
sha256hash	string	Hash SHA256 del file per cui si desidera arrestare il processo.
path	string	Percorso del file che si desidera eliminare.
caseSensitive	boolean	Fare distinzione tra maiuscole e minuscole durante la ricerca del file.

Esempio

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Isolamento di rete del computer - isolateHost

Impostazioni di isolamento di rete del computer

Parametro	Tipo	Descrizione
`action`	`string`	Modalità operativa Isolamento di rete.

Esempio

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Prevenzione dell'esecuzione - preventExecution

Impostazioni di Prevenzione dell'esecuzione

Parametro	Tipo	Descrizione
`hash`	`string`	Hash MD5 del file di cui si desidera impedire l'esecuzione.
`path`	`string`	Percorso del file di cui si desidera impedire l'esecuzione.
`caseSensitive`	`boolean`	Fare distinzione tra maiuscole e minuscole durante la ricerca del file.

Esempio

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Scansione malware – onDemandScan

Impostazioni attività di Scansione malware

Parametro	Tipo	Descrizione
`path`	`string`	Elenco di file e cartelle delimitato da spazi per Scansione personalizzata.
`recursive`	`boolean`	Modalità di scansione ricorsiva.

Parametro	Tipo	Descrizione
type	number	Ambito della scansione.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Esempio

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

Appendice 12. Account utente nelle regole dei componenti dell'applicazione

Per configurare alcuni componenti dell'applicazione, è necessario aggiungere regole speciali. Ad esempio, per Controllo Web è necessario aggiungere una regola con un elenco di indirizzi Web che si desidera vengano bloccati dall'applicazione. Nelle regole dei componenti dell'applicazione è inoltre possibile configurare una pianificazione per il componente o selezionare gli utenti a cui l'applicazione deve applicare la regola.

È necessario aggiungere regole per configurare i seguenti componenti dell'applicazione:

- Controllo applicazioni.
- Controllo Web.
- Controllo dispositivi.
- Log Inspection.
- Controllo adattivo delle anomalie.
- Monitoraggio integrità di sistema.

A partire da Kaspersky Endpoint Security for Windows 12.5, è possibile selezionare gli utenti non solo da Active Directory, ma anche nell'elenco degli utenti in Kaspersky Security Center. È inoltre possibile immettere manualmente i dati dell'account utente locale. Ciò significa che è possibile aggiungere utenti nei seguenti modi:

- Active Directory (consigliato)
- Elenco degli utenti in Kaspersky Security Center
- Account utente locale

Per utilizzare correttamente tutti i metodi di selezione utente, è necessario aggiornare l'applicazione Kaspersky Endpoint Security e il plug-in di gestione alla versione 12.5 o superiore.

Kaspersky consiglia di utilizzare account utente locali solo in casi speciali in cui non è possibile utilizzare account utente di dominio. Per informazioni dettagliate sui rischi per la sicurezza derivanti dall'utilizzo degli account locali, consultare la Knowledge Base di Microsoft. L'utente ha la piena responsabilità della protezione di un computer se vengono utilizzati account utente locali; ciò include in particolare la responsabilità del controllo e della limitazione dell'accesso alle impostazioni di Kaspersky Endpoint Security.

L'applicazione utilizza il SID (Security Identifier) dell'utente per identificare gli utenti. Quando si utilizzano account utente di Active Directory o dell'elenco di utenti di Kaspersky Security Center, l'applicazione determina il SID in Administration Server. Questo significa che l'applicazione non sovraccarica il computer per identificare un utente. Se sono stati aggiunti più di 1000 account utente locali a una regola dell'applicazione, l'applicazione contatta il controller di dominio per identificare l'utente. Ciò significa che il carico sul computer è aumentato. Per ottimizzare l'impatto sulle prestazioni del computer, è consigliabile utilizzare gli account utente di Active Directory o l'elenco di utenti di Kaspersky Security Center.

L'applicazione utilizza i nomi NetBIOS per l'identificazione degli account utente aggiunti manualmente nei formati `<username>` e `<hostname>\<username>`. Un nome NetBIOS può avere una lunghezza massima di 16 byte (15 caratteri). Se il nome del computer supera i 15 caratteri, l'applicazione non è in grado di identificare l'utente. L'applicazione disabilita la regola e genera un errore, ad esempio *Controllo Web: attivazione delle regole disabilitata per gli account utente senza corrispondenza dell'identificativo di sicurezza (SID)*. Per far funzionare la regola, è necessario accorciare manualmente il nome del computer. È possibile aggiungere account utente da Active Directory o Kaspersky Security Center. In questo caso, l'applicazione accorcia automaticamente il nome del computer.

Kaspersky Endpoint Security supporta anche utenti e gruppi predefiniti (ad esempio il gruppo "Tutti") nelle regole. A causa della modalità di determinazione del SID di un utente, l'applicazione consente di utilizzare solo account utente predefiniti aggiunti da Active Directory o dall'elenco degli utenti in Kaspersky Security Center. Le regole in cui un account utente predefinito viene aggiunto in locale non funzionano.

Informazioni legali

Trasmissione dei dati

Questa sezione contiene informazioni sui dati che l'applicazione Kaspersky Endpoint Security può archiviare nel dispositivo e trasmettere automaticamente a Kaspersky durante il suo funzionamento.

Le informazioni ricevute sono protette da Kaspersky in conformità alla legge e ai requisiti e alle normative applicabili di Kaspersky. I dati vengono trasmessi tramite canali di comunicazione criptati.

Trasmissione dei dati nell'ambito del Contratto di licenza con l'utente finale

Se viene applicato un codice di attivazione per attivare Kaspersky Endpoint Security, si accetta di inviare periodicamente a Kaspersky le seguenti informazioni in modo automatico per verificare il corretto utilizzo dell'applicazione:

- Tipo, versione e versione localizzata di Kaspersky Endpoint Security;
- Versioni degli aggiornamenti installati per Kaspersky Endpoint Security;
- ID del computer e ID dell'installazione specifica di Kaspersky Endpoint Security nel computer;
- Numero di serie e identificatore chiave attiva;
- Tipo, versione e velocità in bit del sistema operativo e nome dell'ambiente virtuale (se Kaspersky Endpoint Security è installato in un ambiente virtuale);
- ID richiesta univoco ai servizi del Titolare dei diritti;
- ID dei componenti di Kaspersky Endpoint Security attivi quando vengono trasmesse le informazioni.

Kaspersky può inoltre utilizzare queste informazioni per generare statistiche sulla distribuzione e sull'utilizzo del software Kaspersky.

Utilizzando un codice di attivazione, l'utente accetta di trasmettere automaticamente i dati sopra elencati. Se non si accetta di trasmettere queste informazioni a Kaspersky, è necessario utilizzare un file chiave per attivare Kaspersky Endpoint Security.

Accettando le condizioni del Contratto di licenza con l'utente finale, si accetta di trasmettere automaticamente le seguenti informazioni:

- Durante l'upgrade di Kaspersky Endpoint Security:
  - Versione di Kaspersky Endpoint Security;
  - ID di Kaspersky Endpoint Security;

- Chiave attiva;
- ID univoco dell'avvio dell'attività di aggiornamento;
- ID univoco dell'installazione di Kaspersky Endpoint Security.

- Quando vengono selezionati i collegamenti dall'interfaccia di Kaspersky Endpoint Security:
  - Versione di Kaspersky Endpoint Security;
  - Versione del sistema operativo;
  - Data di attivazione di Kaspersky Endpoint Security;
  - data di scadenza della licenza;
  - Kata di creazione della chiave;
  - Data di installazione di Kaspersky Endpoint Security;
  - ID di Kaspersky Endpoint Security;
  - ID della vulnerabilità rilevata nel sistema operativo;
  - ID dell'ultimo aggiornamento installato per Kaspersky Endpoint Security;
  - Hash del file rilevato con una minaccia e nome della minaccia secondo la classificazione di Kaspersky;
  - Categoria dell'errore di attivazione di Kaspersky Endpoint Security;
  - Codice dell'errore di attivazione di Kaspersky Endpoint Security;
  - Numero di giorni mancanti alla scadenza della chiave;
  - Numero di giorni trascorsi dall'aggiunta della chiave;
  - Numero di giorni trascorsi dalla scadenza della licenza;
  - Numero di computer in cui è applicata la licenza corrente;
  - Chiave attiva;
  - Periodo di validità della licenza di Kaspersky Endpoint Security;
  - Stato corrente della licenza;
  - Tipo di licenza corrente;
  - Tipo di applicazione;
  - ID univoco dell'avvio dell'attività di aggiornamento;
  - ID univoco dell'installazione di Kaspersky Endpoint Security nel computer;
  - Lingua dell'interfaccia di Kaspersky Endpoint Security.

Le informazioni ricevute sono protette da Kaspersky in conformità alla legge e ai requisiti e alle normative applicabili di Kaspersky. I dati vengono trasmessi tramite canali di comunicazione criptati.

Leggere il Contratto di licenza con l'utente finale e visitare il sito Web di Kaspersky per informazioni su come vengono ricevute, elaborate, archiviate ed eliminate le informazioni sull'utilizzo dell'applicazione una volta che si accettano il Contratto di licenza con l'utente finale e l'Informativa di Kaspersky Security Network. I file license.txt e ksn_<ID lingua>.txt contengono il testo del Contratto di licenza con l'utente finale e l'Informativa di Kaspersky Security Network e sono inclusi nel kit di distribuzione dell'applicazione.

Trasmissione dei dati durante l'utilizzo di Kaspersky Security Network

Il set di dati che Kaspersky Endpoint Security invia a Kaspersky dipende dal tipo di licenza e dalle impostazioni di utilizzo di Kaspersky Security Network.

Utilizzo di KSN con licenza su un massimo di 4 computer

Accettando l'Informativa di Kaspersky Security Network, si accetta di trasmettere automaticamente le seguenti informazioni:

- informazioni sugli aggiornamenti di configurazione KSN: identificatore della configurazione attiva, identificatore della configurazione ricevuta, codice di errore dell'aggiornamento di configurazione;
- informazioni sui file e sugli indirizzi URL da esaminare: checksum del file esaminato (MD5, SHA2-256, SHA1) e modelli di file (MD5), dimensioni del modello, tipo di minaccia rilevata e il relativo nome secondo la classificazione del Titolare dei diritti, identificatore dei database anti-virus, indirizzo URL per cui è richiesta la reputazione, nonché l'indirizzo URL di riferimento, identificatore del protocollo della connessione e il numero della porta utilizzata;
- ID dell'attività di scansione che ha rilevato la minaccia;
- informazioni sui certificati digitali utilizzati necessari per verificarne l'autenticità: checksum (SHA256) del certificato utilizzato per firmare l'oggetto esaminato e la chiave pubblica del certificato;
- identificatore del componente Software che esegue l'analisi;
- ID dei database anti-virus e dei record in questi database anti-virus;
- Informazioni sull'attivazione del Software nel Computer: intestazione firmata del ticket del servizio di attivazione (identificatore del centro di attivazione dell'area di riferimento, checksum del codice di attivazione, checksum del ticket, data di creazione del ticket, identificatore univoco del ticket, versione del ticket, stato della licenza, data di inizio e fine e ora di validità del ticket, identificatore univoco della licenza, versione della licenza), identificatore del certificato utilizzato per firmare l'intestazione del ticket, checksum (MD5) del file chiave;
- Informazioni sul Software del Titolare dei diritti: versione completa, tipo e versione del protocollo utilizzato per la connessione ai servizi Kaspersky.

