

kaspersky

Kaspersky Endpoint Security for Windows 11.9.0

© 2024 AO Kaspersky Lab

Sommario

[Guida di Kaspersky Endpoint Security for Windows](#)

[Novità](#)

[Domande frequenti](#)

[Kaspersky Endpoint Security for Windows](#)

[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](#)

[Modifica componenti dell'applicazione](#)

[Upgrade da una versione precedente 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](#)

[Attivazione dell'applicazione tramite Kaspersky Security Center](#)

[Utilizzo dell'Attivazione guidata per attivare l'applicazione](#)

[Visualizzazione delle informazioni sulla licenza](#)

[Acquisto di una licenza](#)

[Rinnovo dell'abbonamento](#)

[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](#)

[Conformità alla legislazione dell'Unione Europea \(GDPR\)](#)

[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](#)

[Guida introduttiva](#)

[Gestione dei criteri](#)

[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](#)

[Scansione virus del computer](#)

[Scansione del computer](#)

[Scansione delle unità rimovibili quando vengono connesse al computer](#)

[Scansione in background](#)

[Scansione dal menu di scelta rapida](#)

[Application Integrity Control](#)

[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](#)

[Configurazione degli aggiornamenti da una cartella condivisa](#)

[Aggiornamento dei moduli dell'applicazione](#)

[Utilizzo di un server proxy per gli aggiornamenti](#)

[Ultimo rollback degli aggiornamenti](#)

[Utilizzo delle minacce attive](#)

[Disinfezione delle minacce attive nelle workstation](#)

[Disinfezione delle minacce attive nei server](#)

[Abilitazione o disabilitazione di Tecnologia Avanzata di Disinfezione](#)

[Elaborazione delle minacce attive](#)

[Protezione del computer](#)

[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](#)

[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](#)

[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 della protezione dagli attacchi di rete per tipo](#)

[Firewall](#)

[Abilitazione o disabilitazione di Firewall](#)

[Modifica della categoria della 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](#)

[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 Attacchi BadUSB](#)

[Abilitazione e disabilitazione di Prevenzione Attacchi BadUSB](#)

[Utilizzo di Tastiera sullo schermo per l'autorizzazione di dispositivi USB](#)

[Protezione AMSI](#)

[Abilitazione e disabilitazione di Protezione AMSI](#)

[Utilizzo di Protezione AMSI per eseguire la scansione dei file compositi](#)

[Prevenzione Exploit](#)

[Abilitazione e disabilitazione di Prevenzione Exploit](#)

[Selezione di un'azione da eseguire quando viene rilevato un exploit](#)

[Protezione della memoria dei processi di sistema](#)

[Rilevamento del Comportamento](#)

[Abilitazione e disabilitazione di Rilevamento del Comportamento](#)

[Selezione dell'azione da intraprendere se viene rilevata un'attività malware](#)

[Protezione delle cartelle condivise dal criptaggio esterno](#)

[Abilitazione e disabilitazione della protezione delle cartelle condivise dal criptaggio esterno](#)

[Selezione dell'azione da eseguire se viene rilevato criptaggio esterno delle cartelle condivise](#)

[Creazione di un'esclusione per la protezione delle cartelle condivise dal criptaggio esterno](#)

[Configurazione degli indirizzi delle esclusioni dalla protezione delle cartelle condivise dal criptaggio esterno](#)

[Esportazione e importazione di un elenco di esclusioni dalla protezione delle cartelle condivise dal criptaggio esterno](#)

[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](#)

[Motore di Remediation](#)

[Kaspersky Security Network](#)

[Abilitazione e disabilitazione dell'utilizzo di Kaspersky Security Network](#)

[Limitazioni di KSN Privato](#)

[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](#)

[Scansione delle connessioni criptate in Firefox e Thunderbird](#)

[Esclusione delle connessioni criptate dalla scansione](#)

[Cancella dati](#)

[Controllo del computer](#)

[Controllo Web](#)

[Abilitazione e disabilitazione di Controllo Web](#)

[Azioni con le regole di accesso alle risorse Web](#)

[Aggiunta di una regola di accesso alle risorse Web](#)

[Assegnazione di priorità alle regole di accesso alle risorse Web](#)

[Abilitazione e disabilitazione di una regola di accesso alle risorse Web](#)

[Esportazione e importazione dell'elenco degli indirizzi Web attendibili](#)

[Verifica delle regole di accesso alle risorse Web](#)

[Esportazione e importazione dell'elenco di indirizzi delle risorse Web](#)
[Monitoraggio dell'attività Internet dell'utente](#)
[Modifica dei modelli dei messaggi di Controllo Web](#)
[Modifica delle maschere per gli indirizzi di risorse Web](#)
[Migrazione delle regole di accesso alle risorse Web da versioni precedenti dell'applicazione](#)

[Controllo dispositivi](#)

[Abilitazione e disabilitazione di Controllo dispositivi](#)
[Informazioni sulle regole di accesso](#)
[Modifica di una regola di accesso ai dispositivi](#)
[Modifica di una regola di accesso ai bus di connessione](#)
[Aggiunta di una rete Wi-Fi all'elenco delle reti attendibili](#)
[Monitoraggio dell'utilizzo delle unità rimovibili](#)
[Modificare la durata della memorizzazione nella cache](#)
[Azioni con i dispositivi attendibili](#)
[Aggiunta di un dispositivo all'elenco Attendibili dall'interfaccia dell'applicazione](#)
[Aggiunta di un dispositivo all'elenco Attendibili da Kaspersky Security Center](#)
[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](#)

[Abilitazione e disabilitazione 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](#)
[Visualizzazione dei rapporti di Controllo adattivo delle anomalie](#)

[Controllo applicazioni](#)

[Limitazioni delle funzionalità di Controllo applicazioni](#)
[Abilitazione e disabilitazione di Controllo applicazioni](#)
[Selezione della modalità di Controllo applicazioni](#)
[Utilizzo delle regole di Controllo applicazioni nell'interfaccia dell'applicazione](#)
[Aggiunta di una regola di Controllo applicazioni](#)
[Aggiunta di una condizione di attivazione per una regola di Controllo applicazioni](#)
[Modifica dello stato di una regola di Controllo applicazioni](#)
[Gestione delle regole di Controllo applicazioni in Kaspersky Security Center](#)
[Ricezione delle informazioni sulle applicazioni installate nei computer degli utenti](#)
[Creazione delle categorie di 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 e modifica di una regola di Controllo applicazioni tramite Kaspersky Security Center](#)

[Modifica dello stato di una regola di Controllo applicazioni tramite Kaspersky Security Center](#)

[Esportazione e importazione delle regole di Controllo applicazioni](#)

[Verifica delle regole di Controllo applicazioni tramite Kaspersky Security Center](#)

[Visualizzazione degli eventi generati dall'operazione di test del componente Controllo applicazioni](#)

[Visualizzazione di un rapporto sulle applicazioni bloccate in modalità di test](#)

[Visualizzazione degli eventi generati dall'esecuzione del componente Controllo applicazioni](#)

[Visualizzazione di un rapporto sulle applicazioni bloccate](#)

[Verifica delle regole di 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](#)

[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](#)

[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](#)

[Caratteristiche speciali delle autorizzazioni di Protezione tramite password](#)

[Reimpostazione della password KLAdmin](#)

[Area attendibile](#)

[Creazione di un'esclusione dalla scansione](#)

[Abilitazione e disabilitazione di un'esclusione dalla scansione](#)

[Selezione dei tipi di oggetti rilevabili](#)

[Modifica dell'elenco di applicazioni attendibili](#)

[Abilitazione e disabilitazione delle regole dell'area attendibile per un'applicazione nell'elenco delle applicazioni attendibili](#)

[Utilizzo dell'archivio di certificati di sistema attendibili](#)

[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](#)

[Abilitazione e disabilitazione della difesa gestione esterna](#)

[Supporto delle applicazioni di amministrazione remota](#)

[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](#)

[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 \(SSO\)](#)

[Gestione degli account per l'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](#)

[Selezione del livello di traccia per l'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](#)

[Kaspersky Endpoint Agent](#)

[Migrazione di criteri e attività per Kaspersky Endpoint Agent](#)

[Migrazione della configurazione \[KES+KEA\] alla configurazione \[KES+agente integrato\]](#)

[Managed Detection and Response](#)

[Integrazione con MDR](#)

[Migrazione da Kaspersky Endpoint Agent](#)

[Endpoint Detection and Response](#)

[Integrazione con Kaspersky Endpoint Detection and Response](#)

[Migrazione da Kaspersky Endpoint Agent](#)

[Scansione degli indicatori di compromissione \(attività standard\)](#)

[Sposta il file in Quarantena](#)

[Ottieni file](#)

[Elimina file](#)

[Avvio del processo](#)

[Termina processo](#)

[Prevenzione dell'esecuzione](#)

[Isolamento di rete del computer](#)

[Appendice 1. Estensioni di file supportate per Prevenzione dell'esecuzione](#)

[Appendice 2. Interpreti di script supportati](#)

[Appendice 3. Ambito della scansione IOC nel Registro di sistema \(RegistryItem\)](#)

[Appendice 4. Requisiti del file IOC](#)

[Kaspersky Sandbox](#)

[Integrazione con Kaspersky Sandbox](#)

[Migrazione da Kaspersky Endpoint Agent](#)

[Aggiunta di un certificato TLS](#)

[Aggiunta dei server di Kaspersky Sandbox](#)

[Scansione degli indicatori di compromissione \(attività standalone\)](#)

[Kaspersky Anti Targeted Attack Platform \(KATA EDR\)](#)

[Gestione della quarantena](#)

[Configurazione della dimensione massima della quarantena](#)

[Invio dei dati relativi ai file in quarantena a Kaspersky Security Center](#)

[Kaspersky Security for Windows Server](#)

[Installazione di KES su KSWs](#)

[Attivazione di KES con una chiave di KSWs](#)

[Gestione dell'applicazione su un server in modalità Core](#)

[Gestione dell'applicazione dalla riga di comando](#)

[Installazione dell'applicazione](#)

[Attivazione dell'applicazione](#)

[Rimozione dell'applicazione](#)

[Comandi AVP](#)

[SCAN. Scansione virus](#)

[UPDATE. Aggiornamento di database e moduli software dell'applicazione](#)

[ROLLBACK. Ultimo rollback degli aggiornamenti](#)

[TRACES. Tracciamento](#)

[START. Avvio del 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. Ripristinare i risultati del controllo del disco prima di criptare il disco](#)

[EXIT. Chiudi l'applicazione](#)

[EXITPOLICY. Disabilitazione del criterio](#)

[STARTPOLICY. Abilitazione del criterio](#)

[DISABLE. Disabilitazione della protezione](#)

[SPYWARE. Rilevamento spyware](#)

[KSN. Transizione KSN Globale/Privato](#)

[Comandi KESCLI](#)

[Scan. Scansione virus](#)

[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. Definizione del tempo di completamento dell'aggiornamento](#)

[EnableRTP. Abilitazione della protezione](#)

[GetRealTimeProtectionState. Stato di Protezione minacce file](#)

[Versione. Identificazione della versione dell'applicazione](#)

[Comandi di gestione di Detection and Response](#)

[SANDBOX. Gestione di Kaspersky Sandbox](#)

[PREVENZIONE. Gestione della prevenzione dell'esecuzione](#)

[ISOLAMENTO. Gestione dell'isolamento di rete](#)

[RESTORE. Ripristino dei file dalla quarantena](#)

[IOCSKAN. Scansione degli indicatori di compromissione \(IOC\)](#)

[MDRLICENSE. Attivazione MDR](#)

[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](#)

[Limitazioni e avvisi](#)

[Glossario](#)

[Agente di Autenticazione](#)
[Ambito della protezione](#)
[Ambito della scansione](#)
[Archivio](#)
[Attività](#)
[Autorità di emissione del certificato](#)
[Certificato di licenza](#)
[Chiave aggiuntiva](#)
[Chiave attiva](#)
[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](#)
[Maschera](#)
[Network Agent](#)
[Oggetto OLE](#)
[OpenIOC](#)
[Portable File Manager](#)
[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](#)
[Controllo Web](#)

[Controllo dispositivi](#)
[Controllo applicazioni](#)
[Controllo adattivo delle anomalie](#)
[Sensore Endpoint](#)
[Kaspersky Sandbox](#)
[Endpoint Detection and Response](#)
[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](#)
[Informazioni sul codice di terze parti](#)
[Note relative ai marchi](#)

Guida di Kaspersky Endpoint Security for Windows

🔗 Novità della versione 11.9.0

- [Ora è possibile creare un account di servizio di Agente di Autenticazione per Criptaggio disco Kaspersky.](#)
- [Interfaccia dei dettagli dell'avviso migliorata per EDR Optimum](#)
- [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](#)

🛡️ Eliminazione delle minacce

- [Sulle workstation](#)
- [Sui server](#)
- Reazione al rilevamento di un indicatore di compromissione ([Isolamento di rete](#) → [Quarantena](#) → [Prevenzione dell'esecuzione](#))

🔗 Utilizzo di KES come parte di altre soluzioni

- [Kaspersky EDR](#)
- [Kaspersky Sandbox](#)
- [Kaspersky MDR](#)

📄 Trasmissione dei dati

- [Ai sensi del Contratto di licenza con l'utente finale](#)
- [Quando si utilizza KSN](#)

- [GDPR](#)

Novità


Aggiornamento 11.9.0

Kaspersky Endpoint Security 11.9.0 for Windows offre i seguenti miglioramenti e funzionalità:

1. Ora è possibile [creare un account di servizio di Agente di Autenticazione](#) quando si utilizza Criptaggio disco Kaspersky. 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.
2. Il pacchetto di distribuzione di Kaspersky Endpoint Agent non fa più parte del [kit di distribuzione dell'applicazione](#). Per supportare le soluzioni [Detection and Response](#), è possibile utilizzare l'agente integrato di Kaspersky Endpoint Security. Se necessario, è possibile scaricare il pacchetto di distribuzione di Kaspersky Endpoint Agent dal kit di distribuzione di Kaspersky Anti Targeted Attack Platform.
3. L'interfaccia dei dettagli degli avvisi di [Kaspersky Endpoint Detection and Response Optimum \(EDR Optimum\)](#) è stata migliorata. Le funzionalità di risposta alle minacce ora propongono suggerimenti. Quando vengono rilevati indicatori di compromissione, viene visualizzata anche un'istruzione dettagliata per assicurare la sicurezza dell'infrastruttura aziendale.
4. Ora è possibile attivare Kaspersky Endpoint Security for Windows con una chiave di licenza di Kaspersky Hybrid Cloud Security.
5. Nuovi eventi aggiunti sullo [stabilimento di una connessione con domini dotati di certificati non attendibili](#) ed errori di scansione delle connessioni crittate.