Utilizzo di KSN con licenza su 5 o più computer

Accettando l'Informativa di Kaspersky Security Network, si accetta di trasmettere automaticamente le seguenti informazioni:

Se la casella di controllo **Kaspersky Security Network** è selezionata e la casella di controllo **Abilita modalità KSN estesa** è deselezionata, l'applicazione invia le seguenti informazioni:

- informazioni sugli aggiornamenti di configurazione KSN: identificatore della configurazione attiva, identificatore della configurazione ricevuta, codice di errore dell'aggiornamento di configurazione;
- informazioni sui file e sugli indirizzi URL da esaminare: checksum del file esaminato (MD5, SHA2-256, SHA1) e modelli di file (MD5), dimensioni del modello, tipo di minaccia rilevata e il relativo nome secondo la classificazione del Titolare dei diritti, identificatore dei database anti-virus, indirizzo URL per cui è richiesta la reputazione, nonché l'indirizzo URL di riferimento, identificatore del protocollo della connessione e il numero della porta utilizzata;
- ID dell'attività di scansione che ha rilevato la minaccia;
- informazioni sui certificati digitali utilizzati necessari per verificarne l'autenticità: checksum (SHA256) del certificato utilizzato per firmare l'oggetto esaminato e la chiave pubblica del certificato;
- identificatore del componente Software che esegue l'analisi;
- ID dei database anti-virus e dei record in questi database anti-virus;
- Informazioni sull'attivazione del Software nel Computer: intestazione firmata del ticket del servizio di attivazione (identificatore del centro di attivazione dell'area di riferimento, checksum del codice di attivazione, checksum del ticket, data di creazione del ticket, identificatore univoco del ticket, versione del ticket, stato della licenza, data di inizio e fine e ora di validità del ticket, identificatore univoco della licenza, versione della licenza), identificatore del certificato utilizzato per firmare l'intestazione del ticket, checksum (MD5) del file chiave;
- Informazioni sul Software del Titolare dei diritti: versione completa, tipo e versione del protocollo utilizzato per la connessione ai servizi Kaspersky.

Se oltre alla casella di controllo **Kaspersky Security Network** è selezionata anche la casella di controllo **Abilita modalità KSN estesa**, l'applicazione invia anche le seguenti informazioni, oltre a quelle elencate precedentemente:

- informazioni sui risultati della categorizzazione delle risorse Web richieste che contengono l'URL elaborata e l'indirizzo IP dell'host, versione del componente del Software che ha eseguito la categorizzazione, metodo di categorizzazione e set di categorie determinato per la risorsa Web;
- informazioni sul software installato nel Computer: nomi delle applicazioni software e dei produttori software, chiavi del Registro di sistema e relativi valori, informazioni sui file dei componenti software installati (checksum (MD5, SHA2-256, SHA1), nome, percorso del file nel Computer, dimensioni, versione e la firma digitale);
- informazioni sullo stato della protezione anti-virus del Computer: le versioni e i timestamp di rilascio dei database anti-virus utilizzati, l'ID dell'attività e l'ID del Software che esegue la scansione;

- informazioni sui file scaricati dall'utente finale: gli indirizzi URL e IP del download e pagine di download, identificatore del protocollo di download e numero di porta della connessione, stato dannoso o non dannoso delle URL, attributi del file, dimensioni e checksum (MD5, SHA2-256, SHA1), informazioni sul processo che ha scaricato il file (checksum (MD5, SHA2-256, SHA1), data e ora di creazione/build, stato di riproduzione automatica, attributi, nomi delle utilità di compressione, informazioni sulle firme, contrassegno del file eseguibile, identificatore del formato ed entropia), nome del file e relativo percorso nel Computer, firma digitale del file e marca timestamp della relativa generazione, indirizzo dell'URL in cui si è verificato il rilevamento, numero dello script nella pagina che viene considerata sospetta o dannosa, informazioni relative alle richieste HTTP generate e risposta a tali richieste;

- informazioni sulle applicazioni in esecuzione e sui relativi moduli: dati sui processi in esecuzione nel sistema (ID processo (PID), nome del processo, informazioni sull'account da cui è stato avviato il processo, l'applicazione e il comando che ha avviato il processo, identificatore del processo o del programma attendibile, percorso completo dei file del processo e relativi checksum (MD5, SHA2-256, SHA1), la riga di comando iniziale, livello di integrità del processo, una descrizione del prodotto a cui appartiene il processo (il nome del prodotto e le informazioni sull'editore), nonché i certificati digitali in uso e le informazioni necessarie per verificarne l'autenticità o informazioni sull'assenza della firma digitale di un file) e informazioni sui moduli caricati nei processi (relativi nomi, dimensioni, tipi, date di creazione, attributi, checksum (MD5, SHA2-256, SHA1), relativi percorsi nel computer), informazioni sull'intestazione dei file PE, nomi delle utilità di compressione (se il file è stato compresso);

- informazioni su tutte le attività e gli oggetti potenzialmente dannosi: nome dell'oggetto rilevato e percorso completo dell'oggetto nel computer, checksum dei file elaborati (MD5, SHA2-256, SHA1), data e ora di rilevamento, nomi e dimensioni dei file infetti e relativi percorsi, codice del modello di percorso, contrassegno del file eseguibile, indicatore che stabilisce se l'oggetto è un contenitore, nomi del programma di compressione (se il file è compresso), codice del tipo di file, ID formato file, elenco delle azioni eseguite dal malware e decisione del software e dell'utente in risposta a tali azioni, ID dei database anti-virus e dei record presenti in questi database anti-virus utilizzati per la decisione, indicatore di un oggetto potenzialmente dannoso, nome della minaccia rilevata secondo la classificazione del Titolare dei diritti, livello di pericolosità, stato di rilevamento e metodo di rilevamento, motivo dell'inclusione nel contesto analizzato e numero progressivo del file nel contesto, checksum (MD5, SHA2-256, SHA1), nome e attributi del file eseguibile dell'applicazione tramite cui è stato trasmesso il messaggio o il collegamento infetto, indirizzi IP (IPv4 e IPv6) anonimi dell'host dell'oggetto bloccato, entropia file, indicatore di esecuzione automatica del file, ora del primo rilevamento del file nel sistema, numero di volte in cui il file è stato eseguito dall'ultimo invio delle statistiche, informazioni sul nome, checksum (MD5, SHA2-256, SHA1) e dimensioni del client di posta tramite il quale è stato ricevuto l'oggetto dannoso, ID dell'attività software che ha eseguito la scansione, indicatore di verifica della firma o della reputazione del file, risultato di elaborazione del file, checksum (MD5) del modello raccolto per l'oggetto, dimensioni del modello in byte e specifiche tecniche delle tecnologie di rilevamento applicate;

- informazioni sugli oggetti esaminati: il gruppo di attendibilità assegnato in/da cui è stato inserito il file, il motivo per cui il file è stato inserito in tale categoria, identificatore di categoria, informazioni sull'origine delle categorie e versione del database di categorie, contrassegno del certificato attendibile del file, nome del produttore del file, versione del file, nome e versione dell'applicazione software che include il file;

- informazioni sulle vulnerabilità rilevate: ID vulnerabilità nel database delle vulnerabilità, classe di pericolo della vulnerabilità;

- informazioni sull'emulazione del file eseguibile: dimensioni del file e relativi checksum (MD5, SHA2-256, SHA1), versione del componente di emulazione, livello di emulazione, un array di proprietà dei blocchi logici e funzioni all'interno dei blocchi logici ottenuti durante l'emulazione, dati delle intestazioni PE del file eseguibile;

- gli indirizzi IP del computer che ha originato l'attacco (IPv4 e IPv6), il numero della porta nel Computer a cui è diretto l'attacco di rete, identificatore del protocollo del pacchetto IP che contiene l'attacco, destinazione dell'attacco (nome dell'organizzazione, sito Web), contrassegno per la reazione all'attacco, peso dell'attacco, livello di attendibilità;

- informazioni relative agli attacchi associati alle risorse di rete contraffatte e indirizzi DNS e IP (IPv4 o IPv6) dei siti Web visitati;

- indirizzi IP e DNS (IPv4 or IPv6) della risorsa Web richiesta, informazioni sul file e sul Web client che accede alla risorsa Web, nome, dimensioni e checksum (MD5, SHA2-256, SHA1) del file, percorso completo del file e codice del modello di percorso, risultato della verifica della firma digitale e il relativo stato in KSN;

- informazioni sul rollback delle azioni del malware: dati sul file per cui è stato eseguito il rollback delle attività (nome del file, percorso completo del file, dimensioni e checksum di riferimento (MD5, SHA2-256, SHA1)), dati sulle azioni andate e non andate a buon fine mirate a eliminare, rinominare e copiare i file e ripristinare i valori nel Registro di sistema (nomi delle chiavi di registro e relativi valori) e informazioni sui file di sistema modificati dal malware, prima e dopo il rollback;

- informazioni sulle esclusioni impostate per il componente Controllo adattivo delle anomalie: l'ID e lo stato della regola che è stata attivata, l'azione eseguita dal Software durante l'attivazione della regola, il tipo di account utente con cui il processo o il thread esegue l'attività sospetta, informazioni sul processo che ha eseguito o subito l'attività sospetta (ID script o nome del file di processo, percorso completo del file di processo, codice del modello di percorso, checksum (MD5, SHA2-256, SHA1) del file del processo); informazioni sull'oggetto che ha eseguito le azioni sospette e sull'oggetto che ha subito le azioni sospette (nome della chiave del Registro di sistema o nome del file, percorso completo del file, codice del modello di percorso e checksum (MD5, SHA2-256, SHA1) del file).

- Informazioni sui moduli software caricati: nome, dimensioni e checksum (MD5, SHA2-256, SHA1) del file del modulo, percorso completo e codice del modello di percorso, impostazioni della firma digitale del file del modulo, data e ora di creazione della firma, nome del soggetto e dell'organizzazione che ha firmato il file del modulo, ID del processo in cui è stato caricato il modulo, nome del fornitore del modulo e numero di sequenza del modulo nella coda di caricamento;

- informazioni sulla qualità dell'interazione del Software con i servizi KSN: ora e data di inizio e fine del periodo in cui sono state generate le statistiche, informazioni sulla qualità delle richieste e connessione a ciascun servizio KSN utilizzato (ID del servizio KSN, numero richieste andate e buon fine, numero di richieste con risposte dalla cache, numero di richieste non andate a buon fine (problemi di rete, KSN disabilitato nelle impostazioni del Software, routing errato), intervallo temporale delle richieste andate a buon fine, intervallo temporale delle richieste annullate, intervallo temporale delle richieste con limite di tempo superato, numero di connessioni a KSN provenienti dalla cache, numero di connessioni a KSN andate a buon fine, numero di connessioni a KSN non andate a buon fine, numero di transazioni andate a buon fine, numero di transazioni non andate a buon fine, intervallo temporale delle connessioni a KSN andate a buon fine, intervallo temporale delle connessioni a KSN non andate a buon fine, intervallo temporale delle transazioni andate a buon fine, intervallo temporale delle transazioni non andate a buon fine);

- se viene rilevato un oggetto potenzialmente dannoso, vengono fornite informazioni sui dati nella memoria dei processi: gli elementi della gerarchia degli oggetti di sistema (ObjectManager), i dati nella memoria UEFI BIOS, i nomi delle chiavi del Registro di sistema e i relativi valori;

- informazioni sugli eventi nei registri di sistema: timestamp dell'evento, nome del registro in cui è stato rilevato l'evento, tipo e categoria dell'evento, nome dell'origine dell'evento e descrizione dell'evento;

- informazioni sulle connessioni di rete: versione e checksum (MD5, SHA2-256, SHA1) del file da cui è stato avviato il processo che ha aperto la porta, percorso del file del processo e relativa firma digitale, indirizzi IP locali e remoti, numeri delle porte di connessione locali e remote, stato della connessione e timestamp di apertura della porta;

- informazioni sulla data di installazione e attivazione del Software nel Computer: l'ID del partner che ha venduto la licenza, il numero di serie della licenza, l'intestazione firmata del ticket del servizio di attivazione (l'ID di un centro di attivazione regionale, il checksum del codice di attivazione, il checksum del ticket, la data di creazione del ticket, l'ID univoco del ticket, la versione del ticket, lo stato della licenza, la data e ora di inizio/fine del ticket, l'ID univoco della licenza, la versione della licenza), l'ID del certificato utilizzato per firmare l'intestazione del ticket, il checksum (MD5) del file chiave, l'ID univoco dell'installazione del Software nel Computer, il tipo e l'ID dell'applicazione che viene aggiornata, l'ID dell'attività di aggiornamento;

- informazioni sul set di tutti gli aggiornamenti installati e il set di aggiornamenti installati o rimossi più di recente, il tipo di evento che ha causato l'invio delle informazioni sull'aggiornamento, periodo trascorso dall'installazione dell'ultimo aggiornamento, informazioni su tutti i database anti-virus attualmente installati;

- Informazioni sul funzionamento del software nel computer: dati sull'utilizzo della CPU, dati sull'utilizzo della memoria (byte privati, pool non di paging, pool di paging), numero di thread attivi nel processo del software e thread in sospeso, nonché durata dell'esecuzione del software prima dell'errore;

- numero di dump del software e di dump del sistema (schermata blu di errore) dall'installazione del Software e dall'ultimo aggiornamento, identificatore e versione del modulo Software in cui si è verificato l'arresto anomalo, stack di memoria nel processo del Software e informazioni sui database anti-virus al momento dell'arresto anomalo;

- dati sul dump del sistema (schermata blu di errore): un contrassegno che indica la comparsa della schermata blu di errore nel computer, il nome del driver che ha causato la schermata blu di errore, l'indirizzo e lo stack di memoria nel driver, un contrassegno che indica la durata della sessione del sistema operativo prima della comparsa della schermata blu di errore, stack di memoria del driver in cui si è verificato l'arresto anomalo, tipo di dump della memoria archiviato, contrassegno relativo alla sessione del sistema operativo prima della schermata blu di errore con durata superiore ai 10 minuti, identificatore univoco del dump, timestamp della schermata blu di errore;

- informazioni sugli errori o sui problemi di prestazioni che si sono verificati durante l'esecuzione dei componenti Software: ID dello stato del Software, tipo di errore, codice e causa e momento in cui si è verificato l'errore, ID del componente, modulo e processo del prodotto in cui si è verificato l'errore, l'ID della categoria di aggiornamento o attività in cui si è verificato l'errore, registri dei driver utilizzati dal Software (codice di errore, nome del modulo, nome del file di origine e riga in cui si è verificato l'errore);

- informazioni sugli aggiornamenti dei database anti-virus e componenti Software: nome, data e ora dei file indice scaricati durante l'ultimo aggiornamento e scaricati durante l'aggiornamento corrente;

- informazioni sull'arresto anomalo dell'esecuzione del Software: timestamp di creazione del dump, il tipo, il tipo di evento che ha causato l'arresto anomalo dell'esecuzione del Software (spegnimento improvviso, arresto anomalo dell'applicazione di terzi), data e ora dello spegnimento improvviso;

- informazioni sulla compatibilità dei driver Software con i requisiti hardware e Software: le informazioni sulle proprietà del sistema operativo che limitano le funzionalità dei componenti Software (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), il tipo di software di download installato (UEFI, BIOS), l'identificatore TPM (Trusted Platform Module), la versione della specifica TPM, le informazioni sulla CPU installata nel Computer, la modalità operativa e i parametri di Code Integrity e Device Guard, la modalità operativa dei driver e il motivo dell'utilizzo della modalità corrente, la versione dei driver Software, lo stato di supporto della virtualizzazione hardware e software del Computer;

- informazioni sulle applicazioni di terzi che hanno causato l'errore: nome, versione e localizzazione, codice di errore e informazioni sull'errore contenute nel registro di sistema delle applicazioni, indirizzo dell'errore e stack di memoria dell'applicazione di terzi, contrassegno che indica la presenza dell'errore nel componente software, periodo di esecuzione dell'applicazione di terzi prima dell'errore, checksum (MD5, SHA2-256, SHA1) dell'immagine del processo dell'applicazione in cui si è verificato l'errore, percorso dell'immagine del processo dell'applicazione e codice del modello di percorso, informazioni del registro di sistema con una descrizione dell'errore associato all'applicazione, informazioni sul modulo dell'applicazione in cui si è verificato l'errore (identificatore eccezione, indirizzo di memoria dell'arresto anomalo come offset nel modulo dell'applicazione, nome e versione del modulo, identificatore dell'arresto anomalo dell'applicazione nel plug-in del Titolare dei diritti e stack di memoria dell'arresto anomalo, durata della sessione dell'applicazione prima dell'arresto anomalo);

- versione del componente di aggiornamento del Software, numero di arresti anomali del componente di aggiornamento durante l'esecuzione delle attività di aggiornamento per tutta la durata del componente, ID del tipo di attività di aggiornamento, numero di tentativi non andati a buon fine del componente di aggiornamento per il completamento delle attività di aggiornamento;

- informazioni sul funzionamento dei componenti di monitoraggio del sistema Software: versioni complete dei componenti, data e ora di avvio dei componenti, codice dell'evento che ha causato l'overflow della coda di eventi e il numero di tali eventi, il numero totale degli eventi di overflow della coda, informazioni sul file del processo dell'iniziatore dell'evento (nome del file e relativo percorso nel Computer, codice del modello del percorso del file, checksum (MD5, SHA2-256, SHA1) del processo associato al file, versione del file), identificatore dell'intercettazione di eventi che si è verificata, la versione completa del filtro di intercettazione, identificatore del tipo di evento intercettato, dimensioni della coda di eventi e il numero di eventi tra il primo evento nella coda e l'evento corrente, numero di eventi scaduti nella coda, informazioni sul file del processo dell'iniziatore dell'evento corrente (nome del file e relativo percorso nel Computer, codice del modello del percorso del file, checksum (MD5, SHA2-256, SHA1) del processo associato al file), durata dell'elaborazione degli eventi, durata massima dell'elaborazione degli eventi, probabilità di invio delle statistiche, informazioni sugli eventi del sistema operativo per cui è stato superato il limite di tempo per l'elaborazione (data e ora dell'evento, numero di inizializzazioni ripetute dei database anti-virus, data e ora dell'ultima inizializzazione ripetuta dei database anti-virus dopo il relativo aggiornamento, ritardo di elaborazione degli eventi per ogni componente di monitoraggio del sistema, numero di eventi in coda, numero di eventi elaborati, numero di eventi posticipati del tipo corrente, ritardo totale per gli eventi del tipo corrente, ritardo totale per tutti gli eventi);

- informazioni provenienti dallo strumento di tracciamento degli eventi di Windows (ETW, Event Tracing for Windows) in caso di problemi di prestazioni del Software, fornitori di eventi SysConfig / SysConfigEx / WinSATAssessment di Microsoft: informazioni sul Computer (modello, produttore, fattori di forma dell'alloggiamento, versione), informazioni sulle metriche delle prestazioni Windows (valutazioni WinSAT, indice prestazioni di Windows), nome di dominio, informazioni sui processori logici e fisici (numero di processori logici e fisici, produttore, modello, livello di stepping, numero di core, frequenza di clock, CPUID, caratteristiche della cache, caratteristiche del processore logico, indicatori delle modalità supportate e istruzioni), informazioni sui moduli RAM (tipo, fattore di forma, produttore, modello, capacità, granularità di allocazione della memoria), informazioni sulle interfacce di rete (indirizzi IP e MAC, nome, descrizione, configurazione delle interfacce di rete, suddivisione del numero e dimensioni dei pacchetti di rete in base al tipo, velocità dello scambio di rete, suddivisione del numero degli errori di rete in base al tipo), configurazione del controller IDE, indirizzi IP dei server DNS, informazioni sulla scheda video (modello, descrizione, produttore, compatibilità, capacità della memoria video, autorizzazione dello schermo, numero di bit per pixel, versione BIOS), informazioni sui dispositivi plug-and-play (nome, descrizione, identificatore dispositivo [PnP, ACPI], informazioni sui dischi e sui dispositivi archiviazione (numero di dischi o unità flash, produttore, modello, capacità del disco, numero di cilindri, numero di tracce per cilindro, numero di settori per traccia, capacità settore, caratteristiche della cache, numero progressivo, numero di partizioni, configurazione del controller SCSI), informazioni sui dischi logici (numero sequenziale, capacità partizione, capacità volume, lettera volume, tipo di partizione, tipo di file system, numero di cluster, dimensioni cluster, numero di settori per cluster, numero di cluster vuoti e occupati, lettera del volume avviabile, indirizzo di offset della partizione in relazione all'avvio del disco), informazioni sulla scheda madre BIOS (produttore, data di rilascio, versione), informazioni sulla scheda madre (produttore, modello, tipo), informazioni sulla memoria fisica (capacità condivisa e disponibile), informazioni sui servizi del sistema operativo (nome, descrizione, stato, tag, informazioni sui processi [nome e PID]), parametri di consumo energetico per il Computer, configurazione del controller di interrupt, percorso delle cartelle di sistema Windows (Windows e System32), informazioni sul sistema operativo (versione, build, data di rilascio, nome, tipo, data di installazione), dimensioni del file di paging, informazioni sui monitor (numero, produttore, autorizzazione dello schermo, capacità di risoluzione, tipo), informazioni sul driver della scheda video (produttore, data di rilascio, versione);