Aggiornamento 11.8.0

Kaspersky Endpoint Security 11.8.0 for Windows offre i seguenti miglioramenti e funzionalità:

1. [Aggiunto l'agente integrato per supportare il funzionamento della soluzione Kaspersky Endpoint Detection and Response Expert](#). *Kaspersky Endpoint Detection and Response Expert* 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. 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](#) .
2. L'interfaccia di [Monitor di rete](#) è stata migliorata. Monitor di rete ora mostra il protocollo UDP oltre a TCP.
3. L'attività [Scansione virus](#) è stata migliorata. Se il computer è stato riavviato durante la scansione, Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui la scansione era stata interrotta.
4. Ora è possibile impostare un limite per il tempo di esecuzione delle attività. È possibile limitare il tempo di esecuzione delle attività *Scansione virus* e *Scansione IOC*. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security arresta l'attività. Per ridurre il tempo di esecuzione dell'attività *Scansione virus*, è possibile, ad esempio, [configurare l'ambito della scansione](#) oppure [ottimizzare la scansione](#).

5. Le limitazioni delle piattaforme server vengono eliminate per l'applicazione installata in Windows 10 Enterprise multisessione. Kaspersky Endpoint Security ora considera la multisessione di Windows 10 Enterprise come un sistema operativo di workstation, non un sistema operativo server. Di conseguenza, le [limitazioni della piattaforma server](#) non si applicano più all'applicazione in Windows 10 Enterprise multisessione. L'applicazione utilizza inoltre la chiave di licenza di una workstation per l'attivazione anziché la chiave di licenza di un server.

[Aggiornamento 11.7.0](#)

Kaspersky Endpoint Security for Windows 11.7.0 offre i seguenti miglioramenti e funzionalità:

1. [L'interfaccia di Kaspersky Endpoint Security for Windows](#) è stata aggiornata.

2. [Supporto di Windows 11, Windows 10 21H2 e Windows Server 2022](#).

3. Sono stati aggiunti nuovi componenti:

- [È stato aggiunto un agente integrato per l'integrazione con Kaspersky Sandbox](#). La soluzione Kaspersky Sandbox rileva e blocca automaticamente le minacce avanzate sui computer. Kaspersky Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Kaspersky Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Kaspersky Sandbox). Per ulteriori dettagli sulla soluzione, consultare la Guida di [Kaspersky Sandbox](#).

Per utilizzare Kaspersky Sandbox, non è più necessario Kaspersky Endpoint Agent. Kaspersky Endpoint Security può eseguire tutte le funzioni di Kaspersky Endpoint Agent. Per eseguire la migrazione di tutti i criteri di Kaspersky Endpoint Agent, usare la [migrazione guidata](#). Affinché tutte le funzioni di Kaspersky Sandbox vengano eseguite correttamente, è necessario Kaspersky Security Center 13.2. Per informazioni dettagliate sulla migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows, consultare la [guida dell'applicazione](#).

- [Aggiunto l'agente integrato per supportare il funzionamento della soluzione Kaspersky Endpoint Detection and Response Optimum](#). Kaspersky Endpoint Detection and Response Optimum è una soluzione che consente di proteggere l'infrastruttura IT dell'organizzazione 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](#).

Per utilizzare Kaspersky Endpoint Detection and Response, non è più necessario Kaspersky Endpoint Agent. Kaspersky Endpoint Security può eseguire tutte le funzioni di Kaspersky Endpoint Agent. Per eseguire la migrazione di tutti i criteri e le attività di Kaspersky Endpoint Agent, usare la [migrazione guidata](#). Per utilizzare tutte le funzioni, Kaspersky Endpoint Detection and Response Optimum richiede Kaspersky Security Center 13.2. Per informazioni dettagliate sulla migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows, consultare la [guida dell'applicazione](#).

4. È stata aggiunta la [migrazione guidata](#) per i criteri e le attività di Kaspersky Endpoint Agent. La migrazione guidata crea nuovi criteri e attività uniti per Kaspersky Endpoint Security for Windows. La procedura guidata consente di eseguire la migrazione delle soluzioni Detection and Response da Kaspersky Endpoint Agent a Kaspersky Endpoint Security. Le soluzioni Detection and Response includono Kaspersky Sandbox, Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) e Kaspersky Managed Detection and Response (MDR).

5. [Kaspersky Endpoint Agent](#), incluso nel kit di distribuzione, è aggiornato alla versione 3.11.

Quando si esegue l'upgrade di Kaspersky Endpoint Security, l'applicazione rileva la versione e lo scopo designato di Kaspersky Endpoint Agent. Se Kaspersky Endpoint Agent è designato per l'esecuzione di Kaspersky Sandbox, Kaspersky Managed Detection and Response (MDR) e Kaspersky Endpoint Detection and Response Optimum (EDR Optimum), Kaspersky Endpoint Security trasferisce l'esecuzione di tali soluzioni all'agente integrato dell'applicazione. Per Kaspersky Sandbox ed EDR Optimum, l'applicazione disinstalla automaticamente Kaspersky Endpoint Agent. Per MDR, è possibile disinstallare Kaspersky Endpoint Agent manualmente. Se l'applicazione è designata per l'esecuzione di Kaspersky Endpoint Detection and Response Expert (EDR Expert), Kaspersky Endpoint Security esegue l'upgrade della versione di Kaspersky Endpoint Agent. Per maggiori dettagli sull'applicazione, fare riferimento alla documentazione delle soluzioni Kaspersky che supportano Kaspersky Endpoint Agent.

6. Funzionalità Criptaggio BitLocker migliorata:

- è ora possibile utilizzare PIN avanzato con [Crittografia unità BitLocker](#). *PIN avanzato* consente di utilizzare altri caratteri oltre a quelli numerici: lettere latine maiuscole e minuscole, caratteri speciali e spazi.
 - È stata aggiunta una funzionalità di [disabilitazione dell'autenticazione BitLocker per l'upgrade del sistema operativo o l'installazione dei pacchetti di aggiornamento](#). L'installazione degli aggiornamenti può richiedere più riavvii del computer. Per installare gli aggiornamenti correttamente, è possibile disattivare temporaneamente l'autenticazione BitLocker e riabilitarla dopo l'installazione degli aggiornamenti.
 - Ora è possibile [impostare un'ora di scadenza per la password o il PIN di Criptaggio BitLocker](#). Quando la password o il PIN scade, Kaspersky Endpoint Security richiede una nuova password all'utente.
7. Ora è possibile configurare il numero massimo di tentativi di autorizzazione tastiera per Prevenzione Attacchi BadUSB. Quando viene raggiunto [il numero configurato di tentativi non riusciti di immissione del codice di autorizzazione](#), il dispositivo USB viene temporaneamente bloccato.
8. La funzionalità firewall è stata migliorata:
- Ora è possibile configurare un intervallo di indirizzi IP per le [regole dei pacchetti firewall](#). È possibile immettere un intervallo di indirizzi in formato IPv4 o IPv6. Ad esempio, 192.168.1.1-192.168.1.100 o 12:34::2-12:34::99.
 - Ora è possibile immettere i nomi DNS per le [regole dei pacchetti firewall](#) anziché gli indirizzi 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.
9. Ricerca delle [regole di Controllo Web](#) migliorata. Per cercare una regola di accesso alle risorse Web, oltre al nome della regola, è possibile utilizzare l'URL del sito Web, un nome utente, una categoria di contenuti o un tipo di dati.
10. L'attività *Scansione virus* è stata migliorata:
- L'attività [Scansione virus](#) in modalità inattiva è stata migliorata. Se il computer è stato riavviato durante la scansione, Kaspersky Endpoint Security esegue automaticamente l'attività, continuando dal punto in cui la scansione era stata interrotta.
 - L'attività [Scansione virus](#) è stata ottimizzata. Per impostazione predefinita, Kaspersky Endpoint Security esegue la scansione solo quando il computer è inattivo. È possibile configurare le tempistiche della scansione del computer nelle proprietà dell'attività.
11. È ora possibile limitare l'accesso degli utenti ai dati forniti da [Monitor attività applicazioni](#). *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'amministrazione può nascondere Monitor attività applicazioni all'utente nelle proprietà dei criteri dell'applicazione.
12. [Sicurezza della gestione dell'applicazione tramite la REST API](#). Ora Kaspersky Endpoint Security convalida la firma delle richieste inviate tramite la REST API. Per gestire il programma, è necessario installare un certificato di identificazione della richiesta.

[Aggiornamento 11.6.0](#)

Kaspersky Endpoint Security 11.6.0 for Windows offre i seguenti miglioramenti e funzionalità:

1. [Supporto per Windows 10 21H1](#). Per informazioni dettagliate sul supporto per il sistema operativo Microsoft Windows 10, fare riferimento alla [Knowledge Base dell'Assistenza tecnica](#).
2. [È stato aggiunto il componente Managed Detection and Response](#). Questo componente facilita l'interazione con la soluzione nota come Kaspersky Managed Detection and Response. Kaspersky Managed Detection and Response (MDR) garantisce protezione 24 ore su 24 da un numero crescente di minacce in grado di eludere i meccanismi di protezione automatizzata per le organizzazioni che hanno difficoltà a trovare esperti altamente qualificati o che dispongono di risorse interne limitate. Per informazioni dettagliate sul funzionamento della soluzione, fare riferimento alla Guida di Kaspersky Managed Detection and Response.
3. [Kaspersky Endpoint Agent](#), incluso nel kit di distribuzione, è stato aggiornato alla versione 3.10. Kaspersky Endpoint Agent 3.10 offre nuove funzionalità, risolve alcuni problemi precedenti ed è dotato di una maggiore stabilità. Per maggiori dettagli sull'applicazione, fare riferimento alla documentazione delle soluzioni Kaspersky che supportano Kaspersky Endpoint Agent.
4. Adesso consente di gestire la protezione contro attacchi come il flooding di rete e la scansione delle porte in [Impostazioni Protezione minacce di rete](#).
5. È stato aggiunto un nuovo metodo per la creazione di regole di rete per Firewall. È possibile aggiungere [regole per i pacchetti](#) e [regole dell'applicazione](#) per le connessioni visualizzate nella finestra [Monitor di rete](#). Tuttavia, le impostazioni di connessione delle regole di rete verranno configurate automaticamente.
6. L'interfaccia di [Monitor di rete](#) è stata migliorata. Sono state aggiunte le informazioni sull'attività di rete: ID processo da cui è stata avviata l'attività di rete; tipo di rete (rete locale o Internet); porte locali. Per impostazione predefinita, le informazioni sul tipo di rete sono nascoste.
7. Adesso è possibile creare automaticamente account dell'Agente di Autenticazione per i nuovi utenti di Windows. L'Agente consente a un utente di completare l'autenticazione per l'accesso alle unità [criptate utilizzando la tecnologia Criptaggio disco Kaspersky](#) e di caricare il sistema operativo. L'applicazione controlla le informazioni sugli account utente Windows nel computer. 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. Questo vuol dire che non è necessario [aggiungere manualmente gli account dell'Agente di Autenticazione](#) per i computer con unità già criptate.
8. Adesso è possibile monitorare il processo di criptaggio del disco nell'interfaccia dell'applicazione nei computer degli utenti (Criptaggio disco Kaspersky e BitLocker). È possibile eseguire lo strumento Monitoraggio criptaggio dalla [finestra principale dell'applicazione](#).

[Aggiornamento 11.5.0](#)

Kaspersky Endpoint Security 11.5.0 for Windows offre i seguenti miglioramenti e funzionalità:

1. [Supporto per Windows 10 20H2](#). Per informazioni dettagliate sul supporto per il sistema operativo Microsoft Windows 10, fare riferimento alla [Knowledge Base dell'Assistenza tecnica](#).
2. È stata aggiornata l'[interfaccia dell'applicazione](#). Sono state aggiornate anche l'[icona dell'applicazione nell'area di notifica](#), le notifiche dell'applicazione e le finestre di dialogo.
3. È stata migliorata l'interfaccia del plug-in Web di Kaspersky Endpoint Security per i componenti Controllo applicazioni, Controllo dispositivi e Controllo adattivo delle anomalie.
4. È stata aggiunta la funzionalità per importare ed esportare gli elenchi di regole ed esclusioni in formato XML. Il formato XML consente di modificare gli elenchi dopo l'esportazione. È possibile gestire gli elenchi solo in Kaspersky Security Center Console. I seguenti elenchi sono disponibili per l'esportazione o l'importazione:
 - [Rilevamento del Comportamento \(elenco di esclusioni\)](#).
 - [Protezione minacce Web \(elenco di indirizzi Web attendibili\)](#).
 - [Protezione minacce di posta \(elenco delle estensioni del filtro degli allegati\)](#).
 - [Protezione minacce di rete \(elenco di esclusioni\)](#).
 - [Firewall \(elenco di regole per i pacchetti di rete\)](#).
 - [Controllo applicazioni \(elenco di regole\)](#).
 - [Controllo Web \(elenco di regole\)](#).
 - [Monitoraggio delle porte di rete \(elenchi di porte e applicazioni monitorate da Kaspersky Endpoint Security\)](#).
 - [Criptaggio disco Kaspersky \(elenco delle esclusioni\)](#).
 - [Criptaggio unità rimovibili \(elenco di regole\)](#).
5. Le informazioni sull'oggetto MD5 sono state aggiunte al [rapporto sul rilevamento delle minacce](#). Nelle versioni precedenti dell'applicazione Kaspersky Endpoint Security visualizzava solo il valore SHA256 di un oggetto.
6. È stata aggiunta la possibilità di [assegnare la priorità per le regole di accesso al dispositivo](#) nelle impostazioni di Controllo dispositivi. L'assegnazione delle priorità consente una configurazione più flessibile dell'accesso degli utenti ai dispositivi. 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. 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 0 per il gruppo degli amministratori e assegnare la priorità 1 per il gruppo Tutti. È possibile configurare la priorità solo per i dispositivi che dispongono di un file system. Sono inclusi dischi rigidi, unità rimovibili, dischi floppy, unità CD/DVD e dispositivi portatili (MTP).
7. Sono state aggiunte nuove funzionalità:
 - [Gestisci le notifiche audio](#).

- Con Limitazione traffico di rete Kaspersky Endpoint Security limita il traffico di rete se la connessione Internet è limitata (ad esempio, tramite una connessione mobile).
 - [Gestisci le impostazioni di Kaspersky Endpoint Security tramite applicazioni di amministrazione remota attendibili](#) (come TeamViewer, LogMeln Pro e Remotely Anywhere). È possibile utilizzare applicazioni di amministrazione remota per avviare Kaspersky Endpoint Security e gestire le impostazioni nell'interfaccia dell'applicazione.
 - [Gestisci le impostazioni per la scansione del traffico sicuro in Firefox e Thunderbird](#). È possibile selezionare l'archivio dei certificati che verrà utilizzato da Mozilla: l'archivio dei certificati Windows o l'archivio dei certificati Mozilla. Questa funzionalità è disponibile solo per i computer che non dispongono di un criterio applicato. Se un criterio viene applicato a un computer, Kaspersky Endpoint Security abilita automaticamente l'utilizzo dell'archivio dei certificati Windows in Firefox e Thunderbird.
8. È stata aggiunta la funzionalità per [configurare la modalità di scansione del traffico sicuro](#): il traffico viene sempre esaminato anche se i componenti di protezione sono disabilitati oppure il traffico viene analizzato su richiesta dei componenti di protezione.
9. È stata rivista la procedura per l'[eliminazione delle informazioni dai rapporti](#). Un utente può eliminare solo tutti i rapporti. Nelle versioni precedenti dell'applicazione un utente poteva selezionare specifici componenti dell'applicazione le cui informazioni sarebbero state eliminate dai rapporti.
10. È stata rivista la procedura per [importare un file di configurazione contenente le impostazioni di Kaspersky Endpoint Security](#) ed è stata rivista la procedura per il [ripristino delle impostazioni dell'applicazione](#). Prima dell'importazione o del ripristino, Kaspersky Endpoint Security mostra solo un avviso. Nelle versioni precedenti dell'applicazione era possibile visualizzare i valori delle nuove impostazioni prima che venissero applicate.
11. È stata semplificata la [procedura per il ripristino dell'accesso a un'unità criptata da BitLocker](#). Dopo aver completato la procedura di ripristino dell'accesso, Kaspersky Endpoint Security richiede all'utente di impostare una nuova password o un nuovo codice PIN. Dopo aver impostato una nuova password, BitLocker cripta l'unità. Nella versione precedente dell'applicazione l'utente doveva reimpostare manualmente la password nelle impostazioni di BitLocker.
12. Gli utenti ora hanno la possibilità 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. Un amministratore può consentire o bloccare l'uso di esclusioni locali o applicazioni attendibili locali. Un amministratore può utilizzare Kaspersky Security Center per visualizzare, aggiungere, modificare o eliminare gli elementi dell'elenco nelle proprietà del computer.
13. È stata aggiunta la possibilità di [inserire commenti nelle proprietà delle applicazioni attendibili](#). I commenti consentono di semplificare le ricerche e l'ordinamento delle applicazioni attendibili.
14. [Gestione dell'applicazione tramite REST API](#):
- Ora è possibile configurare le impostazioni dell'estensione Protezione minacce di posta per Outlook.
 - È vietato disabilitare il rilevamento di virus, worm e Trojan.

[Aggiornamento 11.4.0](#)

Kaspersky Endpoint Security 11.4.0 for Windows offre i seguenti miglioramenti e funzionalità:

1. Nuovo design [dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni](#). La nuova icona  viene ora visualizzata al posto dell'icona  precedente. Se all'utente viene richiesto di eseguire un'azione (ad esempio riavviare il computer dopo l'aggiornamento dell'applicazione), l'icona diventerà . Se i componenti di protezione dell'applicazione sono disabilitati o non funzionano correttamente, l'icona diventerà  o . Passando il mouse sopra l'icona, Kaspersky Endpoint Security visualizzerà una descrizione del problema nella protezione del computer.
2. Kaspersky Endpoint Agent, incluso nel kit di distribuzione, è stato aggiornato alla versione 3.9. Kaspersky Endpoint Agent 3.9 supporta l'integrazione con le nuove soluzioni Kaspersky. Per maggiori dettagli sull'applicazione, fare riferimento alla documentazione delle soluzioni Kaspersky che supportano Kaspersky Endpoint Agent.
3. È stato aggiunto lo stato *Non supportato dalla licenza* per i componenti di Kaspersky Endpoint Security. È possibile visualizzare lo stato dei componenti nell'elenco dei componenti nella [finestra principale dell'applicazione](#).
4. Sono stati aggiunti nuovi eventi relativi a [Prevenzione Exploit](#) ai [rapporti](#).
5. I driver per la [tecnologia Criptaggio disco Kaspersky](#) ora vengono aggiunti automaticamente a Windows Recovery Environment (WinRE) all'avvio del criptaggio dell'unità. La versione precedente di Kaspersky Endpoint Security aggiungeva i driver durante l'installazione dell'applicazione. L'aggiunta di driver a WinRE può migliorare la stabilità dell'applicazione durante il ripristino del sistema operativo su computer protetti dalla tecnologia Criptaggio disco Kaspersky.

Il componente Sensore Endpoint è stato rimosso da Kaspersky Endpoint Security. È comunque 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.

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?](#)



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?](#)

[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 virus 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?](#)

[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.

Tecnologie di rilevamento delle minacce

<p> Machine Learning</p> <p>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).</p> <p> Analisi cloud</p> <p>Kaspersky Endpoint Security riceve i dati relativi alle minacce da Kaspersky Security Network. <i>Kaspersky Security Network (KSN)</i> 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.</p> <p> Analisi degli esperti</p> <p>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.</p>	<p> Analisi del comportamento</p> <p>Kaspersky Endpoint Security analizza l'attività di un oggetto in tempo reale.</p> <p> Analisi automatica</p> <p>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.</p> <p> Kaspersky Sandbox</p> <p>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.</p>
--	--

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.

Struttura di selezione

Sezione	Componente
<p>Protezione minacce essenziale</p> <p></p>	<p>Protezione minacce file</p> <p>Il componente Protezione minacce file consente di impedire l'infezione del file system del computer. Per impostazione predefinita, il componente Protezione minacce file risiede nella RAM del computer. Il componente esegue la scansione dei file in tutte le unità del computer, nonché nelle unità connesse. Il componente garantisce la protezione del computer mediante database anti-virus, il servizio cloud Kaspersky Security Network e l'analisi euristica.</p> <p>Protezione minacce Web</p>

Il componente Protezione minacce Web impedisce il download di file dannosi da Internet e blocca inoltre i 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 esegue inoltre la scansione dei messaggi alla ricerca di collegamenti dannosi e di phishing. Per impostazione predefinita, il componente Protezione minacce di posta risiede nella RAM del computer ed esegue la scansione di tutti i messaggi ricevuti o inviati utilizzando i protocolli POP3, SMTP, IMAP o NNTP oppure il client di posta Microsoft Office Outlook (MAPI). Il componente garantisce la protezione del computer mediante database anti-virus, il [servizio cloud Kaspersky Security Network](#) e l'analisi euristica.

Protezione minacce di rete

Il componente Protezione minacce di Rete esamina il traffico di rete in entrata alla ricerca di attività tipiche degli attacchi di rete. Quando Kaspersky Endpoint Security 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 di Kaspersky Endpoint Security 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

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 terze parti 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.

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 l'utente sta partecipando a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla categoria e sulla reputazione dei file esaminati, nonché informazioni sulla reputazione degli indirizzi Web esaminati.

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 (Behavior Stream Signature) 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 assicura una difesa proattiva del computer.

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.

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

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 tenere traccia dei comportamenti inusuali (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.

Attività



Scansione virus

Kaspersky Endpoint Security esamina la presenza di eventuali virus e altre minacce nel computer. Scansione virus 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

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.

Ultimo rollback degli aggiornamenti

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

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).

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](#).

Kaspersky Sandbox

Agente integrato della soluzione Kaspersky Sandbox. *La soluzione Kaspersky Sandbox* rileva e blocca automaticamente le minacce avanzate sui computer. Kaspersky Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Kaspersky Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Kaspersky Sandbox). Per ulteriori dettagli sulla soluzione, consultare la Guida di [Kaspersky Sandbox](#).

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](#).

Funzioni di servizio dell'applicazione

Kaspersky Endpoint Security include numerose funzioni di servizio. Le funzioni di servizio hanno l'obiettivo di mantenere aggiornata l'applicazione, espanderne le funzionalità e fornire supporto all'utente per il relativo utilizzo.

- **Rapporti.** Durante l'esecuzione, l'applicazione archivia un rapporto per ogni componente dell'applicazione. È inoltre possibile utilizzare i rapporti per tenere traccia dei risultati delle attività completate. I rapporti contengono elenchi di eventi che si sono verificati durante l'esecuzione di Kaspersky Endpoint Security e tutte le operazioni eseguite dall'applicazione. In caso di problemi, è possibile inviare i rapporti a Kaspersky, per consentire agli specialisti dell'Assistenza tecnica di verificare in dettaglio il problema.
- **Backup.** Se vengono rilevati file infetti durante la scansione del computer alla ricerca di virus e altre minacce, l'applicazione blocca tali file. Le copie dei file disinfettati o eliminati vengono archiviate in *Backup*. I file che non vengono elaborati per qualsiasi motivo vengono spostati nell'*elenco delle minacce attive*. È possibile esaminare i file, ripristinare i file nelle cartelle originali e svuotare l'archiviazione dei dati.
- **Notifiche.** Il servizio di notifica consente all'utente di tenere traccia degli eventi che influiscono sullo stato della protezione del computer e sull'esecuzione di Kaspersky Endpoint Security. Le notifiche possono essere visualizzare sullo schermo oppure inviate tramite e-mail.
- **Kaspersky Security Network.** La partecipazione degli utenti a Kaspersky Security Network migliora l'efficacia della protezione del computer attraverso l'utilizzo in tempo reale di informazioni sulla reputazione di file, risorse Web e software ricevute dagli utenti di tutto il mondo.
- **Licenza.** L'acquisto di una licenza rende disponibili tutte le funzionalità dell'applicazione, consente di accedere agli aggiornamenti dei database e dei moduli dell'applicazione e permette di ricevere assistenza tramite e-mail in merito ai problemi relativi all'installazione, la configurazione e l'utilizzo dell'applicazione.
- **Assistenza.** Tutti gli utenti registrati di Kaspersky Endpoint Security possono contattare gli specialisti dell'Assistenza tecnica per richiedere assistenza. È possibile inviare una richiesta all'Assistenza tecnica di Kaspersky tramite il portale Kaspersky CompanyAccount o contattare telefonicamente l'Assistenza tecnica.

Kit di distribuzione

Il kit di distribuzione include i seguenti pacchetti di distribuzione:

- **Criptaggio avanzato (AES256)**
Questo pacchetto di distribuzione contiene strumenti di criptaggio che implementano l'algoritmo di criptaggio AES (Advanced Encryption Standard) con una lunghezza della chiave effettiva di 256 bit.
- **Criptaggio base (AES56)**
Questo pacchetto di distribuzione contiene strumenti di criptaggio che implementano l'algoritmo di criptaggio AES con una lunghezza della chiave effettiva di 56 bit.

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 del plug-in di gestione di Kaspersky Endpoint Security per Kaspersky Security Center.
bases.cab	File di pacchetti di aggiornamento utilizzati durante l'installazione.
cleaner.cab	File per la rimozione del software incompatibile.
incompatible.txt	File contenente un elenco di software incompatibile.
ksn_<ID_lingua>.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.
keswin_web_plugin.zip	Archivio contenente i file necessari per l'installazione del plug-in Web di Kaspersky Endpoint Security .

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

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

Requisiti minimi generali:

- 2 GB di spazio libero su disco rigido;
- CPU:
 - Workstation: 1 GHz;
 - Server: 1.4 GHz;
 - Supporto per il set di istruzioni SSE2.
- RAM:
 - Workstation (x86): 1 GB;
 - Workstation (x64): 2 GB;
 - Server: 2 GB.

Workstation

Sistemi operativi supportati per workstation:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 o versioni successive;
- 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.

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. La modalità Core è supportata con [limitazioni](#):

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 o versioni successive;
- Windows Server 2012 Foundation/Essentials/Standard/Datacenter;
- Windows Server 2012 R2 Foundation/Essentials/Standard/Datacenter;
- Windows Server 2016 Essentials/Standard/Datacenter;
- Windows Server 2019 Essentials/Standard/Datacenter;
- Windows Server 2022.

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](#).

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;

Piattaforme virtuali

Piattaforme virtuali supportate:

- VMware Workstation 16.2.2 Pro;
- VMware ESXi 7.0 Update 3b;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps and Desktops 7 2112;
- Citrix Provisioning 2112;
- Citrix Hypervisor 8.2.

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

- Kaspersky Security Center 11;
- Kaspersky Security Center 12;
- Kaspersky Security Center 12 Patch A;
- Kaspersky Security Center 12 Patch B;
- Kaspersky Security Center 13;
- Kaspersky Security Center 13.1;

- Kaspersky Security Center 13.2;
- Kaspersky Security Center 13.2.2.

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).

Confronto delle funzionalità Kaspersky Endpoint Security

Funzionalità	Workstation	Server
Protezione minacce avanzata		
Kaspersky Security Network	✓	✓
Rilevamento del Comportamento	✓	✓
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		
Controllo applicazioni	✓	✓
Controllo dispositivi	✓	✓
Controllo Web	✓	✓
Controllo adattivo delle anomalie	✓	–
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	✓	✓
Kaspersky Sandbox	✓	✓
Managed Detection and Response (MDR)	✓	✓

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 in qualsiasi computer con accesso ad Administration Server.

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](#).

Confronto delle funzionalità Kaspersky Endpoint Security

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	✓	✓	✓
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			
Controllo applicazioni	✓	✓	✓
Controllo dispositivi	✓	✓	✓
Controllo Web	✓	✓	✓
Controllo adattivo delle anomalie	✓	✓	✓
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	–	–	✓
Kaspersky Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Attività			
Aggiungi chiave	✓	✓	✓
Modifica componenti dell'applicazione	✓	✓	✓
Inventario	✓	✓	✓
Aggiornamento	✓	✓	✓
Rollback degli aggiornamenti	✓	✓	✓
Scansione virus	✓	✓	✓
Controllo integrità	✓	✓	–
Cancella dati	✓	✓	✓
Gestisci gli account per l'Agente di Autenticazione (Criptaggio disco Kaspersky)	✓	✓	–
Scansione IOC (EDR)	–	✓	✓
Sposta file in Quarantena (EDR)	–	✓	✓
Ottieni file (EDR)	–	✓	✓
Elimina file (EDR)	–	✓	✓
Avvio del processo (EDR)	–	✓	✓
Termina processo (EDR)	–	✓	✓

Compatibilità con altre applicazioni

Prima dell'installazione, Kaspersky Endpoint Security verifica la presenza di applicazioni Kaspersky nel computer. L'applicazione controlla anche la presenza di software incompatibile nel computer. L'elenco del software incompatibile è disponibile nel file incompatible.txt incluso nel [kit di distribuzione](#).



[SCARICA IL FILE INCOMPATIBLE.TXT](#)

Kaspersky Endpoint Security è incompatibile con le seguenti applicazioni Kaspersky:

- Kaspersky Small Office Security.
- Kaspersky Endpoint Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (incluso il componente Sensore Endpoint).
- Kaspersky Sandbox (incluso Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (incluso il componente Sensore Endpoint).

Se il componente Endpoint Agent è stato installato in un computer utilizzando gli strumenti di distribuzione delle applicazioni Kaspersky, il componente verrà rimosso automaticamente durante l'installazione di Kaspersky Endpoint Security. Kaspersky Endpoint Security può anche includere il componente Sensore Endpoint o il componente Kaspersky Endpoint Agent se è stato selezionato Endpoint Agent nell'elenco dei componenti dell'applicazione.