- informazioni provenienti da ETW, fornitori di eventi EventTrace / EventMetadata di Microsoft: informazioni sulla sequenza degli eventi di sistema (tipo, ora, data, fuso orario), metadati relativi al file con i risultati del tracciamento (nome struttura, parametri di tracciamento, suddivisione del numero di operazioni di tracciamento in base al tipo), informazioni sul sistema operativo (nome, tipo, versione, build, data di rilascio, ora di inizio);

- informazioni provenienti da ETW, fornitori di eventi Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power di Microsoft: informazioni sui processi avviati e completati (nome, PID, parametri di avvio, riga di comando, codice di reso, parametri di risparmio energia, ora di avvio e completamento, tipo di token di accesso, SID, SessionID, numero di descrittori installati), informazioni sulle modifiche apportate alle priorità del thread (TID, priorità, ora), informazioni sulle operazioni disco del processo (tipo, ora, capacità, numero), cronologia delle modifiche alla struttura e capacità dei processi di memoria utilizzabili;

- informazioni provenienti da ETW, fornitori di eventi StackWalk / Perfinfo di Microsoft: informazioni sui contatori delle prestazioni (prestazioni delle singole sezioni di codice, sequenza delle chiamate di funzione, PID, TID, indirizzi e attributi di ISR e DPC);

- informazioni provenienti da ETW, fornitore di eventi KernelTraceControl-ImageID di Microsoft: informazioni sui file eseguibili e sulle librerie dinamiche (nome, dimensioni immagine, percorso completo), informazioni sui file PDB (nome, identificatore), dati risorse VERSIONINFO per i file eseguibili (nome, descrizione, creatore, localizzazione, versione applicazione e identificatore, versione del file e identificatore);

- informazioni provenienti da ETW, fornitori di eventi FileIo / DiskIo / Image / Windows Kernel Disk di Microsoft: informazioni sulle operazioni file e disco (tipo, capacità, ora di inizio, ora di completamento, durata, stato di completamento, PID, TID, indirizzi chiamate di funzione driver, IRP (I/O Request Packet), attributi dell'oggetto file Windows), informazioni sui file coinvolti nelle operazioni file e disco (nome, versione, dimensioni, percorso completo, attributi, offset, checksum immagine, opzioni di apertura e accesso);

- informazioni provenienti da ETW, fornitore di eventi PageFault di Microsoft: informazioni sugli errori di accesso alla pagina di memoria (indirizzo, ora, capacità, PID, TID, attributi dell'oggetto file Windows, parametri di allocazione della memoria);

- informazioni provenienti da ETW, fornitore degli eventi Thread di Microsoft: informazioni su creazione/completamento thread, informazioni sui thread avviati (PID, TID, dimensioni stack, priorità e allocazione delle risorse della CPU, risorse I/O, pagine di memoria fra i thread, indirizzo stack, indirizzo della funzione init, indirizzo di TEB (Thread Environment Block), tag di servizio Windows);

- informazioni provenienti da ETW, fornitore degli eventi Microsoft Windows Kernel Memory di Microsoft: informazioni sulle operazioni di gestione della memoria (stato di completamento, ora, quantità, PID), struttura di allocazione della memoria (tipo, capacità, SessionID, PID);

- informazioni sul funzionamento del software in caso di problemi di prestazioni: identificatore di installazione del Software, tipo e valore del calo delle prestazioni, informazioni sulla sequenza di eventi all'interno del Software (ora, fuso orario, tipo, stato di completamento, identificatore componente Software, identificatore dello scenario operativo del Software, TID, PID, indirizzi chiamate di funzione), informazioni sulle connessioni di rete da verificare (URL, direzione della connessione, dimensioni del pacchetto di rete), informazioni sui file PDB (nome, identificatore, dimensioni immagine del file eseguibile), informazioni sui file da verificare (nome, percorso completo, checksum), parametri di monitoraggio delle prestazioni del Software;

- informazioni sull'ultimo riavvio non riuscito del sistema operativo: numero di riavvii non andati a buon fine dall'installazione del sistema operativo, dati sul dump del sistema (codice e parametri di un errore, nome, versione e checksum (CRC32) del modulo che ha causato un errore nell'esecuzione del sistema operativo, indirizzo dell'errore come offset nel modulo, checksum (MD5, SHA2-256, SHA1) del dump di sistema);

- informazioni per verificare l'autenticità dei certificati digitali utilizzati per firmare i file: impronta digitale del certificato, algoritmo checksum, chiave pubblica del certificato e numero di serie, nome dell'emittente del certificato, risultato della convalida del certificato e identificatore di database del certificato;

- informazioni sul processo che esegue l'attacco contro l'auto-difesa del Software: nome e dimensioni del file del processo, relativi checksum (MD5, SHA2-256, SHA1), percorso completo del file del processo e codice del modello di percorso file, timestamp di creazione/build, contrassegno del file eseguibile, attributi del file di processo, informazioni sul certificato utilizzato per firmare il file di processo, codice dell'account utilizzato per avviare il processo, ID delle operazioni eseguite per l'accesso al processo, tipo di risorsa con cui viene eseguita l'operazione (processo, file, oggetto del Registro di sistema, funzione di ricerca FindWindow), nome della risorsa con cui viene eseguita l'operazione, contrassegno di completamento dell'operazione, stato del file del processo e la relativa firma in base a KSN;

- informazioni sul Software del Titolare dei diritti: versione completa, tipo, localizzazione e stato operativo del Software utilizzato, versioni dei componenti Software installati e relativo stato operativo, informazioni sugli aggiornamenti Software installati, valore del filtro TARGET, versione del protocollo utilizzato per connettersi ai servizi del Titolare dei diritti;
- informazioni relative all'hardware installato nel Computer: tipo, nome, nome del modello, versione firmware, parametri dei dispositivi integrati e collegati, identificatore univoco del Computer in cui è installato il Software;
- informazioni sulle versioni del sistema operativo e sugli aggiornamenti installati, dimensioni parola, edizione e parametri della modalità di esecuzione del sistema operativo, versione e checksum (MD5, SHA2-256, SHA1) del file kernel del sistema operativo e data e ora di avvio del sistema operativo;
- file eseguibili e non eseguibili, interamente o parzialmente;
- porzioni di RAM del computer;
- settori coinvolti nel processo di avvio del sistema operativo;
- pacchetti di dati relativi al traffico di rete;
- e-mail e pagine Web contenenti oggetti sospetti e dannosi;
- descrizione delle classi e delle istanze delle classi del repository WMI;
- rapporti sull'attività dell'applicazione:
  - il nome, la dimensione e la versione del file inviato, la relativa descrizione e i checksum (MD5, SHA2-256, SHA1), l'identificatore del formato del file, il nome del fornitore del file, il nome del prodotto a cui appartiene il file, il percorso completo del file nel Computer, il codice modello del percorso, i timestamp di creazione e modifica del file;
  - data/ora di inizio e fine del periodo di validità del certificato (se il file dispone di una firma digitale), la data e l'ora della firma, il nome dell'emittente del certificato, informazioni sul titolare del certificato, l'impronta digitale, la chiave pubblica del certificato e gli algoritmi appropriati, nonché il numero di serie del certificato;
  - il nome dell'account dal quale è in esecuzione il processo;
  - checksum (MD5, SHA2-256, SHA1) del nome del Computer in cui è in esecuzione il processo;
  - titoli delle finestre dei processi;
  - identificativo per i database anti-virus, nome della minaccia rilevata secondo la classificazione del Titolare dei diritti;
  - dati sulla licenza installata, il relativo ID, il tipo e la data di scadenza;
  - ora locale del Computer al momento della fornitura delle informazioni;
  - nomi e percorsi dei file a cui ha avuto accesso il processo;
  - nomi delle chiavi del Registro di sistema e relativi valori a cui ha avuto accesso il processo;
  - URL e indirizzi IP a cui ha avuto accesso il processo;
  - URL e indirizzi IP da cui è stato scaricato il file in esecuzione.

Trasmissione dei dati quando si utilizzano le soluzioni Detection and Response

Nei computer in cui è installato Kaspersky Endpoint Security, vengono archiviati i dati preparati per l'invio automatico ai server di Kaspersky Endpoint Detection and Response, Kaspersky Sandbox e Kaspersky Anti Targeted Attack Platform. I file vengono archiviati nei computer in forma semplice e non criptata.

Il set di dati specifico dipende dalla soluzione all'interno della quale viene utilizzato Kaspersky Endpoint Security.

Kaspersky Endpoint Detection and Response

Tutti i dati che l'applicazione archivia in locale nel computer vengono eliminati dal computer quando Kaspersky Endpoint Security viene disinstallato.

Dati ricevuti dopo aver eseguito l'attività Scansione IOC (attività standard)

Kaspersky Endpoint Security invia automaticamente i dati sui risultati dell'esecuzione dell'attività *Scansione IOC* a Kaspersky Security Center.

I dati nei risultati dell'esecuzione dell'attività *Scansione IOC* possono contenere le seguenti informazioni:

- Indirizzo IP dalla tabella ARP
- Indirizzo fisico dalla tabella ARP
- Tipo e nome del record DNS
- Indirizzo IP del computer protetto
- Indirizzo fisico (indirizzo MAC) del computer protetto
- Identificatore nella voce del registro eventi
- Nome dell'origine dati nel registro
- Nome log
- Ora dell'evento
- Hash MD5 e SHA256 del file
- Nome completo del file (incluso il percorso)
- Dimensione del file
- Indirizzo IP remoto e porta con cui è stata stabilita la connessione durante la scansione

- Indirizzo IP della scheda locale
- Porta aperta sulla scheda locale
- Protocollo come numero (secondo lo standard IANA)
- Nome del processo
- Argomenti di processo
- Percorso del file di processo
- Identificatore di Windows (PID) del processo
- Identificatore di Windows (PID) del processo entità superiore
- Account utente che ha avviato il processo
- Data e ora in cui è stato avviato il processo
- Nome servizio
- Descrizione del servizio
- Percorso e nome del servizio DLL (per svchost)
- Percorso e nome del file eseguibile del servizio
- Identificatore di Windows (PID) del servizio
- Tipo di servizio (ad esempio, una scheda o un driver kernel)
- Stato del servizio
- Modalità di avvio del servizio
- Nome dell'account utente.
- Nome del volume
- Lettera del volume
- Tipo di volume
- Valore del Registro di sistema di Windows
- Valore hive del Registro di sistema
- Percorso della chiave del Registro di sistema (senza hive e nome del valore)
- Impostazione del Registro di sistema
- Sistema (ambiente)
- Nome e versione del sistema operativo installato nel computer

- Nome della rete del computer protetto
- Dominio o gruppo a cui appartiene il computer protetto
- Nome del browser
- Versione del browser
- L'ora dell'ultimo accesso alla risorsa Web
- URL dalla richiesta HTTP
- Nome dell'account utilizzato per la richiesta HTTP
- Nome file del processo che ha effettuato la richiesta HTTP
- Percorso completo del file del processo che ha effettuato la richiesta HTTP
- Identificatore di Windows (PID) del processo che ha effettuato la richiesta HTTP
- Provenienza HTTP (URL di origine della richiesta HTTP)
- URI della risorsa richiesta su HTTP
- Informazioni sull'agente utente HTTP (l'applicazione che ha effettuato la richiesta HTTP)
- Ora di esecuzione della richiesta HTTP
- Identificatore univoco del processo che ha effettuato la query HTTP

Dati per la creazione di una catena di sviluppo delle minacce

I dati per la creazione di una catena di sviluppo delle minacce vengono archiviati per sette giorni per impostazione predefinita. I dati vengono inviati automaticamente a Kaspersky Security Center.