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

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](#) ²).
- 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](#).

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

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. 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](#).

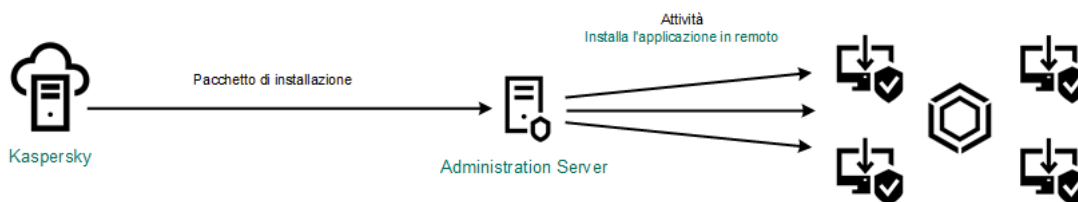
Installazione standard dell'applicazione

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 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. In Administration Console accedere alla cartella **Administration Server** → **Avanzate** → **Installazione remota**.

2. 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 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 3. 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.** 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 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 installare 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 4. 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 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. 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 7. 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 8. Avvio dell'installazione

Chiusura della 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, selezionare **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.** Selezione del metodo di installazione dell'applicazione:
 - **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 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 installare 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

Chiusura della 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 accedere 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 sul pulsante **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 11.9.0*.

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 inoltre possibile selezionare i componenti dell'applicazione e configurare le impostazioni di installazione dell'applicazione (vedere la tabella di seguito). 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 e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **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 sul pulsante **Aggiungi**.

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**.

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.

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.

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 inoltre possibile selezionare i componenti dell'applicazione e configurare le impostazioni di installazione dell'applicazione (vedere la tabella di seguito). 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.

Impostazioni del pacchetto di installazione

Sezione	Descrizione
Componenti della protezione	<p>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 <i>Modifica componenti dell'applicazione</i>. I componenti Prevenzione Attacchi BadUSB, Detection and Response e i componenti di criptaggio dei dati non sono installati per impostazione predefinita. Questi componenti possono essere aggiunti nelle impostazioni del pacchetto di installazione.</p> <p>Se è necessario installare i componenti di Detection and Response, Kaspersky Endpoint Security supporta le seguenti configurazioni:</p> <ul style="list-style-type: none">• Solo Endpoint Detection and Response Optimum• Solo Endpoint Detection and Response Expert• Solo Kaspersky Sandbox• Endpoint Detection and Response Optimum e Kaspersky Sandbox

	<ul style="list-style-type: none"> Endpoint Detection and Response Expert e Kaspersky Sandbox. <p>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.</p>
Chiave di licenza	<p>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.</p>
Applicazioni incompatibili	<p>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.</p>
Impostazioni di installazione	<p>Aggiungi il percorso dell'applicazione alla variabile di ambiente %PATH%. È possibile aggiungere il percorso di installazione alla variabile %PATH% per agevolare l'utilizzo dell'interfaccia della riga di comando.</p> <p>Non proteggere 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 Desktop remoto di Windows), è possibile disabilitare la protezione del processo di installazione.</p> <p>Garantisci la compatibilità con Citrix PVS (necessario solo quando si utilizza Citrix PVS). È possibile abilitare il supporto dei servizi di provisioning Citrix per installare Kaspersky Endpoint Security in una macchina virtuale.</p> <p>Percorso della 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%\Kaspersky Lab\Kaspersky Endpoint Security for Windows.</p> <p>File di configurazione. È possibile caricare un file che definisce le impostazioni di Kaspersky Endpoint Security. È possibile creare un file di configurazione nell'interfaccia locale dell'applicazione.</p>

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 gli aggiornamenti nell'archivio di 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. In Administration Console accedere 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. Aprire le proprietà del pacchetto di installazione.
3. Nella sezione **Generale** fare clic sul pulsante **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, selezionare **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 applicazione in remoto* è progettata per l'installazione remota di Kaspersky Endpoint Security. L'attività *Installa 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. In Administration Console accedere alla cartella **Administration Server** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 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. Altre operazioni

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.** 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 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 installare 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 11.9.0*.

Passaggio 10. Completamento della creazione dell'attività

Chiusura della 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 **k** verrà aggiunta all'area di notifica del computer dell'utente. Se l'icona si presenta in questo modo **k**, 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, selezionare **Dispositivi** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 applicazione in remoto**.

3. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Installazione di Kaspersky Endpoint Security for Managers*.

4. Nel blocco **Selezionare i 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 (11.9.0).

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.** 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 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 installare 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 soddisfa 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 **k** 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.

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_ks.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:

- Presenza di un software incompatibile installato (l'elenco del software incompatibile è disponibile nel file incompatible.txt incluso nel [kit di distribuzione](#)).
- Se i [requisiti hardware e software](#) sono soddisfatti o meno.
- 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.

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 11.9.0 for Windows e la versione precedente dell'applicazione viene rimossa automaticamente. Questo si applica alle seguenti versioni dell'applicazione:

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (build 10.3.3.304).
- Kaspersky Endpoint Security 11.1.0 for Windows (build 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (build 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (build 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 for Windows (build 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (build 11.5.0.590).

- Kaspersky Endpoint Security 11.6.0 for Windows (build 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 for Windows (build 11.7.0.669).
- Kaspersky Endpoint Security 11.8.0 for Windows (build 11.8.0.384).

Componenti di Kaspersky Endpoint Security

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

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

- [Prevenzione Attacchi BadUSB](#).
- [Componenti di criptaggio dei dati](#).
- Componenti di Detection and Response.

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
- Solo Kaspersky Sandbox
- Endpoint Detection and Response Optimum e Kaspersky Sandbox
- Endpoint Detection and Response Expert e Kaspersky Sandbox.

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.

Impostazioni avanzate

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 Desktop remoto di Windows), è possibile disabilitare la protezione del processo di installazione.

Garantisci la compatibilità con Citrix PVS (necessario solo quando si utilizza Citrix PVS). È possibile abilitare il supporto dei servizi di provisioning Citrix per installare Kaspersky Endpoint Security in una macchina virtuale.

Aggiungi il percorso dell'applicazione alla variabile di ambiente %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.



[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. 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. Anche il componente Managed Detection and Response non è presente in questo blocco. Per installare questo componente, è necessario [attivare Managed Detection and Response in Kaspersky Security Center Console](#).
- **[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` e `enabled`.

In alternativa al valore 0, è possibile utilizzare i valori `no`, `off`, `disable` e `disabled`.

Impostazioni del file setup.ini

Sezione	Parametro	Descrizione
[Setup]	InstallDir	Percorso della cartella di installazione dell'applicazione.
	ActivationCode	Codice di attivazione di Kaspersky Endpoint Security.
	EULA=1	<p>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.</p> <div style="border: 1px solid black; padding: 5px;"><p>L'accettazione delle condizioni del Contratto di licenza con l'utente finale è necessaria per installare l'applicazione o eseguire l'aggiornamento della versione.</p></div>
	PrivacyPolicy=1	<p>Accettazione dell'Informativa sulla privacy. Il testo dell'Informativa sulla privacy è incluso nel kit di distribuzione di Kaspersky Endpoint Security.</p> <div style="border: 1px solid black; padding: 5px;"><p>Per installare l'applicazione o eseguire l'upgrade della versione dell'applicazione, è necessario accettare la Informativa sulla privacy.</p></div>
	KSN	<p>Accettazione o rifiuto della partecipazione a Kaspersky Security Network. 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:</p> <ul style="list-style-type: none">• 1 – accettazione della partecipazione a KSN.• 0 – rifiuto della partecipazione a KSN (valore predefinito). <p>Il pacchetto di distribuzione di Kaspersky Endpoint Security è ottimizzato per l'utilizzo con Kaspersky Security Network. Se si è scelto di non partecipare a Kaspersky Security Network, è necessario aggiornare Kaspersky Endpoint Security subito dopo il completamento dell'installazione.</p>
	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

		<p>Password e PasswordArea. Per impostazione predefinita, viene utilizzato il nome utente KLAdmin.</p>
	<p>Password</p>	<p>Specificare una password per accedere a funzionalità e impostazioni di Kaspersky Endpoint Security (la password è specificata insieme ai parametri Login e PasswordArea).</p> <p>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.</p>
	<p>PasswordArea</p>	<p>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 Nome accesso e Password).</p> <p>Utilizzare il carattere " ; " per specificare più valori.</p> <p>Valori disponibili:</p> <ul style="list-style-type: none"> • 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.
	<p>SelfProtection</p>	<p>Abilitazione o disabilitazione del meccanismo di protezione dell'installazione dell'applicazione. Valori disponibili:</p> <ul style="list-style-type: none"> • 1 – il meccanismo di protezione dell'installazione dell'applicazione è abilitato (valore predefinito). • 0 – il meccanismo di protezione dell'installazione dell'applicazione è disabilitato.

		<p>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 Desktop remoto di Windows), è possibile disabilitare la protezione del processo di installazione.</p>
	Reboot=1	<p>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.</p> <p>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.</p>
	AddEnvironment	<p>Nella variabile di sistema %PATH% è possibile aggiungere il percorso dei file eseguibili contenuti nella cartella di installazione di Kaspersky Endpoint Security. Valori disponibili:</p> <ul style="list-style-type: none"> • 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.
	AMPPL	<p>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.</p> <p>La tecnologia AM-PPL è disponibile per i sistemi operativi Windows 10 versione 1703 (RS2) o successiva e Windows Server 2019.</p> <p>Valori disponibili:</p> <ul style="list-style-type: none"> • 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.
	SetupReg	<p>Consente la scrittura delle chiavi del Registro di sistema del file setup.reg nel Registro di sistema. Valore del parametro SetupReg: setup.reg.</p>
	EnableTraces	<p>Abilitazione o disabilitazione del tracciamento dell'applicazione. Dopo l'avvio, Kaspersky Endpoint</p>

		<p>Security salva i file di traccia nella cartella %ProgramData%\Kaspersky Lab\KES\Traces. Valori disponibili:</p> <ul style="list-style-type: none"> • 1 - il tracciamento è abilitato. • 0 - il tracciamento è disabilitato (valore predefinito).
	TracesLevel	<p>Livello di dettaglio delle tracce. Valori disponibili:</p> <ul style="list-style-type: none"> • 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	<p>Gestione dell'applicazione tramite REST API. Per gestire l'applicazione tramite REST API, è necessario specificare il nome utente (parametro RESTAPI_User).</p> <p>Valori disponibili:</p> <ul style="list-style-type: none"> • 1 - la gestione tramite REST API è consentita. • 0 - la gestione tramite l'API REST è bloccata (valore predefinito). <p>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.</p>
	RESTAPI_User	<p>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 <DOMINIO>\<Nome utente> (ad esempio RESTAPI_User=COMPANY\Administrator). È possibile selezionare un solo utente per l'utilizzo dell'API REST.</p> <p>L'aggiunta di un nome utente è un prerequisito per la gestione dell'applicazione tramite REST API.</p>
	RESTAPI_Port	<p>Porta utilizzata per la gestione dell'applicazione tramite REST API. La porta 6782 è utilizzata per impostazione predefinita.</p>
		<p>Certificato per l'identificazione delle richieste (ad</p>

	RESTAPI_Certificate	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.
[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. Per via delle modalità con cui le soluzioni Detection and Response sono supportate, i componenti di Kaspersky Sandbox ed Endpoint Detection and Response Optimum vengono installati nel computer. Il componente Endpoint Detection and Response Expert 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.
	FileEncryption	Librerie di Criptaggio a livello di file.
	DiskEncryption	Librerie di Criptaggio dell'intero disco.
	BadUSBAttackPrevention	Prevenzione Attacchi BadUSB.
	EDR	Endpoint Detection and Response Optimum (EDR Optimum). Il componente non è compatibile con il componente EDR Expert (EDRCloud).
	EDRCloud	Endpoint Detection and Response Expert (EDR Expert).

		Il componente non è compatibile con il componente EDR Optimum (EDR).
	SB	Kaspersky Sandbox.
	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 terze parti. A tale scopo, Kaspersky Endpoint Security fornisce un'API. Valori disponibili: <ul style="list-style-type: none"> • 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.
[Tasks]	ScanMyComputer	Attività Scansione completa. Valori disponibili: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

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.

- Da remoto tramite Kaspersky Security Center.

L'attività *Modifica 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.

[Come aggiungere o rimuovere componenti dell'applicazione in Administration Console \(MMC\)](#),²

1. In Administration Console accedere alla cartella **Administration Server** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)** → **Modifica componenti dell'applicazione**.

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

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

Selezionare la casella di controllo **Rimuovi le applicazioni di terze parti incompatibili**. L'elenco delle applicazioni incompatibili può essere visualizzato in `incompatible.txt`, incluso nel [kit di distribuzione](#). Se nel computer sono installate applicazioni incompatibili, l'installazione di Kaspersky Endpoint Security termina con un errore.

Se necessario, abilitare la [protezione tramite password](#) per l'esecuzione delle attività:

1. Fare clic su **Avanzate**.

2. Selezionare la casella di controllo **Usa password per la modifica del set di componenti dell'applicazione**.

3. Immettere le credenziali dell'account utente KLAdmin.

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 *Aggiungi il componente Controllo applicazioni*.

Passaggio 6. Completamento della creazione dell'attività

Chiusura della 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, 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.

[Come aggiungere o rimuovere i componenti dell'applicazione in Web Console e Cloud Console](#) 

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

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

2. Nell'elenco a discesa **Tipo di attività** selezionare **Modifica componenti dell'applicazione**.

3. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Aggiungere il componente Controllo applicazioni*.

4. Nel blocco **Selezionare i 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 completare la procedura guidata. Nelle proprietà dell'attività selezionare la scheda **Impostazioni applicazione** e selezionare i componenti dell'applicazione che saranno disponibili.

Se necessario, abilitare la [protezione tramite password](#) per l'esecuzione delle attività:

1. Nel blocco **Impostazioni Avanzate**, selezionare la casella di controllo **Usa password per la modifica del set di componenti dell'applicazione**.

2. Immettere le credenziali dell'account utente KLAdmin.

Salvare le modifiche ed eseguire l'attività.

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.

Upgrade da 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.
- Se il computer dispone di dischi rigidi criptati mediante [Criptaggio dell'intero disco \(FDE\)](#), è necessario decriptare tutti i dischi rigidi criptati per eseguire l'upgrade di Kaspersky Endpoint Security dalla versione 10 alla versione 11.0.0 o successiva.


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.

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

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (build 10.3.3.304).
- Kaspersky Endpoint Security 11.1.0 for Windows (build 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (build 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (build 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (build 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 for Windows (build 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (build 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 for Windows (build 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 for Windows (build 11.7.0.669).
- Kaspersky Endpoint Security 11.8.0 for Windows (build 11.8.0.384).