I dati per la creazione di una catena di sviluppo delle minacce possono contenere le seguenti informazioni:

- Data e ora dell'incidente
- Nome del rilevamento
- Modalità di scansione
- Stato dell'ultima azione correlata al rilevamento
- Motivo per cui l'elaborazione del rilevamento non è riuscita
- Tipo di oggetto rilevato
- Nome dell'oggetto rilevato
- Stato della minaccia dopo l'elaborazione dell'oggetto

- Motivo per cui l'esecuzione delle azioni sull'oggetto non è riuscita
- Azioni eseguite per il rollback delle azioni dannose
- Informazioni sull'oggetto elaborato:
  - Identificatore univoco del processo
  - Identificatore univoco del processo entità superiore
  - Identificatore univoco del file di processo
  - Identificatore di processo di Windows (PID)
  - Riga di comando del processo
  - Account utente che ha avviato il processo
  - Codice della sessione di accesso in cui è in esecuzione il processo
  - Tipo di sessione in cui è in esecuzione il processo
  - Livello di integrità del processo in elaborazione
  - Appartenenza dell'account utente che ha avviato il processo nei gruppi locali e di dominio con privilegi
  - Identificatore dell'oggetto elaborato
  - Nome completo dell'oggetto elaborato
  - Identificativo del dispositivo protetto
  - Nome completo dell'oggetto (nome del file locale o indirizzo Web del file scaricato)
  - Hash MD5 o SHA256 dell'oggetto elaborato
  - Tipo dell'oggetto elaborato
  - Data di creazione dell'oggetto elaborato
  - Data dell'ultima modifica dell'oggetto elaborato
  - Dimensione dell'oggetto elaborato
  - Attributi dell'oggetto elaborato
  - Organizzazione che ha firmato l'oggetto elaborato
  - Risultato della verifica dei certificati digitali dell'oggetto elaborato
  - Identificatore di sicurezza (SID) dell'oggetto elaborato
  - Identificatore del fuso orario dell'oggetto elaborato
  - Indirizzo Web del download dell'oggetto processato (solo per file su disco)

- Nome dell'applicazione che ha scaricato il file
- Hash MD5 e SHA256 dell'applicazione che ha scaricato il file
- Nome dell'ultima applicazione che ha modificato il file
- Hash MD5 e SHA256 dell'ultima applicazione che ha modificato il file
- Numero di avviamenti di oggetti elaborati
- Data e ora in cui l'oggetto elaborato è stato avviato per la prima volta
- Identificatori univoci del file
- Nome completo del file (nome file locale o indirizzo Web del file scaricato)
- Percorso della variabile elaborata del Registro di sistema di Windows
- Nome della variabile elaborata del Registro di sistema di Windows
- Valore della variabile elaborata del Registro di sistema di Windows
- Tipo della variabile elaborata del Registro di sistema di Windows
- Indicatore dell'appartenenza alla chiave del Registro di sistema elaborata nel punto di esecuzione automatica
- Indirizzo Web della richiesta Web elaborata
- Origine del collegamento della richiesta Web elaborata
- Agente utente della richiesta Web elaborata
- Tipo della richiesta Web elaborata (`GET` o `POST`)
- Porta IP locale della richiesta Web elaborata
- Porta IP remota della richiesta Web elaborata
- Direzione della connessione (in entrata o in uscita) della richiesta Web elaborata
- Identificatore del processo in cui è stato incorporato il codice dannoso

Kaspersky Sandbox

Tutti i dati che l'applicazione archivia in locale nel computer vengono eliminati dal computer quando Kaspersky Endpoint Security viene disinstallato.

Dati di servizio

Kaspersky Endpoint Security archivia i seguenti dati elaborati durante la risposta automatica:

- File elaborati e dati immessi dall'utente durante la configurazione dell'agente integrato di Kaspersky Endpoint Security:
  - File in quarantena
  - Chiave pubblica del certificato utilizzato per l'integrazione con Kaspersky Sandbox
- Cache dell'agente integrato di Kaspersky Endpoint Security:
  - Ora in cui i risultati della scansione sono stati scritti nella cache
  - Hash MD5 dell'attività di scansione
  - Identificatore dell'attività di scansione
  - Risultato della scansione per l'oggetto
- Coda delle richieste di scansione dell'oggetto:
  - ID dell'oggetto nella coda
  - Ora in cui l'oggetto è stato inserito nella coda
  - Stato di elaborazione dell'oggetto in coda
  - ID della sessione utente nel sistema operativo in cui è stata creata l'attività di scansione dell'oggetto
  - Identificatore di sistema (SID) dell'utente del sistema operativo il cui account è stato usato per creare l'attività
  - Hash MD5 dell'attività di scansione dell'oggetto
- Informazioni sulle attività per le quali l'agente integrato di Kaspersky Endpoint Security attende i risultati della scansione da Kaspersky Sandbox:
  - Ora in cui è stata ricevuta l'attività di scansione dell'oggetto
  - Stato di elaborazione dell'oggetto
  - ID della sessione utente nel sistema operativo in cui è stata creata l'attività di scansione dell'oggetto
  - Identificatore dell'attività di scansione dell'oggetto
  - Hash MD5 dell'attività di scansione dell'oggetto
  - Identificatore di sistema (SID) dell'utente del sistema operativo il cui account è stato usato per creare l'attività
  - Schema XML dell'IOC creato automaticamente

- Hash MD5 o SHA256 dell'oggetto sottoposto a scansione
- Errori di elaborazione
- Nomi degli oggetti per i quali è stata creata l'attività
- Risultato della scansione per l'oggetto

Dati nelle richieste a Kaspersky Sandbox

I seguenti dati delle richieste dall'agente integrato di Kaspersky Endpoint Security a Kaspersky Sandbox vengono archiviati in locale nel computer:

- Hash MD5 dell'attività di scansione
- Identificatore dell'attività di scansione
- Oggetto sottoposto a scansione e tutti i file correlati

Dati ricevuti dopo aver eseguito l'attività Scansione IOC (attività standalone)

Kaspersky Endpoint Security invia automaticamente i dati sui risultati dell'esecuzione dell'attività *Scansione IOC* a Kaspersky Security Center.

I dati nei risultati dell'esecuzione dell'attività *Scansione IOC* possono contenere le seguenti informazioni:

- Indirizzo IP dalla tabella ARP
- Indirizzo fisico dalla tabella ARP
- Tipo e nome del record DNS
- Indirizzo IP del computer protetto
- Indirizzo fisico (indirizzo MAC) del computer protetto
- Identificatore nella voce del registro eventi
- Nome dell'origine dati nel registro
- Nome log
- Ora dell'evento
- Hash MD5 e SHA256 del file
- Nome completo del file (incluso il percorso)
- Dimensione del file

- Indirizzo IP remoto e porta con cui è stata stabilita la connessione durante la scansione
- Indirizzo IP della scheda locale
- Porta aperta sulla scheda locale
- Protocollo come numero (secondo lo standard IANA)
- Nome del processo
- Argomenti di processo
- Percorso del file di processo
- Identificatore di Windows (PID) del processo
- Identificatore di Windows (PID) del processo entità superiore
- Account utente che ha avviato il processo
- Data e ora in cui è stato avviato il processo
- Nome servizio
- Descrizione del servizio
- Percorso e nome del servizio DLL (per svchost)
- Percorso e nome del file eseguibile del servizio
- Identificatore di Windows (PID) del servizio
- Tipo di servizio (ad esempio, una scheda o un driver kernel)
- Stato del servizio
- Modalità di avvio del servizio
- Nome dell'account utente.
- Nome del volume
- Lettera del volume
- Tipo di volume
- Valore del Registro di sistema di Windows
- Valore hive del Registro di sistema
- Percorso della chiave del Registro di sistema (senza hive e nome del valore)
- Impostazione del Registro di sistema
- Sistema (ambiente)

- Nome e versione del sistema operativo installato nel computer
- Nome della rete del computer protetto
- Dominio o gruppo a cui appartiene il computer protetto
- Nome del browser
- Versione del browser
- L'ora dell'ultimo accesso alla risorsa Web
- URL dalla richiesta HTTP
- Nome dell'account utilizzato per la richiesta HTTP
- Nome file del processo che ha effettuato la richiesta HTTP
- Percorso completo del file del processo che ha effettuato la richiesta HTTP
- Identificatore di Windows (PID) del processo che ha effettuato la richiesta HTTP
- Provenienza HTTP (URL di origine della richiesta HTTP)
- URI della risorsa richiesta su HTTP
- Informazioni sull'agente utente HTTP (l'applicazione che ha effettuato la richiesta HTTP)
- Ora di esecuzione della richiesta HTTP
- Identificatore univoco del processo che ha effettuato la query HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

Tutti i dati che l'applicazione archivia in locale nel computer vengono eliminati dal computer quando Kaspersky Endpoint Security viene disinstallato.

Dati di servizio

L'agente integrato di Kaspersky Endpoint Security archivia in locale i seguenti dati:

- Dati richiesti per l'integrazione con il componente EDR Expert (on-premises):
  - Indirizzo e porta per la connessione al server KATA Central Node
  - Indirizzo e porta per la connessione al server di trasmissione della telemetria
  - Indirizzo e porta per la connessione al server di risposta

    - Informazioni sui certificati utilizzati per l'integrazione con KATA Central Node
    - Informazioni sui certificati utilizzati per l'integrazione con il server di trasmissione della telemetria
    - Informazioni sui certificati utilizzati per l'integrazione con il server di risposta
- File in quarantena

Dati provenienti dagli eventi di telemetria trasmessi

- **Dati di telemetria**
    - Dati sui file:
        - Identificatori univoci del file
        - Tipo di file
        - Percorso completo del file
        - Dimensione del file
        - Attributi del file
        - Identificatore di zona
        - Data e ora di creazione del file
        - Data e ora dell'ultima modifica del file
        - Nome originale del file
        - Nome dell'applicazione
        - Versione dell'applicazione.
        - Fornitore dell'applicazione
        - Descrizione del file
        - Versione del file.
        - Hash MD5 e SHA256 dell'oggetto
        - Risultato della verifica della firma del file
        - Nome dell'emittente del certificato
        - Nome del titolare del certificato
        - Numero di serie del certificato

- Dati sulla scansione AMSI:
  - Identificatore univoco del processo che ha avviato l'attività
  - Tipo di contenuto dell'oggetto passato ad AMSI
  - Contenuto dell'oggetto passato ad AMSI
  - Nome dell'oggetto
  - Hash MD5 e SHA256 dell'oggetto
- Dati sul blocco delle applicazioni:
  - Identificatore univoco del processo che ha avviato il blocco dell'applicazione
  - Identificatore univoco del processo entità superiore
  - Identificatore di sistema univoco del processo
  - Comando utilizzato per avviare un processo
  - ID della sessione di accesso
  - Livello di integrità del processo
  - Stato del processo
  - Identificatore univoco del file di processo
  - Riga di comando del processo
  - Elenco di identificatori univoci dei file interpretati
- Dati sulle aperture dei file bloccati:
  - Identificatore univoco del processo che ha avviato l'apertura del file
  - Identificatori univoci del file
- Dati sul caricamento del driver:
  - Identificatore univoco del driver caricato
- Dati sugli eventi:
  - Identificatore univoco dell'evento
  - Data e ora dell'evento
- Dati sulla modifica del file:
  - Identificatore univoco del processo che ha avviato la modifica del file
  - Identificatori univoci del file

- Tipo di operazione di modifica
- Contrassegno che indica che il file verrà eliminato dopo il riavvio del computer
- Identificatore univoco del file modificato
- Identificatore univoco del file prima della modifica
- Set di contrassegni di bit che determinano il modo in cui il file è stato aperto
- Dati sulle operazioni nell'elenco di controllo degli accessi
- Dati sulle modifiche apportate alla proprietà o al gruppo principale del file

- Dati sulla sessione di accesso:
  - ID della sessione di accesso
  - Nome dell'utente che ha effettuato l'accesso
  - Tipo di account utente
  - Tipo di sessione
- Dati sulle connessioni di rete:
  - Identificatore univoco del processo che ha avviato la connessione
  - Indirizzo IP locale utilizzato per avviare la connessione
  - Indirizzo IP remoto dell'endpoint di connessione
  - Direzione di connessione
  - Protocollo di trasferimento dati
  - Metodo HTTP
  - Percorso senza il nome host
  - Nome host
  - Stato del processo dinamico al momento della connessione
  - Contrassegno che indica che la connessione è aperta a livello di socket non elaborato
  - Versione di TLS utilizzata nella sessione di connessione
  - Nome del server TLS
  - Hash MD5 e SHA1 del certificato del server TLS
  - Elenco dei Subject Alternative Name (SAN) del certificato
  - Nome dell'emittente del certificato TLS

    - Numero di serie del certificato
    - Algoritmo di criptaggio utilizzato
    - Date di inizio e fine del certificato
    - Impronta digitale JA3 del client TLS
    - Impronta digitale JA3S del server
- Dati acquisiti durante l'ascolto su una porta di rete:
    - Identificatore univoco del processo che ha avviato la connessione
- Dati di input della riga di comando:
    - Identificatore univoco del processo che ha avviato l'input della console
    - Tipo di input della console
    - Testo immesso da un utente o da un processo
- Dati sulla creazione del processo:
    - Identificatore univoco del processo
    - Identificatore univoco del processo entità superiore
    - Identificatore di sistema univoco del processo
    - Comando utilizzato per avviare un processo
    - ID della sessione di accesso
    - Livello di integrità del processo
    - Identificatore univoco del file di processo
    - Elenco di identificatori univoci dei file interpretati
    - Tipo di processo
- Dati sul modulo caricato dal processo:
    - Identificatore univoco del processo che ha avviato il download
    - Percorso completo del file che è stato caricato nel processo
    - Identificatore univoco del file del modulo
    - Nome completo dell'assembly .NET, se il file caricato è un modulo .NET
    - Contrassegini dell'assembly .NET definito nel relativo manifest

- Dati sull'interruzione del processo:
  - Identificatore univoco del processo terminato
- Dati sulla modifica del Registro di sistema:
  - Identificatore univoco del processo che ha avviato la modifica del Registro di sistema
  - Tipo di operazione del Registro di sistema
  - Percorso completo della chiave del Registro di sistema
  - Nome del valore in una chiave del Registro di sistema
  - Tipo di dati archiviati nel valore della chiave del Registro di sistema
  - Dati specificati nel valore della chiave del Registro di sistema
  - Nome della chiave prima della ridenominazione
  - Informazioni relative a una modifica della proprietà della chiave o del gruppo di chiavi primario
  - Elenco delle modifiche apportate all'elenco di controllo degli accessi (ACL) della chiave
- Dati sulla minaccia rilevata e sulla relativa elaborazione:
  - Contrassegno che indica che il rilevamento delle minacce è stato eseguito in background
  - Verdetto minaccia
  - Nome del verdetto
  - Identificatore univoco del record del database
  - Ora in cui il record della minaccia è stato salvato nel database
  - Modalità di elaborazione della minaccia
  - Tipo di oggetto infetto
  - Nome dell'oggetto infetto
  - Hash MD5 e SHA256 dell'oggetto
  - Identificatore univoco dell'oggetto infetto
  - Identificatore univoco del processo che ha scaricato l'oggetto infetto da Internet
  - URL da cui è stato scaricato l'oggetto infetto
  - Indirizzo e-mail del mittente che ha inviato l'oggetto infetto
  - Protocollo di rete tramite il quale è stato ricevuto l'oggetto infetto
  - Indirizzo locale da cui è stato ricevuto l'oggetto infetto

    - Indirizzo esterno da cui è stato ricevuto l'oggetto infetto
    - Tipo di contenuto dell'oggetto
    - Contenuto dell'oggetto
- Dati sull'accesso ai processi:
    - Identificatore univoco del processo che ha tentato l'accesso
    - Identificatore univoco del processo di destinazione a cui è stato eseguito l'accesso
    - Set di diritti richiesti dal processo di destinazione
    - Tipo di operazione
    - Set di chiamate al momento dell'accesso a un processo
    - Descrittore del processo di origine
    - Descrittore di processo di destinazione
- Dati sul DNS:
    - Identificatore univoco del processo che ha avviato la query DNS
    - Indirizzo IP del server DNS
    - Contrassegni che gestiscono il comportamento di una query DNS
    - Stato di completamento della richiesta
    - Nome di dominio completo specificato nella query DNS
    - Tipo di dati nella query DNS
    - Risposte del server DNS
- Dati sull'inoculazione del codice:
    - Identificatore univoco del processo che ha tentato di inoculare il codice
    - Metodo di accesso utilizzato
    - Set di chiamate nel momento in cui è stato rilevato il codice inoculato
    - Identificatore univoco del processo di destinazione in cui è stato caricato il codice
    - Dati sulle modifiche nella sequenza di comandi del processo di destinazione
    - Indirizzo del processo di destinazione
    - Nome della libreria DLL caricata nel processo di destinazione
    - Percorso completo del file DDL

- Dati sulle operazioni con i canali denominati:
  - Identificatore univoco del processo che ha creato o si è connesso al canale
  - Nome completo del canale denominato
  - Tipo di operazione (creazione o connessione)
- Dati sulle query WMI:
  - Identificatore univoco del processo che ha avviato l'operazione WMI
  - Tipo di operazione WMI
  - Nome del dispositivo di destinazione per la query WMI
  - Account utente che ha avviato la query WMI
  - Testo della query WMI
  - Spazio dei nomi in cui viene eseguita la query WMI
  - Nome del filtro WMI
  - Nome dell'oggetto consumer
  - Testo che descrive l'azione dell'oggetto consumer
- Dati sulle query LDAP:
  - Identificatore univoco del processo che ha effettuato la query LDAP
  - Ambito di ricerca delle query LDAP
  - Filtro LDAP
  - Parametro che specifica la partizione di Active Directory a cui è stata indirizzata la query
  - Attributi di ricerca LDAP
- Dati sui dispositivi USB connessi:
  - Tipo di operazione del dispositivo USB
  - Tipo di dispositivo USB
  - Identificativo del dispositivo USB
  - Nome del dispositivo USB
  - Percorso del dispositivo USB
  - Contrassegno che indica che il dispositivo USB è un'unità di sistema
- Dati sulla creazione, l'eliminazione e la modifica di un'attività pianificata

- Dati sulla creazione, l'eliminazione e la modifica dei servizi
- Dati sul montaggio/smontaggio del file system
- Dati sul funzionamento del componente EDR Expert on-premise:
  - Informazioni sull'avvio/arresto dell'agente
  - Informazioni sull'installazione/disinstallazione dell'agente
  - Identificatore univoco per l'avvio dell'agente
  - Identificatore di sistema del processo dell'agente
  - Identificatore univoco del processo dell'agente
  - Motivo dell'interruzione dell'agente
  - Codice di interruzione del processo dell'agente

- Impostazioni di filtraggio degli eventi:
  - Nomi dei moduli
  - Percorsi completi degli oggetti
  - Hash MD5 e SHA256 degli oggetti
  - Identificatori delle voci nel registro eventi di Windows
  - Impostazioni dei certificati digitali
  - Direzione del traffico, indirizzi IP, porte, protocolli, percorsi completi dei file eseguibili
  - Nomi utente
  - Tipi di accesso utente
  - Tipi di eventi di telemetria per i quali vengono applicati i filtri

Dati dalle richieste del componente EDR Expert all'agente integrato di Kaspersky Endpoint Security

- Impostazioni attività generali:
  - Tipo di attività
  - Impostazioni di pianificazione delle attività
  - Nomi e password degli account con cui è possibile eseguire le attività
  - Versioni delle impostazioni

- Identificatori di oggetti in quarantena
- Percorsi degli oggetti
- Hash MD5 e SHA256 degli oggetti
- Riga di comando per avviare il processo con gli argomenti
- Contrassegni delle azioni aggiuntive eseguite al completamento delle attività
- Identificatori dei file IOC da recuperare dal server
- File IOC
- Nome servizio
- Tipo di avvio del servizio
- Cartelle per cui devono essere ricevuti i risultati dell'attività di *recupero dei dati forensi*
- Maschere dei nomi e delle estensioni degli oggetti per l'attività di *recupero dei dati forensi*

- Impostazioni dell'isolamento di rete:
  - Tipi di impostazioni
  - Versioni delle impostazioni
  - Elenchi di esclusioni dell'isolamento di rete e impostazioni di esclusione: direzione del traffico, indirizzi IP, porte, protocolli e percorsi completi dei file eseguibili
  - Contrassegni delle azioni aggiuntive
  - Ora di disabilitazione dell'isolamento automatico
- Impostazioni di Prevenzione dell'esecuzione:
  - Tipi di impostazioni
  - Versioni delle impostazioni
  - Elenchi di regole di prevenzione dell'esecuzione e impostazioni delle regole: percorsi degli oggetti, tipi di oggetti, hash MD5 e SHA256 degli oggetti
  - Contrassegni delle azioni aggiuntive

Dati provenienti dalle richieste inviate da Kaspersky Endpoint Security al componente EDR Expert

Durante l'integrazione con la soluzione EDR Expert (on-premises), i seguenti dati vengono archiviati in locale nei computer.