Durante l'upgrade di Kaspersky Endpoint Security 10 Service Pack 2 for Windows a Kaspersky Endpoint Security 11.9.0 for Windows, i file che sono stati spostati in Backup o Quarantena nella versione precedente dell'applicazione vengono trasferiti in Backup nella nuova versione dell'applicazione. Per le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, i file inseriti in Backup e Quarantena in una versione precedente dell'applicazione non vengono migrati alla versione più recente.

Kaspersky Endpoint Security può essere aggiornato nel 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](#).

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 e Cloud Console. Durante l'aggiornamento di Kaspersky Endpoint Security, tenere presente quanto segue:

- Kaspersky Security Center Web Console o Kaspersky Security Center Cloud 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, un componente come Prevenzione Attacchi BadUSB verrà rimosso dal computer, poiché 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](#).

Rimozione dell'applicazione

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

Disinstallazione dell'applicazione da remoto

È possibile disinstallare in remoto l'applicazione utilizzando l'attività *Disinstalla 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. In Administration Console accedere alla cartella **Administration Server** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 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 (11.9.0)**.

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 soddisfa 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 11.9.0*.

Passaggio 10. Completamento della creazione dell'attività

Chiusura della 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 **Dispositivi** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 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 **Selezionare i 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 **Disinstalla l'applicazione gestita**.

2. Selezionare **Kaspersky Endpoint Security for Windows (11.9.0)**.

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 soddisfa 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 KAdmin nelle proprietà dell'attività *Disinstalla applicazione in remoto*. Senza la password, l'attività non verrà eseguita.

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

1. Nella finestra principale di Web Console, selezionare **Dispositivi → Attività**.
Viene aperto l'elenco delle attività.
2. Fare clic sull'attività di Kaspersky Security Center **Disinstalla applicazione in remoto**.
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 KAdmin.
6. Salvare le modifiche.

È inoltre possibile eliminare l'applicazione da remoto tramite l'editor Gestione Criteri di gruppo di Microsoft Windows (per ulteriori dettagli, visitare il [sito Web del supporto tecnico di Microsoft](#)).

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.

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 specifica alcun dato, l'applicazione viene rimossa completamente.

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 di 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.

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\Kaspersky Endpoint Security for Windows\Doc\\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.
- *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:

- Chiave 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.

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 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
Protezione minacce avanzata						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Rilevamento del Comportamento	✓	✓	✓	✓	✓	✓
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						
Controllo applicazioni	✓	✓	✓	✓	✓	✓
Controllo dispositivi	✓	✓	✓	✓	✓	✓
Controllo Web	✓	✓	✓	✓	✓	✓
Controllo adattivo delle anomalie	–	✓	✓	✓	✓	✓
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							
Kaspersky Sandbox <i>(La licenza Kaspersky Sandbox deve essere acquistata separatamente)</i>	✓	✓	✓	✓	✓	✓	✓

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 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
Protezione minacce avanzata							
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓
Rilevamento del Comportamento	✓	✓	✓	✓	✓	✓	✓
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								
Controllo applicazioni	-	✓	✓	✓	✓	✓	✓	-
Controllo dispositivi	-	✓	✓	✓	✓	✓	✓	✓
Controllo Web	-	✓	✓	✓	✓	✓	✓	✓
Controllo adattivo delle anomalie	-	-	-	-	-	-	-	-
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	-	-	-	-	-	✓	-	-
Kaspersky Sandbox <i>(La licenza Kaspersky Sandbox deve essere acquistata separatamente)</i>	✓	✓	✓	✓	✓	✓	✓	✓

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:

- In locale, dall'interfaccia dell'applicazione, mediante l'[Attivazione guidata](#). In questo modo è possibile aggiungere sia la chiave attiva che la chiave di riserva.
- In remoto tramite il software [Kaspersky Security Center](#), creando e quindi avviando un'attività di aggiunta della chiave di licenza. In questo modo è possibile aggiungere sia la chiave attiva che la chiave di riserva.
- In remoto distribuendo file chiave e codici di attivazione archiviati nell'archivio delle chiavi di Kaspersky Security Center Administration Server ai computer client. Per ulteriori dettagli sulla distribuzione delle chiavi, consultare la [Guida di Kaspersky Security Center](#). In questo modo è possibile aggiungere sia la chiave attiva che la chiave di riserva.

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

- 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.

Attivazione dell'applicazione tramite Kaspersky Security Center


È possibile attivare l'applicazione in remoto tramite Kaspersky Security Center nei seguenti modi:

- Tramite l'attività *Aggiungi chiave*.
Questo metodo consente di aggiungere una chiave a un computer specifico o ai computer appartenenti a un gruppo di amministrazione.
- 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](#).
- 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.

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.

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

- Visualizzare il *Rapporto sull'utilizzo delle chiavi* per l'infrastruttura dell'organizzazione (**Monitoraggio e generazione dei rapporti** → **Rapporti**).
- Visualizzare gli stati dei computer nella scheda **Dispositivi** → **Dispositivi gestiti**. 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.
- Visualizzare le proprietà della chiave (**Operazioni** → **Gestione delle licenze**).

[Come attivare l'applicazione in Administration Console \(MMC\)](#) 

1. In Administration Console accedere alla cartella **Administration Server** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)** → **Aggiungere una 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

Chiusura della 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.

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

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

2. Nell'elenco a discesa **Tipo di attività** selezionare **Aggiungere una chiave**.

3. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Attivazione di Kaspersky Endpoint Security for Windows*.

4. Nel blocco **Selezionare i 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** → **Gestione delle licenze**).

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.

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 o viene eliminata. 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 accedere alla cartella **Administration Server** → **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 **Chiave di licenza distribuita automaticamente**.
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, selezionare **Operazioni** → **Gestione delle licenze** → **Licenze di Kaspersky**.

Viene visualizzato un elenco di chiavi di licenza.

2. Aprire le proprietà della chiave di licenza.
3. In corrispondenza della scheda **Generale**, attivare l'interruttore **Distribuisce automaticamente la chiave di licenza**.
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**.

Utilizzo dell'Attivazione guidata per attivare l'applicazione

Per attivare Kaspersky Endpoint Security tramite l'Attivazione guidata:

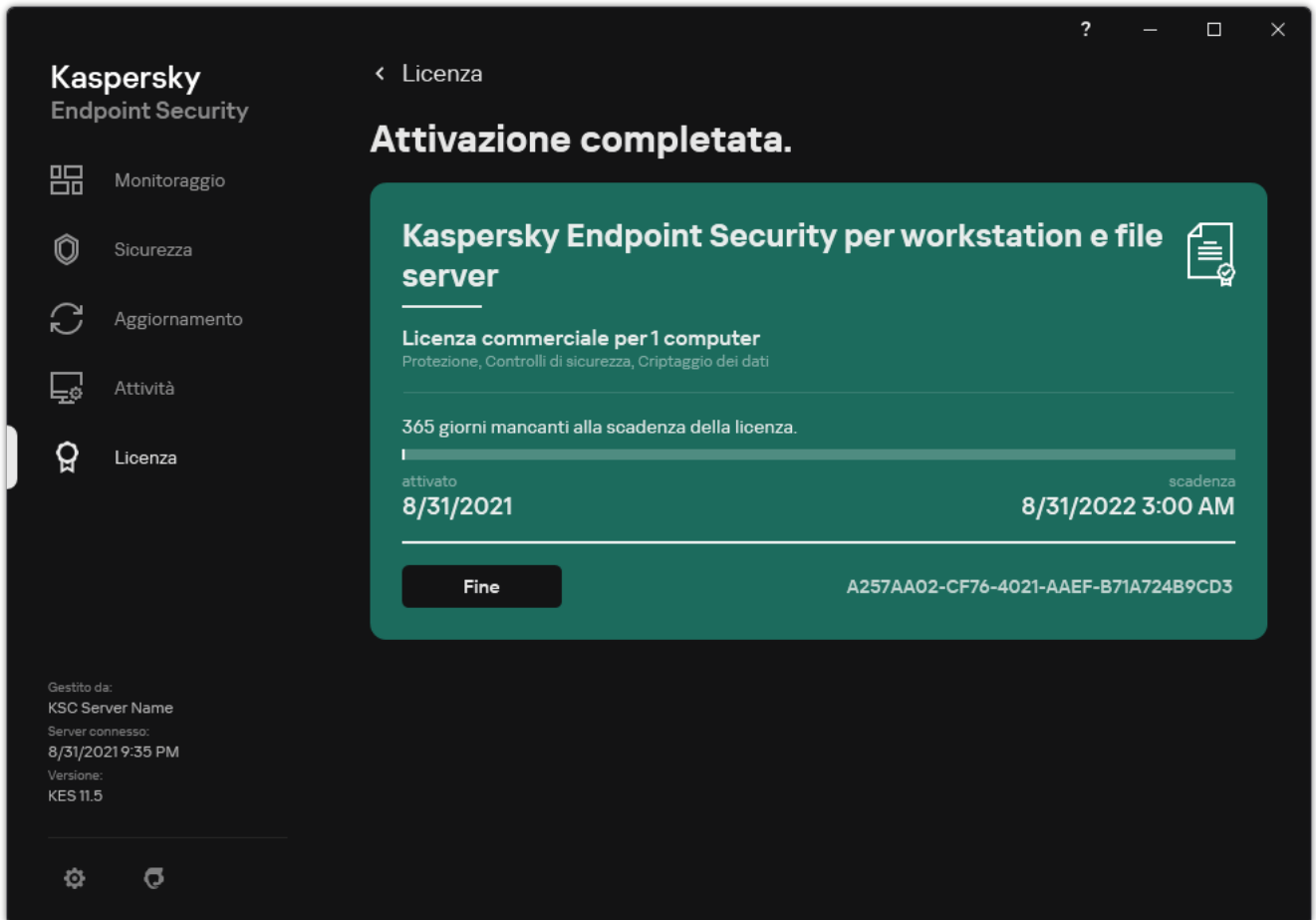
1. Nella finestra principale dell'applicazione, andare alla sezione **Licenza**.
2. Fare clic su **Attivare l'applicazione utilizzando una nuova licenza**.

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

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 la 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.
- **Attivare 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 la 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.

Trasmissione dei dati

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 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 attiva;
- Chiave attiva;
- Periodo di validità della licenza di Kaspersky Endpoint Security;
- Stato corrente della licenza;
- Tipo di licenza attiva;
- 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 **Abilita modalità KSN estesa** è selezionata anche la casella di controllo **Kaspersky Security Network**, 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 terze parti), 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 terze parti 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 terze parti, contrassegno che indica la presenza dell'errore nel componente software, periodo di esecuzione dell'applicazione di terze parti 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](#) e [Kaspersky Sandbox](#). 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 richiesta 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 richiesta HTTP

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.
- Scrittura di dump.

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 KSN privato o [disabilitare l'uso di KSN](#). Per ulteriori dettagli su KSN Privato, fare riferimento alla *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.

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](#) ².

Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (di seguito denominato anche "*Web Console*") è un'applicazione Web destinata all'esecuzione centralizzata delle attività principali per gestire e amministrare il sistema di sicurezza di una rete aziendale. Web Console è un componente di Kaspersky Security Center che fornisce un'interfaccia utente. Per informazioni dettagliate su Kaspersky Security Center Web Console, consultare la [Guida di Kaspersky Security Center](#) ².

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](#) ².

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. A differenza del plug-in di gestione per Kaspersky Security Center Administration Console, installato nella workstation dell'amministratore, 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**. Per ulteriori dettagli sulla compatibilità delle versioni dei plug-in Web e di Web Console, consultare la [Guida di Kaspersky Security Center](#).

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.

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 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. 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

Kaspersky Endpoint Security può essere gestito 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.

Upgrade del plug-in di gestione di Kaspersky Endpoint Security 10 for Windows

Se il plug-in di gestione di Kaspersky Endpoint Security 10 for Windows è installato in Administration Console, tenere in considerazione i seguenti aspetti durante l'installazione del plug-in di gestione di Kaspersky Endpoint Security 11 for Windows:


- Il plug-in di gestione di Kaspersky Endpoint Security 10 for Windows non verrà rimosso e potrà essere utilizzato. Si avrà quindi accesso a due plug-in di gestione per l'utilizzo delle versioni dell'applicazione 10 e 11.
- Il plug-in di gestione di Kaspersky Endpoint Security 11 for Windows non supporta la gestione di Kaspersky Endpoint Security 10 for Windows nei computer degli utenti.
- Il plug-in di gestione di Kaspersky Endpoint Security 11 for Windows non supporta gli elementi (ad esempio, criteri o attività) creati utilizzando il plug-in di gestione di Kaspersky Endpoint Security 10 for Windows.

È possibile utilizzare la conversione guidata in batch di criteri e attività per convertire criteri e attività dalla versione 10 alla versione 11. Per informazioni dettagliate sulla conversione di criteri e attività, consultare la [Guida di Kaspersky Security Center](#).



Upgrade del plug-in di gestione di Kaspersky Endpoint Security 11 for Windows

Se il plug-in di gestione di Kaspersky Endpoint Security 11 for Windows è installato in Administration Console, tenere in considerazione i seguenti aspetti durante l'installazione di una nuova versione del plug-in di gestione di Kaspersky Endpoint Security 11 for Windows:

- La versione precedente del plug-in di gestione di Kaspersky Endpoint Security 11 for Windows verrà rimossa.
- La nuova versione del plug-in di gestione di Kaspersky Endpoint Security 11 for Windows supporta la gestione della versione precedente di Kaspersky Endpoint Security 11 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.
- Quando si esegue l'upgrade del plug-in di gestione alla versione 11.2.0, è necessario aprire un criterio per convertirlo automaticamente. Durante questa operazione, Kaspersky Endpoint Security richiederà la conferma di partecipazione a KSN. Se è già stato eseguito l'upgrade dell'applicazione alla versione 11.20 nei computer dell'organizzazione, la partecipazione a KSN sarà disabilitata finché non si accettano i termini di partecipazione a KSN.

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.