- Nelle richieste di sincronizzazione:
  - ID univoco
  - Parte di base dell'indirizzo Web del server
  - Nome del computer
  - Indirizzo IP del computer
  - Indirizzo MAC del computer
  - Ora locale sul computer
  - Stato di Auto-difesa di Kaspersky Endpoint Security
  - Nome e versione del sistema operativo installato nel computer
  - Versione di Kaspersky Endpoint Security
  - Versioni delle impostazioni dell'applicazione e delle impostazioni delle attività
  - Stati delle attività: identificatori delle attività, stati di esecuzione, codici di errore
- Nelle richieste di recupero di file dal server:
  - Identificatori univoci dei file
  - Identificatore univoco di Kaspersky Endpoint Security
  - Identificatori univoci dei certificati
  - Parte di base dell'indirizzo Web del server con il componente Central Node installato
  - Indirizzo IP dell'host
- Nei rapporti sui risultati dell'esecuzione delle attività:
  - Indirizzo IP dell'host
  - Informazioni sugli oggetti rilevati durante una scansione IOC o YARA
  - Contrassegni delle azioni aggiuntive eseguite al completamento delle attività
  - Errori di esecuzione delle attività e codici restituiti
  - Stati di completamento delle attività

- Ora di completamento delle attività
- Versioni delle impostazioni utilizzate per l'esecuzione delle attività
- Informazioni sugli oggetti inviati al server, oggetti in quarantena e oggetti ripristinati dalla quarantena: percorsi degli oggetti, hash MD5 e SHA256, identificatori degli oggetti in quarantena
- Informazioni sui processi avviati o arrestati in un computer su richiesta del server: PID e UniquePID, codice di errore, hash MD5 e SHA256 degli oggetti
- Informazioni sui servizi avviati o arrestati in un computer su richiesta del server: nome del servizio, tipo di avvio, codice di errore, hash MD5 e SHA256 delle immagini dei file dei servizi
- Informazioni sugli oggetti per i quali è stato creato un dump della memoria per una scansione YARA (percorsi, identificatore del file dump)
- File richiesti dal server

- Dati sui processi in esecuzione:
  - Nome del file eseguibile, incluso il percorso completo e l'estensione
  - Parametri di esecuzione automatica dei processi
  - ID processo
  - ID della sessione di accesso
  - Nome della sessione di accesso
  - Data e ora in cui è stato avviato il processo
  - Hash MD5 e SHA256 dell'oggetto
- Dati sui file:
  - Percorso del file
  - Nome file.
  - Dimensione del file
  - Attributi del file
  - Data e ora di creazione del file
  - Data e ora dell'ultima modifica del file
  - Descrizione del file
  - Nome dell'azienda
  - Hash MD5 e SHA256 dell'oggetto
  - Chiave del Registro di sistema (per i punti di esecuzione automatica)

- Dati negli errori che si verificano quando sono state recuperate le informazioni sugli oggetti:
  - Nome completo dell'oggetto che è stato elaborato quando si è verificato un errore
  - Codice di errore
- Dati nei risultati della scansione YARA:

  L'agente integrato di Kaspersky Endpoint Security trasferisce automaticamente i risultati della scansione YARA a Kaspersky Anti Targeted Attack Platform per creare una catena di sviluppo delle minacce.

  I dati vengono archiviati temporaneamente in locale nella coda per l'invio dei risultati dell'esecuzione dell'attività al server di Kaspersky Anti Targeted Attack Platform. I dati vengono eliminati dalla memoria temporanea una volta inviati.
  - Hash MD5 e SHA256 del file
  - Nome completo del file
  - Percorso del file
  - Dimensione del file
  - Nome del processo
  - Argomenti di processo
  - Percorso del file di processo
  - Identificatore di Windows (PID) del processo
  - Identificatore di Windows (PID) del processo entità superiore
  - Account utente che ha avviato il processo
  - Data e ora in cui è stato avviato il processo
- Dati nei risultati della scansione IOC:
  - Indirizzo IP dalla tabella ARP
  - Indirizzo fisico dalla tabella ARP
  - Nome del record DNS
  - Tipo di record DNS
  - Nome host
  - Indirizzo IP
  - ID evento nel registro
  - Nome dell'origine dati nel registro
  - Nome log

- Nome utente
- Data e ora in cui è stato generato l'evento, in formato ISO
- Hash MD5 e SHA256 del file
- Nome completo del file
- Dimensione del file
- Indirizzo IP remoto e porta con cui è stata stabilita la connessione durante la scansione
- Indirizzo IP e porta della scheda locale
- Protocollo
- Nome del processo
- Argomenti di processo
- Percorso del file di processo
- Identificatore di Windows (PID) del processo
- Identificatore di Windows (PID) del processo entità superiore
- Account utente che ha avviato il processo
- Data e ora in cui è stato avviato il processo
- Percorso della chiave del Registro di sistema
- Nome della chiave del Registro di sistema
- Valore di testo della chiave del Registro di sistema
- Nome servizio
- Descrizione del servizio
- Percorso e nome del servizio DLL
- Percorso e nome del file eseguibile del servizio
- Identificatore di Windows (PID) del servizio
- Tipo di servizio
- Stato del servizio
- Modalità di avvio del servizio
- Nome del sistema operativo
- Versione del sistema operativo

- Nome di rete del computer senza dominio
- Dominio o gruppo di lavoro
- Nome utente
- Nome del volume
- Lettera del volume
- Tipo di volume

Kaspersky Network Detection and Response (KATA)

Tutti i dati che l'applicazione archivia in locale nel computer vengono eliminati dal computer quando Kaspersky Endpoint Security viene disinstallato.

Dati di telemetria

- **Dati sui file**
  - Identificatori univoci del file
  - Tipo di file
  - Percorso completo del file
  - Dimensione del file
  - Attributi del file
  - Identificatore di zona
  - Data e ora di creazione del file
  - Data e ora dell'ultima modifica del file
  - Nome originale del file
  - Nome dell'applicazione
  - Versione dell'applicazione.
  - Fornitore dell'applicazione
  - Descrizione del file
  - Versione del file.

- Hash MD5 e SHA256 dell'oggetto
- Risultato della verifica della firma del file
- Data e ora di creazione della firma del file
- Catene di certificati utilizzate nel file della firma
- Tipo di catena di certificati
- Certificati nella catena
- Nome dell'emittente del certificato
- Nome del titolare del certificato
- Numero di serie del certificato
- Algoritmo di identificazione personale del certificato
- Identificazione personale del certificato
- Periodo di validità del certificato

- **Dati sulla sessione di accesso**
  - ID della sessione di accesso
  - Nome dell'account dell'utente che ha effettuato l'accesso
  - Tipo di account utente
  - Tipo di sessione
  - Indirizzo IP del computer da cui è stato effettuato il tentativo di accesso
  - Indirizzo IP del computer locale per cui è stato effettuato il tentativo di accesso
  - Contrassegno che indica che la sessione rappresentata da questo evento dispone di privilegi elevati e diritti amministrativi
  - Parametro che indica se altre sessioni sono collegate a questa sessione di accesso
  - Protocollo utilizzato per la sessione del terminale
  - Protocollo IPv4 utilizzato per la sessione del terminale
- **Dati sulla comunicazione di rete**
  - Inizio e fine dell'intervallo di tempo in cui sono stati raccolti i dati
  - Elenco delle connessioni
  - Indirizzo IP locale del computer

- Indirizzo MAC locale del computer
- Indirizzo IP remoto del computer
- Indirizzo MAC remoto del computer
- Indirizzo IP del gateway
- Numero di pacchetti di dati trasmessi
- Numero di pacchetti di dati ricevuti
- Numero totale di byte trasferiti
- Protocollo di trasferimento dati
- Campo EtherType frame Ethernet
- Prefisso del payload del primo pacchetto dell'intervallo
- Indirizzo IPv4 dell'interfaccia di rete tramite la quale è stata acquisita la comunicazione

- **Dati sulla connessione di rete**
  - Identificatore univoco del processo che ha avviato la connessione
  - Protocollo di trasferimento dati
  - Indirizzo IP locale utilizzato per avviare la connessione
  - Indirizzo IP remoto dell'endpoint di connessione
  - Metodo HTTP
  - Percorso senza il nome host
  - Nome host
  - Stato del processo dinamico al momento della connessione
  - Direzione di connessione
  - Stato del processo dinamico
  - Campo EtherType frame Ethernet
- **Dati acquisiti durante l'ascolto su una porta di rete**
  - Identificatore univoco del processo che ha avviato la connessione
  - Protocollo di trasferimento dati
  - Indirizzo locale
  - Stato del processo dinamico al momento della connessione

- **Risultato della verifica della connessione**
  - Impostazioni di rete dell'host
  - Descrizione dell'interfaccia di rete
  - Nome di dominio DNS
  - Indirizzo MAC locale del computer
  - Numero della metrica della connessione IP
  - Elenco di indirizzi IP
  - Indirizzo IP
  - Maschera di rete
  - Indirizzo IP del gateway
  - Indirizzo MAC del gateway
  - Elenco delle patch installate
  - Numero di patch
  - Data di installazione della patch
  - Modello di dispositivo
  - Fornitore del dispositivo
  - ID host in Kaspersky Security Center
  - Descrizione dell'antivirus Kaspersky installato
  - Nome del componente dell'antivirus Kaspersky installato
  - Versione del componente dell'antivirus Kaspersky installato
  - Versione del database del componente antivirus Kaspersky installato
  - Data dell'ultimo aggiornamento del database del componente antivirus Kaspersky installato
  - Stato del componente dell'antivirus Kaspersky installato
  - Elenco delle chiavi di licenza
  - Numero di serie della chiave
  - Tipo di chiave

- Data di scadenza della chiave
- Stato della chiave

- **Dati sulla creazione del processo nell'host**
  - Identificatore univoco del processo
  - Identificatore univoco del processo entità superiore
  - Identificatore di sistema univoco del processo
  - Comando utilizzato per avviare un processo
  - ID della sessione di accesso
  - ID della sessione del terminale
  - Identificatore univoco del file di processo
  - Livello di integrità del processo
  - Elenco dei token dei diritti del processo
  - Diritti degli attributi
  - Elenco di identificatori univoci dei file interpretati
  - Stato del processo
  - Comando utilizzato per avviare un processo
- **Dati sull'interruzione del processo**
  - Identificatore univoco del processo
- **Dati sulla minaccia rilevata**
  - Informazioni sulle minacce
  - Verdetto minaccia
  - Numero del record AMR
  - Versione del database antivirus
  - Modalità di rilevamento delle minacce
  - Identificatore univoco della minaccia
  - Tecnologia di protezione
  - Informazioni sull'oggetto infetto
  - Tipo di oggetto infetto