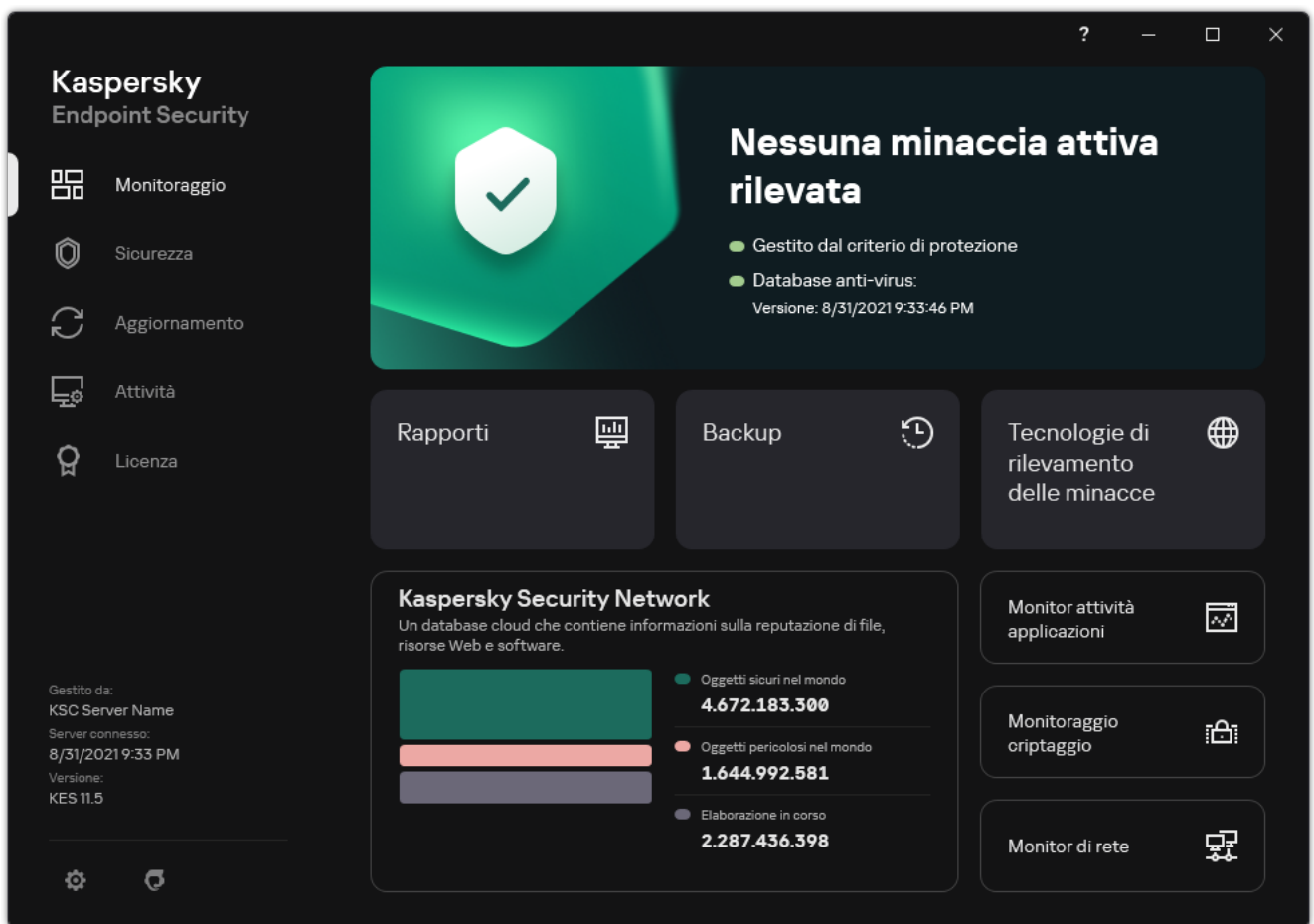
L'uso del canale TLS protegge l'applicazione fornendo le seguenti funzionalità:

- Criptaggio. I contenuti dei messaggi sono riservati e non vengono divulgati a utenti di terze parti.
- 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 certificati autofirmati. 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 l'utente sta partecipando a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla categoria e sulla reputazione dei file esaminati, nonché informazioni sulla reputazione degli indirizzi Web esaminati.
- **Monitor attività applicazioni.** Visualizzare le informazioni sul funzionamento delle applicazioni installate. Controllo sistema 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.

	<ul style="list-style-type: none"> • Monitoraggio criptaggio. Consente di monitorare il processo di criptaggio o decrittaggio 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 virus 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.

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:

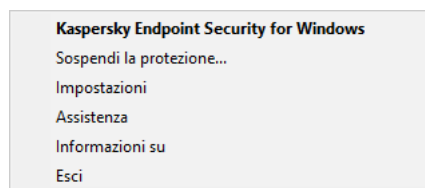
- **Kaspersky Endpoint Security for Windows.** Apre la finestra principale dell'applicazione. In questa finestra è possibile regolare il funzionamento dei componenti e delle attività dell'applicazione e visualizzare le statistiche relative ai file elaborati e alle minacce rilevate.
- **Sospendi la protezione / 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 scansione e aggiornamento. L'applicazione continua inoltre a utilizzare Kaspersky Security Network.

- **Disabilita criterio/Abilita criterio.** Disabilita 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.

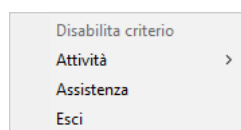


Menu di scelta rapida dell'icona dell'applicazione

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.** Disabilita 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.**
 - **Rollback alla versione precedente del database.**
 - **Scansione completa.**
 - **Scansione selettiva.**
 - **Scansione delle aree critiche.**
 - **Esegui aggiornamenti dei database.**
- **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:

- **Con 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 visualizza inoltre le notifiche sopra l'icona dell'applicazione.
- **Con interfaccia 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.
- **Nessuna interfaccia.** 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Impostazioni generali** → **Interfaccia**.
6. Nel blocco **Interazione con l'utente**, eseguire una delle seguenti operazioni:
 - Selezionare la casella di controllo **Visualizza interfaccia utente** se si desidera visualizzare i seguenti elementi dell'interfaccia nel computer client:
 - Cartella contenente il nome dell'applicazione nel menu **Start**
 - [Icona di Kaspersky Endpoint Security](#), nell'area di notifica della barra delle applicazioni di Microsoft Windows
 - Notifiche pop-up
 - Se questa casella di controllo è selezionata, l'utente può visualizzare e, a seconda dei diritti disponibili, modificare le impostazioni dell'applicazione dall'interfaccia dell'applicazione.
 - Deselezionare la casella di controllo **Visualizza interfaccia utente** se si desidera nascondere tutti gli indicatori di Kaspersky Endpoint Security nel computer client.
7. Nel blocco **Interazione con l'utente**, selezionare la casella di controllo **Visualizza interfaccia semplificata** se si desidera che l'[interfaccia dell'applicazione semplificata](#) sia visualizzata in un computer client in cui è installato Kaspersky Endpoint Security.

[Come configurare la modalità di visualizzazione dell'interfaccia dell'applicazione in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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** → **Interfaccia**.
5. Nel blocco **Interazione con l'utente**, configurare il modo in cui verrà visualizzata l'interfaccia dell'applicazione:
 - **Con 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 visualizza inoltre le notifiche sopra l'icona dell'applicazione.
 - **Con interfaccia 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.
 - **Nessuna interfaccia.** 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.
6. Salvare le modifiche.

Guida introduttiva

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* e *Scansione virus*.

L'attività *Aggiornamento* 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* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. Per creare l'attività *Aggiornamento*, installare il plug-in Web di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

L'attività *Scansione virus* è necessaria per il rilevamento tempestivo di virus e altro malware. È necessario creare manualmente l'attività *Scansione virus*.

[Come creare un'attività di scansione virus in Administration Console \(MMC\)](#) 

1. In Administration Console accedere alla cartella **Administration Server** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)** → **Scansione virus**.

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, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.
- **Disinfetta (se la disinfezione non riesce, avvisa)**. Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non è possibile, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive.
- **Avvisa**. 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.

Configurare la modalità di esecuzione dell'attività utilizzando **Esegui solo quando il computer è inattivo**. Questa casella di controllo consente di abilitare o disabilitare la funzione che sospende l'attività *Scansione virus* quando le risorse del computer sono limitate. Kaspersky Endpoint Security sospende l'attività *Scansione virus* se lo screensaver è disattivato e il computer non è bloccato.

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

Selezionare un account per l'esecuzione dell'attività *Scansione virus*. 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

Chiusura della 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 virus nei computer degli utenti in base alla pianificazione specificata.

[Come creare un'attività di scansione virus in Web Console](#) 

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

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

b. Nell'elenco a discesa **Tipo di attività** selezionare **Scansione virus**.

c. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Scansione settimanale*.

d. Nel blocco **Selezionare i 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. Chiusura della procedura guidata.

Verrà visualizzata una nuova attività nell'elenco delle attività.

6. 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.

7. Selezionare la casella di controllo accanto all'attività.

8. Fare clic sul pulsante **Esegui**.

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 virus nei computer degli utenti in base alla pianificazione specificata.

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.

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.

Criterio attivo e inattivo

Un criterio è destinato a un gruppo di computer gestiti e può essere attivo o inattivo. 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.



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.

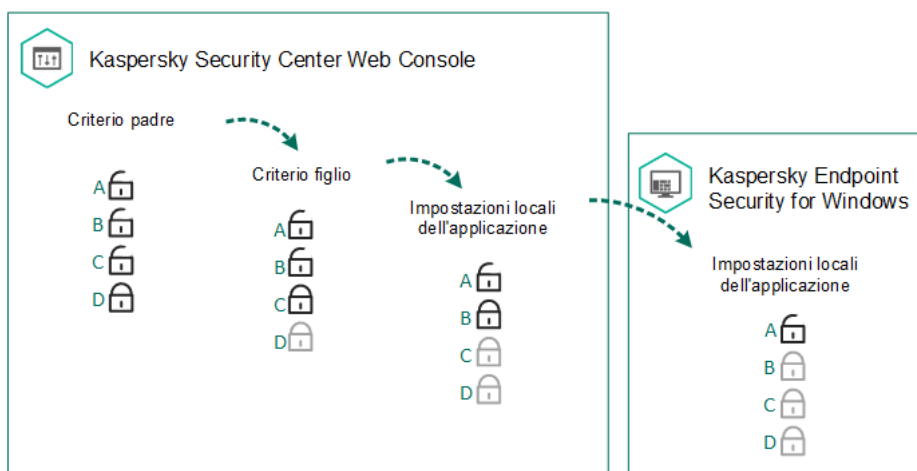
Criterio fuori sede

Un criterio fuori sede viene attivato quando un computer esce dal perimetro di rete dell'organizzazione.

Eredità impostazioni

I criteri, come i gruppi di amministrazione, sono organizzati in una gerarchia. Per impostazione predefinita, un criterio figlio eredita le impostazioni dal criterio padre. 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. È possibile disabilitare l'eredità delle impostazioni dal criterio padre.

Ogni impostazione criterio ha l'attributo , che indica se le impostazioni possono essere modificate nei criteri figlio o nelle [impostazioni locali dell'applicazione](#). L'attributo  è applicabile solo se l'ereditarietà delle impostazioni del criterio padre è abilitata per il criterio figlio. 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 dell'Administration Server di Kaspersky Security Center.



Creazione di un criterio

[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 sul pulsante **Nuovo criterio**.
Verrà avviata la Creazione guidata nuovo criterio.
5. Attenersi alle istruzioni della Creazione guidata nuovo criterio.

[Come creare un criterio in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
2. Fare clic sul pulsante **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. Nella scheda **Generale** 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.
 - **Inattivo**. Criterio di backup. Se necessario, un criterio inattivo può passare allo stato attivo.
 - **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 padre**. 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 figlio**. Se l'interruttore è attivato, i valori delle impostazioni dei criteri vengono propagati ai criteri figlio. Nelle proprietà del criterio figlio l'interruttore **Eredita impostazioni dal criterio padre** 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.
6. Nella scheda **Impostazioni applicazione** è possibile configurare le [impostazioni dei criteri di Kaspersky Endpoint Security](#).
7. Salvare le modifiche.

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](#) .

Indicatore del livello di sicurezza

L'indicatore del livello di sicurezza viene visualizzato nella parte superiore della finestra **Proprietà: <Nome criterio>**. 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.
 - **Importante.** Questa categoria include i seguenti componenti:
 - Kaspersky Security Network.
 - Protezione minacce Web.
 - Protezione minacce di posta.
 - Prevenzione Intrusioni Host.
- **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.

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 virus.** Kaspersky Endpoint Security esamina le aree del computer specificate nelle impostazioni dell'attività alla ricerca di virus e altre minacce. L'attività *Scansione Virus* 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.

- **[Aggiungere una 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 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](#)**. Kaspersky Endpoint Security aggiorna i database e i moduli dell'applicazione. L'attività *Aggiornamento* 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](#)**. 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 gli account per l'Agente di Autenticazione](#)**. Kaspersky Endpoint Security configura le impostazioni dell'account dell'Agente di Autenticazione. Per utilizzare le unità crittate è necessario un Agente di Autenticazione. Prima del caricamento del sistema operativo, l'utente deve completare l'autenticazione con l'Agente.

Le attività vengono eseguite in un computer solo se [Kaspersky Endpoint Security è in esecuzione](#).

Aggiungere una nuova 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 sul pulsante **Nuova attività**.
Verrà avviata la Creazione guidata attività.
4. Attenersi alle istruzioni della Creazione guidata attività.

[Come creare un'attività in Web Console e Cloud Console](#)

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

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

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 **Selezionare i 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. Chiusura della 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 e generazione dei rapporti** → **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](#).

Controllo 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Attività locali** → **Gestione attività**.
6. Configurare la modalità di gestione attività (vedere la tabella seguente).
7. 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 **Dispositivi** → **Criteri e profili**.
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. Accedere ad **Attività locali** → **Gestione attività**.
5. Configurare la modalità di gestione attività (vedere la tabella seguente).
6. Salvare le modifiche.

Impostazioni di Gestione attività

Parametro	Descrizione
Consenti utilizzo delle attività locali	<p>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.</p> <p>Se la casella di controllo è deselezionata, l'uso delle attività locali non è consentito. 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.</p> <p>Un utente può comunque avviare una scansione virus 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.</p>
Consenti la visualizzazione delle attività di gruppo	<p>Se la casella di controllo è selezionata, le attività del gruppo vengono visualizzate nell'interfaccia locale di Kaspersky Endpoint Security. L'utente può visualizzare l'elenco di tutte le attività nell'interfaccia dell'applicazione.</p>

	Se la casella di controllo è deselezionata, Kaspersky Endpoint Security visualizza un elenco di attività vuoto.
Consenti la gestione delle attività di gruppo	<p>Se la casella di controllo è selezionata, gli utenti possono avviare e arrestare le attività di gruppo specificate in Kaspersky Security Center. Gli utenti possono avviare e arrestare le attività nell'interfaccia dell'applicazione o nell'interfaccia dell'applicazione semplificata.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security avvia automaticamente le attività pianificate oppure l'amministratore avvia le attività manualmente in Kaspersky Security Center.</p>

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 appartiene il computer client desiderato.
3. Nell'area di lavoro selezionare la scheda **Dispositivi**.
4. Selezionare il computer per cui si desidera configurare le impostazioni di Kaspersky Endpoint Security.
5. Dal menu di scelta rapida del computer client selezionare **Proprietà**.
Verrà visualizzata la finestra delle proprietà del computer client.
6. Nella finestra delle proprietà del computer client selezionare la sezione **Applicazioni**.
Nella parte destra della finestra delle proprietà del computer client verrà visualizzato un elenco delle applicazioni Kaspersky installate nel computer client.
7. Selezionare Kaspersky Endpoint Security.
8. Fare clic sul pulsante **Proprietà** sotto l'elenco delle applicazioni Kaspersky.
Si apre la finestra delle **impostazioni dell'applicazione Kaspersky Endpoint Security for Windows**.
9. Nella sezione **Impostazioni generali**, configurare Kaspersky Endpoint Security e Rapporti e archivi.
Le altre sezioni della finestra delle **impostazioni dell'applicazione Kaspersky Endpoint Security for Windows** 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**.

10. Salvare le modifiche.

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Dispositivi gestiti**.
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**.
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.

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Impostazioni generali** → **Impostazioni applicazione**.
6. Utilizzare la casella di controllo **Avvia Kaspersky Endpoint Security for Windows all'avvio del computer** per configurare l'avvio dell'applicazione.
7. Salvare le modifiche.

[Come configurare l'avvio di Kaspersky Endpoint Security in Web Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 applicazione**.
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**.
3. Utilizzare la casella di controllo **Avvia Kaspersky Endpoint Security for Windows all'avvio del computer** 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 appartiene il computer client desiderato.
3. Nell'area di lavoro selezionare la scheda **Dispositivi**.
4. Selezionare il computer in cui si desidera avviare o arrestare l'applicazione.
5. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida del computer client, quindi selezionare **Proprietà**.
6. Nella finestra delle proprietà del computer client selezionare la sezione **Applicazioni**.
Nella parte destra della finestra delle proprietà del computer client verrà visualizzato un elenco delle applicazioni Kaspersky installate nel computer client.
7. Selezionare Kaspersky Endpoint Security.
8. Eseguire le 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, selezionare **Dispositivi** → **Dispositivi gestiti**.
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 **Interrompi**.

[Come avviare o arrestare Kaspersky Endpoint Security dalla riga di comando](#)

Per arrestare l'applicazione dalla riga di comando, [abilitare la gestione esterna dei servizi di sistema](#).



Il file klpsm.exe, incluso nel kit di distribuzione di Kaspersky Endpoint Security, viene utilizzato per avviare o arrestare l'applicazione 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. 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`.

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.

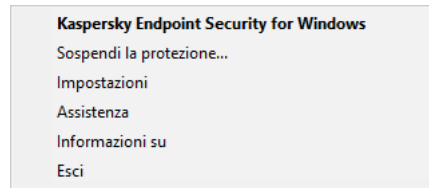
Se sono già state stabilite connessioni di rete quando si sospendono o si riprendono la protezione e il controllo del computer, viene visualizzata una notifica dell'interruzione di tali connessioni di rete.

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 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.
A tale scopo, è necessario salvare il file di configurazione nella stessa cartella in cui è disponibile il pacchetto di distribuzione.
- Eseguire l'installazione remota di Kaspersky Endpoint Security tramite Kaspersky Security Center con le impostazioni predefinite.
- Eseguire la migrazione delle impostazioni di Kaspersky Endpoint Security da un computer a un altro.


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. 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.

5. Salvare il file.

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. Aprire il file.

Tutti i valori delle impostazioni di Kaspersky Endpoint Security saranno configurati in base al file di configurazione selezionato.

Ripristino delle impostazioni predefinite dell'applicazione

È possibile ripristinare in qualsiasi momento le impostazioni consigliate da Kaspersky per Endpoint Security. 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.

Scansione virus del computer

Una scansione virus è essenziale per la sicurezza del computer. L'esecuzione periodica delle scansioni virus 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 dell'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 dell'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
- Cassetta postale di Microsoft Outlook
- 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 visualizza 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

Kaspersky Endpoint Security verifica se i moduli dell'applicazione risultano danneggiati o modificati.

Scansione del computer

Una scansione virus è essenziale per la sicurezza del computer. L'esecuzione periodica delle scansioni virus 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 attività standard *Scansione completa*, *Scansione delle aree critiche*, *Scansione personalizzata* predefinite. Se l'organizzazione ha distribuito il sistema di amministrazione di Kaspersky Security Center, è possibile [creare un'attività Scansione virus](#) e configurare la scansione. L'[attività Scansione in background](#) è disponibile anche in Kaspersky Security Center. La scansione in background non può essere configurata.

[Come eseguire una scansione virus 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.
Se necessario, [creare un'attività Scansione virus](#).
5. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.
6. Configurare l'attività di scansione (vedere la tabella riportata di seguito).
Se necessario, [configurare la pianificazione dell'attività di scansione](#).
7. Salvare le modifiche.
8. 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 una scansione virus in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **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 una scansione virus 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 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**. Se l'attività di scansione non viene visualizzata, significa che l'amministratore [ha vietato l'uso delle attività locali nel criterio](#).

Impostazioni di scansione

Parametro	Descrizione
Livello di sicurezza	<p>Kaspersky Endpoint Security può utilizzare diversi gruppi di impostazioni per eseguire una scansione. I gruppi di impostazioni archiviate nell'applicazione sono denominati <i>livelli di protezione</i>:</p> <ul style="list-style-type: none"> • Alto. Kaspersky Endpoint Security esegue la scansione di tutti i tipi di file. Durante la scansione dei file composti, vengono esaminati anche i file in formato e-mail. • Consigliato. Kaspersky Endpoint Security esamina solo i formati di file specificati in tutti i dischi rigidi, le unità di rete e i supporti rimovibili del computer, oltre agli oggetti OLE incorporati. Kaspersky Endpoint Security non viene eseguita la scansione degli archivi o dei pacchetti di installazione. • Basso. Kaspersky Endpoint Security esamina solo i file nuovi o modificati con le estensioni specificate in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer. Non viene eseguita la scansione dei file composti. <p>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.</p>
Azione se viene rilevata una minaccia	<p>Disinfetta (se non è possibile, elimina). Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.</p> <p>Disinfetta (se non è possibile, blocca). Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non è possibile, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive.</p> <p>Notifica. 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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Prima di tentare di disinfettare o eliminare un file infetto, Kaspersky Endpoint Security crea una copia di backup del file nel caso in cui sia necessario ripristinare il file o se può essere disinfettato in futuro.</p> </div>

	<p>Se vengono rilevati file infetti che fanno parte dell'applicazione Windows Store, Kaspersky Endpoint Security tenta di eliminare il file.</p>
<p>Esegui immediatamente Disinfezione avanzata</p> <p><i>(disponibile solo in Kaspersky Security Center Console)</i></p>	<p>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.</p> <p>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.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non rimuove 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.</p>
<p>Ambito della scansione</p>	<p>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, database di posta, disco rigido, unità rimovibile o unità di rete, cartelle o file.</p>
<p>Pianificazione scansione</p>	<p>Manualmente. Modalità di esecuzione in cui è possibile avviare la scansione manualmente nel momento più opportuno.</p> <p>In base alla pianificazione. In questa modalità di esecuzione dell'attività di scansione, Kaspersky Endpoint Security 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.</p>
<p>Rimanda l'esecuzione dopo l'avvio dell'applicazione di N minuti</p>	<p>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.</p>
<p>Esegui attività ignorate</p>	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security avvia l'attività di scansione ignorata appena possibile. L'attività di scansione può ad esempio essere ignorata se il computer è spento all'orario impostato per l'avvio dell'attività di scansione pianificata. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non esegue le attività di scansione ignorate. Viene invece eseguita l'attività di scansione successiva, in base alla pianificazione corrente.</p>
<p>Esegui solo quando il computer è inattivo</p>	<p>Avvio posticipato dell'attività di scansione 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.</p>
<p>Esegui scansione come</p>	<p>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 di Kaspersky Endpoint Security ed eseguire l'attività di scansione tramite l'account di questo utente.</p>

<p>Tipi di file</p>	<div data-bbox="411 125 1493 286" style="border: 1px solid black; padding: 5px;"> <p>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.</p> </div> <p>Tutti i file. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina tutti i file senza eccezioni (tutti i formati e le estensioni).</p> <p>File esaminati per formato. Se questa impostazione è abilitata, Kaspersky Endpoint Security 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.</p> <p>File esaminati per estensione. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina solo i file infettabili. Il formato del file viene quindi determinato in base all'estensione.</p> <p>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).</p>
<p>Esamina solo i file nuovi e modificati</p>	<p>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 composti.</p>
<p>Ignora oggetti esaminati per più di N secondi.</p>	<p>Viene impostato un limite di tempo per la scansione di un singolo oggetto. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security interrompe la scansione di un file. Questo consente di ridurre la durata di una scansione.</p>
<p>Esamina gli archivi</p>	<p>Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. Kaspersky Endpoint Security 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).</p>
<p>Esamina i pacchetti di distribuzione</p>	<p>Questa casella di controllo consente di abilitare o disabilitare la scansione dei pacchetti di distribuzione di terze parti.</p>
<p>Esamina i file nei formati Microsoft Office</p>	<p>Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE.</p>
<p>Esamina i formati e-mail</p>	<p>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/Outlook Express, nonché i file EML.</p> <div data-bbox="411 1697 1493 1928" style="border: 1px solid black; padding: 5px;"> <p>Kaspersky Endpoint Security non supporta la versione a 64 bit del client di posta elettronica MS Outlook. Di conseguenza, Kaspersky Endpoint Security non esegue la scansione dei file MS Outlook (file PST e OST) se nel computer è installata una versione a 64 bit di MS Outlook, anche se la posta è inclusa nell'ambito della scansione.</p> </div> <p>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.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security analizza il file in formato e-mail come un singolo file.</p>

<p>Esamina gli archivi protetti da password</p>	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security esamina gli archivi protetti tramite password. Prima di eseguire la scansione dei file in un archivio, viene richiesto di immettere la password.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security ignora la scansione degli archivi protetti tramite password.</p>
<p>Non decomprimere i file composti di grandi dimensioni</p>	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security non esegue la scansione dei file composti se la loro dimensione supera il valore specificato.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esamina i file composti di qualsiasi dimensione.</p> <p>Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.</p>
<p>Machine Learning e analisi delle firme</p>	<p>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.</p> <p>In base ai suggerimenti degli esperti Kaspersky, il metodo Machine Learning e analisi delle firme è sempre abilitato.</p>
<p>Analisi euristica</p>	<p>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.</p> <p>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.</p>
<p>Tecnologia iSwift</p> <p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalla scansione 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.</p>
<p>Tecnologia iChecker</p> <p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>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).</p>

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio, selezionare **Attività locali** → **Scansione unità rimovibili**.
6. Nell'elenco a discesa **Azione da eseguire quando viene connessa un'unità rimovibile**, 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 in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 ad **Attività locali** → **Scansione unità rimovibili**.
5. Nell'elenco a discesa **Azione da eseguire quando viene connessa un'unità rimovibile**, selezionare **Scansione dettagliata** o **Scansione rapida**.
6. Configurare le opzioni avanzate per Scansione unità rimovibili (vedere la tabella riportata di seguito).
7. 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'utilizzo delle attività locali nel criterio](#).

Impostazioni dell'attività Scansione unità rimovibili

Parametro	Descrizione
Azione da eseguire quando viene connessa un'unità rimovibile	<p>Scansione dettagliata. Se questa voce è selezionata, quando viene connessa un'unità rimovibile Kaspersky Endpoint Security esamina tutti i file nell'unità rimovibile, 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.</p> <p>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 decompri-me gli oggetti compositi.</p>
Dimensione massima unità rimovibile	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security esegue l'azione selezionata nell'elenco a discesa Azione da eseguire quando viene connessa un'unità rimovibile sulle unità rimovibili con una dimensione inferiore alla dimensione massima specificata.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esegue l'azione selezionata nell'elenco a discesa Azione da eseguire quando viene connessa un'unità rimovibile sulle unità rimovibili di qualsiasi dimensione.</p>
Mostra stato di avanzamento scansione	<p>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.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esegue la scansione delle unità rimovibili in background.</p>
Impedisci l'arresto dell'attività di scansione	<p>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.</p>

Scansione in background

Scansione in background è una modalità di scansione di Kaspersky Endpoint Security che non visualizza 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. 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio, selezionare **Attività locali** → **Scansione in background**.
6. Utilizzare la casella di controllo **Abilita scansione in background** per abilitare o disabilitare la scansione in background.
7. Salvare le modifiche.

[Come abilitare la scansione in background in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 ad **Attività locali** → **Scansione in background**.
5. Utilizzare la casella di controllo **Abilita scansione in background** per abilitare o disabilitare la scansione in background.
6. Salvare le modifiche.

Come abilitare la scansione in background nell'interfaccia dell'applicazione

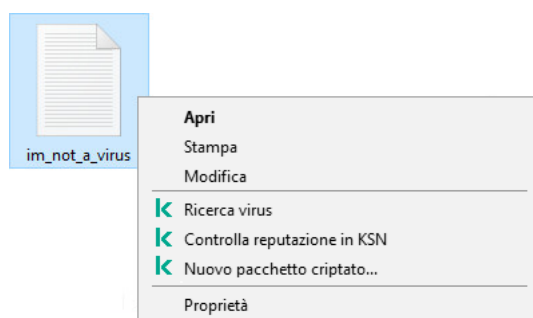
1. Nella finestra principale dell'applicazione, andare alla sezione **Attività**.
2. Nell'elenco delle attività, selezionare l'attività di scansione e fare clic su .
3. Utilizzare l'interruttore **Scansione in background** per abilitare o disabilitare le scansioni in background.
4. Salvare le modifiche.

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Attività locali** → **Scansione dal menu di scelta rapida**.
6. Configurare Scansione dal menu di scelta rapida (vedere la tabella riportata di seguito).
7. Salvare le modifiche.