- Nome dell'oggetto infetto
- Hash MD5 e SHA256 dell'oggetto
- Identificatore univoco del processo infetto
- Identificatore univoco dell'oggetto infetto
- Identificatore univoco del processo che ha scaricato l'oggetto infetto da Internet
- URL da cui è stato scaricato l'oggetto infetto
- Indirizzo e-mail del mittente che ha inviato l'oggetto infetto
- Protocollo di rete tramite il quale è stato ricevuto l'oggetto infetto
- Indirizzo locale da cui è stato ricevuto l'oggetto infetto
- Indirizzo esterno da cui è stato ricevuto l'oggetto infetto
- Tipo di contenuto dell'oggetto
- Contesto della minaccia rilevata
- Contenuto dell'oggetto
- Contrassegno che indica che il rilevamento delle minacce è stato eseguito in background

- **Dati sull'elaborazione delle minacce**
  - Informazioni sulle minacce
  - Verdetto minaccia
  - Numero del record AMR
  - Versione del database antivirus
  - Modalità di rilevamento delle minacce
  - Nome dell'oggetto infetto
  - Hash MD5 e SHA256 dell'oggetto
  - Identificatore univoco del processo infetto
  - Identificatore univoco dell'oggetto infetto
  - Protocollo di rete tramite il quale è stato ricevuto l'oggetto infetto
  - Indirizzo locale da cui è stato ricevuto l'oggetto infetto
  - Indirizzo esterno da cui è stato ricevuto l'oggetto infetto
  - Stato di elaborazione della minaccia

- Motivo per cui non è stato possibile porre rimedio alla minaccia
- Indirizzo fisico locale

- **Dati sugli utenti**
  - SID utente
  - ID utente
  - Nome utente
  - Nome e cognome dell'utente
  - Descrizione utente
  - Se l'account è attivo o bloccato
  - Se la password è scaduta
  - Se è necessaria una modifica della password
  - Se è consentita la modifica della password
  - Tipo di account utente
  - Se l'accesso automatico è abilitato per questo account
  - Elenco dei gruppi a cui appartiene l'utente

Integrazione con Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Tutti i dati che l'applicazione archivia in locale nel computer vengono eliminati dal computer quando Kaspersky Endpoint Security viene disinstallato.

Durante l'integrazione con Kaspersky Unified Monitoring and Analysis Platform (KUMA), i dati delle impostazioni di connessione vengono trasferiti. Inoltre, tutti gli eventi vengono registrati nei Registri di sistema di Windows.

I principali registri di eventi di Windows sono System, Security, Application, ForwardedEvents e HardwareEvents. Gli utenti possono inoltre creare e utilizzare registri personalizzati per soddisfare requisiti specifici.

Conformità alla legislazione dell'Unione Europea (GDPR)

Kaspersky Endpoint Security può trasmettere dati a Kaspersky nei seguenti scenari:

- Utilizzo di Kaspersky Security Network.
- Attivazione dell'applicazione con un codice di attivazione.

- Aggiornamento dei moduli dell'applicazione e dei database anti-virus.
- Selezione dei collegamenti nell'interfaccia dell'applicazione.

Indipendentemente dalla classificazione dei dati e dal territorio dal quale i dati vengono ricevuti, Kaspersky aderisce a standard elevati per la sicurezza dei dati e impiega varie misure legali, organizzative e tecniche per proteggere i dati degli utenti, per garantire la sicurezza e la riservatezza dei dati e anche per garantire l'adempimento dei diritti degli utenti garantiti dalla normativa applicabile. Il testo dell'Informativa sulla privacy è incluso nel kit di distribuzione dell'applicazione ed è disponibile nel sito Web di Kaspersky.

Prima di utilizzare Kaspersky Endpoint Security, leggere attentamente la descrizione dei dati trasmessi nel Contratto di licenza con l'utente finale e nell'Informativa di Kaspersky Security Network. Se dati specifici trasmessi da Kaspersky Endpoint Security in uno qualsiasi degli scenari descritti possono essere classificati come dati personali in base alla legislazione o allo standard locale, è necessario assicurarsi che tali dati vengano elaborati legalmente e ottenere il consenso degli utenti finali per la raccolta e la trasmissione di tali dati.

Leggere il Contratto di licenza con l'utente finale e visitare il sito Web di Kaspersky per informazioni su come vengono ricevute, elaborate, archiviate ed eliminate le informazioni sull'utilizzo dell'applicazione una volta che si accettano il Contratto di licenza con l'utente finale e l'Informativa di Kaspersky Security Network. I file license.txt e ksn_<ID lingua>.txt contengono il testo del Contratto di licenza con l'utente finale e l'Informativa di Kaspersky Security Network e sono inclusi nel kit di distribuzione dell'applicazione.

Se non si desidera trasmettere i dati a Kaspersky, è possibile disabilitare la trasmissione dei dati.

Utilizzo di Kaspersky Security Network

Utilizzando Kaspersky Security Network, l'utente accetta di fornire automaticamente i dati elencati nell'Informativa di Kaspersky Security Network. Se non si accetta di fornire questi dati a Kaspersky, utilizzare Kaspersky Private Security Network (KSN) o disabilitare l'uso di KSN. Per ulteriori dettagli su KPSN, consultare la documentazione relativa a Kaspersky Private Security Network.

Attivazione dell'applicazione con un codice di attivazione

Utilizzando un codice di attivazione, si accetta di fornire automaticamente i dati elencati nel Contratto di licenza con l'utente finale. Se non si accetta di fornire questi dati a Kaspersky, utilizzare un file chiave per attivare Kaspersky Endpoint Security.

Aggiornamento dei moduli dell'applicazione e dei database anti-virus

Utilizzando i server Kaspersky, si accetta di fornire automaticamente i dati elencati nel Contratto di licenza con l'utente finale. Kaspersky richiede queste informazioni per verificare che Kaspersky Endpoint Security venga utilizzato in modo legittimo. Se non si accetta di fornire queste informazioni a Kaspersky, utilizzare Kaspersky Security Center per gli aggiornamenti dei database o Kaspersky Update Utility.

Selezione dei collegamenti nell'interfaccia dell'applicazione

Utilizzando i collegamenti nell'interfaccia dell'applicazione, si accetta di fornire automaticamente i dati elencati nel Contratto di licenza con l'utente finale. L'elenco esatto dei dati trasmessi in ogni collegamento specifico dipende da dove si trova il collegamento nell'interfaccia dell'applicazione e da quale problema si intende risolvere. Se non si accetta di fornire questi dati a Kaspersky, utilizzare l'interfaccia semplificata dell'applicazione o nascondere l'interfaccia dell'applicazione.

Scrittura di dump

Se è stata abilitata la scrittura di dump, Kaspersky Endpoint Security creerà un file di dump che conterrà tutti i dati della memoria dei processi dell'applicazione nel momento in cui è stato creato questo file di dump.

Note relative ai marchi

I marchi registrati e i marchi di servizi sono di proprietà dei rispettivi titolari.

Adobe, Acrobat, Flash, Reader e Shockwave sono marchi o marchi registrati di Adobe negli Stati Uniti e/o in altri paesi.

Amazon, Amazon Web Services, AWS sono marchi di Amazon.com, Inc. o delle sue affiliate.

Apple, FireWire, iTunes, Mac e Safari sono marchi di Apple Inc.

Arm è un marchio registrato di Arm Limited (o delle sue società controllate) negli Stati Uniti e/o altrove.

AutoCAD è un marchio o un marchio registrato di Autodesk, Inc. e/o delle relative filiali e/o consociate negli Stati Uniti e/o in altri paesi.

La parola, il marchio e i logo Bluetooth sono di proprietà di Bluetooth SIG, Inc.

Borland è un marchio o un marchio registrato di Borland Software Corporation.

Cisco, Cisco AnyConnect, IOS sono marchi registrati o marchi di Cisco Systems, Inc. e/o le sue consociate negli Stati Uniti e in alcuni altri paesi.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop e XenServer sono marchi registrati o marchi di Cloud Software Group, Inc. e/o delle relative consociate negli Stati Uniti e/o in altri paesi.

Cloudflare, Cloudflare Workers e il logo Cloudflare sono marchi e/o marchi registrati di Cloudflare, Inc. negli Stati Uniti e in altre giurisdizioni.

Core è un marchio di Intel Corporation o delle sue consociate.

dBase è un marchio di dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC e altri marchi sono marchi di Dell Inc. o delle sue consociate.

Docker e il logo Docker sono marchi e marchi registrati di Docker, Inc. negli Stati Uniti e in altri paesi. Docker, Inc. e altre parti possono anche detenere diritti di marchi in altri termini utilizzati nel presente documento.

ESET è un marchio o un marchio registrato di ESET spol. s.r.o. o la rispettiva entità ESET.

Foxit è un marchio registrato di Foxit Corporation.

Radmin è un marchio registrato di Famatech.

Google, Android, Google Public DNS, Google Chrome, Chrome sono marchi di Google, LLC.

HUAWEI, FusionCompute e FusionSphere sono marchi di Huawei Technologies Co., Ltd.

ICQ è un marchio e/o un marchio di servizio di ICQ LLC.

Intel è un marchio di Intel Corporation o delle sue consociate.

IBM è un marchio registrato di International Business Machines Corporation in diverse giurisdizioni di tutto il mondo.

Lenovo e Lenovo ThinkPad sono marchi di Lenovo negli Stati Uniti e/o in altri paesi.

Linux è il marchio registrato di Linus Torvalds negli Stati Uniti e in altri paesi.

Logitech è un marchio o un marchio registrato di Logitech negli Stati Uniti e/o in altri paesi.

LogMeIn Pro e Remotely Anywhere sono marchi di LogMeIn, Inc.

Mail.ru è un marchio registrato di Mail.Ru LLC.

McAfee è un marchio o un marchio registrato di McAfee LLC o delle sue consociate negli Stati Uniti e/o in altri paesi.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server e Windows Store sono marchi del gruppo di aziende Microsoft.

Mozilla, Firefox e Thunderbird sono marchi di Mozilla Foundation negli Stati Uniti e in altri paesi.

NetApp è un marchio o un marchio registrato di NetApp, Inc. negli Stati Uniti e/o in altri paesi.

OpenSSL è un marchio di proprietà di OpenSSL Software Foundation.

OpenStack è un marchio registrato di OpenStack Foundation negli Stati Uniti e in altri paesi.

Oracle, Java e JavaScript sono marchi registrati di Oracle e/o delle relative consociate.

Python è un marchio o un marchio registrato di Python Software Foundation.

Realtek è un marchio di Realtek Semiconductor Corporation.

SAMSUNG è un marchio di SAMSUNG negli Stati Uniti o in altri paesi.

Thawte è un marchio o un marchio registrato di Symantec Corporation o delle relative consociate negli Stati Uniti e in altri paesi.

Trend Micro è un marchio o un marchio registrato di Trend Micro Incorporated.

VERISIGN è un marchio registrato negli Stati Uniti e in altri paesi o un marchio non registrato di VeriSign, Inc. e delle relative filiali.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools, VMware vSphere sono marchi e/o marchi registrati di VMware, Inc. negli Stati Uniti e/o in altri paesi.

Informazioni sul codice di terze parti

Le informazioni sul codice di terze parti sono contenute nel file legal_notices.txt ubicato nella cartella di installazione dell'applicazione.