Come configurare Scansione dal menu di scelta rapida in Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 ad **Attività locali** → **Scansione dal menu di scelta rapida**.
5. 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'utilizzo 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 <i>livelli di protezione</i> :

	<ul style="list-style-type: none"> • Alto. Kaspersky Endpoint Security esegue la scansione di tutti i tipi di file. Durante la scansione dei file composti, vengono esaminati anche i file in formato e-mail. • Consigliato. Kaspersky Endpoint Security esamina solo i formati di file specificati in tutti i dischi rigidi, le unità di rete e i supporti rimovibili del computer, oltre agli oggetti OLE incorporati. Kaspersky Endpoint Security non viene eseguita la scansione degli archivi o dei pacchetti di installazione. • Basso. Kaspersky Endpoint Security esamina solo i file nuovi o modificati con le estensioni specificate in tutti i dischi rigidi, le unità rimovibili e le unità di rete del computer. Non viene eseguita la scansione dei file composti.
Azione se viene rilevata una minaccia	<p>Disinfetta (se non è possibile, elimina). Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.</p> <p>Disinfetta (se non è possibile, blocca). Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non è possibile, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive.</p> <p>Notifica. 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.</p>
Tipi di file	<div style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>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.</p> </div> <p>Tutti i file. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina tutti i file senza eccezioni (tutti i formati e le estensioni).</p> <p>File esaminati per formato. Se questa impostazione è abilitata, Kaspersky Endpoint Security 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.</p> <p>File esaminati per estensione. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina solo i file infettabili . Il formato del file viene quindi determinato in base all'estensione.</p> <p>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).</p>
Esamina solo i file nuovi e modificati	<p>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 composti.</p>
Ignora oggetti esaminati per più di N secondi.	<p>Viene impostato un limite di tempo per la scansione di un singolo oggetto. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security interrompe la scansione di un file. Questo consente di ridurre la durata di una scansione.</p>
Esamina gli archivi	<p>Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. Kaspersky Endpoint Security 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).</p>
Esamina i	<p>Questa casella di controllo consente di abilitare o disabilitare la scansione dei pacchetti di</p>

pacchetti di distribuzione	distribuzione.
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.
Esamina i formati e-mail	<p>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/Outlook Express, nonché i file EML.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Kaspersky Endpoint Security non supporta la versione a 64 bit del client di posta elettronica MS Outlook. Di conseguenza, Kaspersky Endpoint Security non esegue la scansione dei file MS Outlook (file PST e OST) se nel computer è installata una versione a 64 bit di MS Outlook, anche se la posta è inclusa nell'ambito della scansione.</p> </div> <p>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.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security analizza il file in formato e-mail come un singolo file.</p>
Esamina gli archivi protetti da password	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security esamina gli archivi protetti tramite password. Prima di eseguire la scansione dei file in un archivio, viene richiesto di immettere la password.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security ignora la scansione degli archivi protetti tramite password.</p>
Non decomprimere i file composti di grandi dimensioni	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security non esegue la scansione dei file composti se la loro dimensione supera il valore specificato.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esamina i file composti di qualsiasi dimensione.</p> <p>Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.</p>
Machine Learning e analisi delle firme	<p>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.</p> <p>In base ai suggerimenti degli esperti Kaspersky, il metodo Machine Learning e analisi delle firme è sempre abilitato.</p>
Analisi euristica	<p>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.</p> <p>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.</p>
Tecnologia	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla

iSwift	scansione. I file vengono esclusi dalla scansione 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).

Application Integrity Control

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* serve a esaminare i file delle applicazioni. Eseguire l'attività *Controllo integrità* se Kaspersky Endpoint Security ha rilevato un oggetto dannoso ma non lo ha neutralizzato.

È possibile creare l'attività *Controllo integrità* 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. In Administration Console accedere alla cartella **Administration Server** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)** → **Controllo integrità**.

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

Chiusura della 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 **Dispositivi** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

b. Nell'elenco a discesa **Tipo di attività** selezionare **Controllo integrità**.

c. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Controllare l'integrità dell'applicazione dopo un'infezione del computer*.

d. Nel blocco **Selezionare i 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. Chiusura della procedura guidata.

Verrà visualizzata una nuova attività nell'elenco delle attività.

6. 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* e fare clic **Esegui scansione**.

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 *Controllo integrità* non viene visualizzato, significa che l'amministratore [ha vietato l'utilizzo 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, Kaspersky Endpoint Security 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	Se la casella di controllo è selezionata, Kaspersky Endpoint Security avvia l'attività di

attività ignorate	scansione ignorata appena possibile. L'attività di scansione può ad esempio essere ignorata se il computer è spento all'orario impostato per l'avvio dell'attività di scansione pianificata. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non esegue le attività di scansione ignorate. Viene invece eseguita l'attività di scansione successiva, in base alla pianificazione corrente.
Esegui solo quando il computer è inattivo	Avvio posticipato dell'attività di scansione 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.

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:

- **E-mail.**
File pertinenti per il client di posta Outlook: file di dati (PST), file di dati offline (OST).
- **Memoria del sistema.**
- **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.**

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 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.
Se necessario, [creare un'attività Scansione virus](#).
5. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.
6. Nella sezione **Ambito della scansione**, fare clic su **Impostazioni**.
7. Nella finestra visualizzata, selezionare gli oggetti che si desidera aggiungere o escludere dall'ambito della scansione.
8. 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 l'estensione TXT situati nella cartella denominata `Cartella` e nelle relative sottocartelle. 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 `Cartella` con l'estensione TXT e un nome composto da tre caratteri.

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.

9. Salvare le modifiche.

[Come modificare un'ambito della scansione in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **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 un'attività Scansione virus](#).

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 sul pulsante **Aggiungi**.

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 l'estensione TXT situati nella cartella denominata `Cartella` e nelle relative sottocartelle. 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 `Cartella` con l'estensione TXT e un nome composto da tre caratteri.

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. Nell'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 completa del computer richiede tempo e risorse del computer. Si consiglia di scegliere un momento ottimale per eseguire una scansione del computer, al fine di evitare di influire negativamente sulle prestazioni delle altre applicazioni software. Kaspersky Endpoint Security consente di configurare una normale pianificazione per la scansione del computer. Questa funzionalità risulta comoda se l'organizzazione segue un programma di lavoro. È possibile configurare una scansione del computer affinché venga eseguita di notte o nei fine settimana. Se per qualsiasi motivo non è possibile eseguire l'attività di scansione, 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.

Se la configurazione di una pianificazione della scansione si rivela impossibile, Kaspersky Endpoint Security consente di eseguire una scansione del computer quando si soddisfano le seguenti condizioni:

- 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 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.

- Riattivazione LAN.

Kaspersky Endpoint Security esegue una scansione del computer pianificata anche se il computer è spento. A tale scopo, l'applicazione utilizza la funzionalità di riattivazione LAN del sistema operativo. La funzionalità di riattivazione LAN consente di accendere il computer da remoto inviando un segnale speciale sulla rete locale. Per utilizzare questa funzionalità, è necessario abilitare la riattivazione LAN nelle impostazioni BIOS.

È possibile configurare l'esecuzione della scansione con la riattivazione LAN solo per l'attività *Scansione virus* in Kaspersky Security Center. Non è possibile abilitare la riattivazione 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. Di conseguenza, potrebbero essere necessari diversi giorni prima che l'applicazione completi la scansione completa del computer.

[Come configurare la pianificazione della scansione 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.
Se necessario, [creare un'attività Scansione virus](#).
5. Nella finestra delle proprietà dell'attività, selezionare la sezione **Pianificazione**.
6. Configurare la pianificazione dell'attività di scansione.
7. A seconda della frequenza selezionata, configurare le impostazioni avanzate che specificano la pianificazione di esecuzione dell'attività (vedere la tabella riportata di seguito).
8. Salvare le modifiche.


[Come configurare la pianificazione della scansione in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **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 **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 virus* 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 **Programma 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	<p>Manualmente. Modalità di esecuzione in cui è possibile avviare la scansione manualmente nel momento più opportuno.</p> <p>In base alla pianificazione. In questa modalità di esecuzione dell'attività di scansione, Kaspersky Endpoint Security 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.</p>
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 di scansione ignorata appena possibile. L'attività di scansione può ad esempio essere ignorata se il computer è spento all'orario impostato per l'avvio dell'attività di scansione pianificata. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non esegue le attività di scansione ignorate. Viene invece eseguita l'attività di scansione successiva, in base alla pianificazione corrente.
Esegui solo quando il computer è inattivo	Avvio posticipato dell'attività di scansione 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.
Usa automaticamente il ritardo casuale per l'avvio delle attività	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.

<p><i>(disponibile solo in Kaspersky Security Center Console)</i></p>	<p>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.</p> <p>Se la casella di controllo è deselezionata, l'attività viene eseguita esattamente all'ora pianificata.</p>
<p>Arresta l'attività se è in esecuzione da più di (min.)</p> <p><i>(disponibile solo in Kaspersky Security Center Console)</i></p>	<p>Limitazione della durata di esecuzione dell'attività. Trascorso il 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.</p> <p>Per ridurre il tempo di esecuzione dell'attività, è possibile, ad esempio, configurare l'ambito della scansione oppure ottimizzare la scansione.</p>
<p>Attiva il dispositivo prima dell'avvio dell'attività tramite Wake-on-LAN (min.)</p> <p><i>(disponibile solo in Kaspersky Security Center Console)</i></p>	<p>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.</p> <p>Selezionare la casella di controllo se si desidera eseguire l'attività su tutti i computer, inclusi quelli spenti.</p>

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 di Kaspersky Endpoint Security 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, selezionare **Dispositivi** → **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 su **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

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 composti. 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 composti, come ad esempio archivi o database. Per rilevare i virus e il malware nascosti in questo modo, è necessario decomprimere il file composto, cosa che può rallentare la scansione. È possibile limitare i tipi di file composti 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 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.
Se necessario, [creare un'attività Scansione virus](#).
5. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.
6. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
Si apre la finestra delle impostazioni dell'attività di scansione.
7. Nella sezione **Ottimizzazione della scansione** 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 composti.
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.** Consente di impostare un limite di tempo per la scansione di un singolo oggetto. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security interrompe la scansione di un file. Questo consente di ridurre la durata di una scansione.
8. Fare clic su **Avanzate**.
Si apre la finestra delle impostazioni di scansione dei file composti.
9. Nel blocco **Dimensione massima**, selezionare la casella di controllo **Non decomprimere i file composti di grandi dimensioni**. Viene impostato un limite di tempo per la scansione di un singolo oggetto. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security interrompe la scansione di un file. Questo consente di ridurre la durata di una scansione.

Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi, indipendentemente dal fatto che la casella di controllo **Non decomprimere i file composti di grandi dimensioni** sia selezionata o meno.

10. Fare clic su **OK**.
11. Selezionare la scheda **Avanzate**.
12. 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 dalla scansione 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).

13. Salvare le modifiche.

[Come ottimizzare la scansione in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **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 un'attività Scansione virus](#).

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

4. Nel blocco **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 composti.

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. Selezionare la casella di controllo **Non decomprimere i file composti di grandi dimensioni**. Viene impostato un limite di tempo per la scansione di un singolo oggetto. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security interrompe la scansione di un file. Questo consente di ridurre la durata di una scansione.

Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi, indipendentemente dal fatto che la casella di controllo **Non decomprimere i file composti di grandi dimensioni** sia selezionata o meno.

6. Nel blocco **Impostazioni avanzate**, selezionare la casella di controllo **Ignora i file esaminati per più di N sec**. Viene impostato un limite di tempo per la scansione di un singolo oggetto. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security interrompe la scansione di un file. Questo consente di ridurre la durata di una scansione.

7. 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. Nella sezione **Ottimizzazione della scansione** 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 oggetti esaminati per più di N secondi.** Viene impostato un limite di tempo per la scansione di un singolo oggetto. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security interrompe la scansione di un file. Questo consente di ridurre la durata di una scansione.
5. Nel blocco **Dimensione massima**, selezionare la casella di controllo **Non decomprimere i file compositi di grandi dimensioni**. Viene impostato un limite di tempo per la scansione di un singolo oggetto. Al termine del periodo di tempo specificato, Kaspersky Endpoint Security interrompe la scansione di un file. Questo consente di ridurre la durata di una scansione.

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 dalla scansione 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.

Gli aggiornamenti periodici richiedono una licenza valida. Se non è disponibile alcuna licenza, è possibile eseguire un aggiornamento una sola volta.

La principale sorgente degli aggiornamenti per Kaspersky Endpoint Security è costituita dai server degli aggiornamenti Kaspersky.

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.

I file della Guida sensibile al contesto possono essere aggiornati insieme agli aggiornamenti dei moduli dell'applicazione.

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](#).

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.

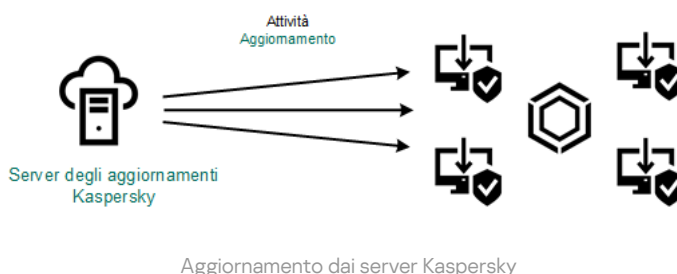
I seguenti oggetti vengono aggiornati nei computer degli utenti:

- 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 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 *Download degli aggiornamenti nell'archivio di Administration Server*.

2. Scaricare il pacchetto di aggiornamenti in una cartella condivisa (opzione facoltativa).

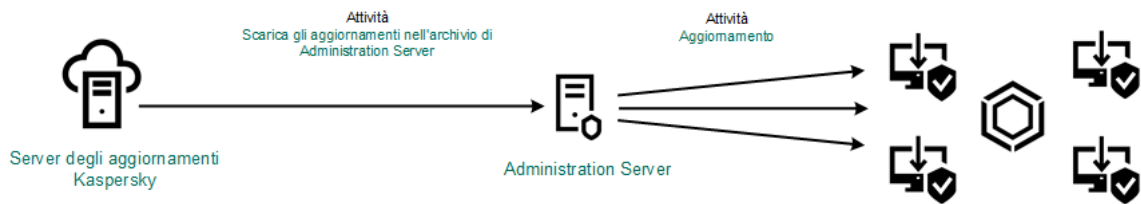
È possibile scaricare il pacchetto di aggiornamenti in una cartella condivisa utilizzando i seguenti metodi:

- Utilizzando l'attività *Aggiornamento* di Kaspersky Endpoint Security. L'attività è destinata a uno dei computer della rete locale dell'azienda.

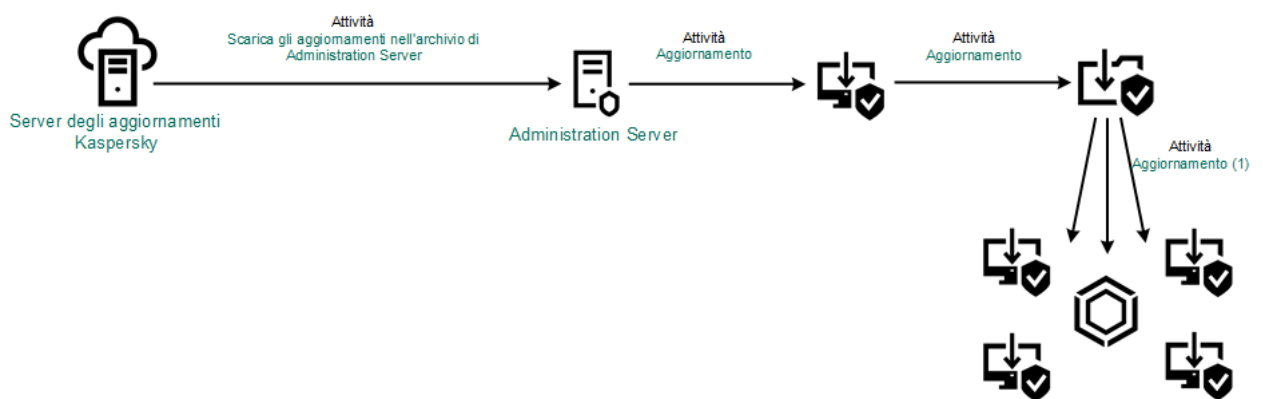
- Tramite Kaspersky Update Utility. Per informazioni dettagliate sull'utilizzo di Kaspersky Update Utility, consultare la [Knowledge Base di Kaspersky](#).

3. Distribuire il pacchetto di aggiornamenti ai computer client.

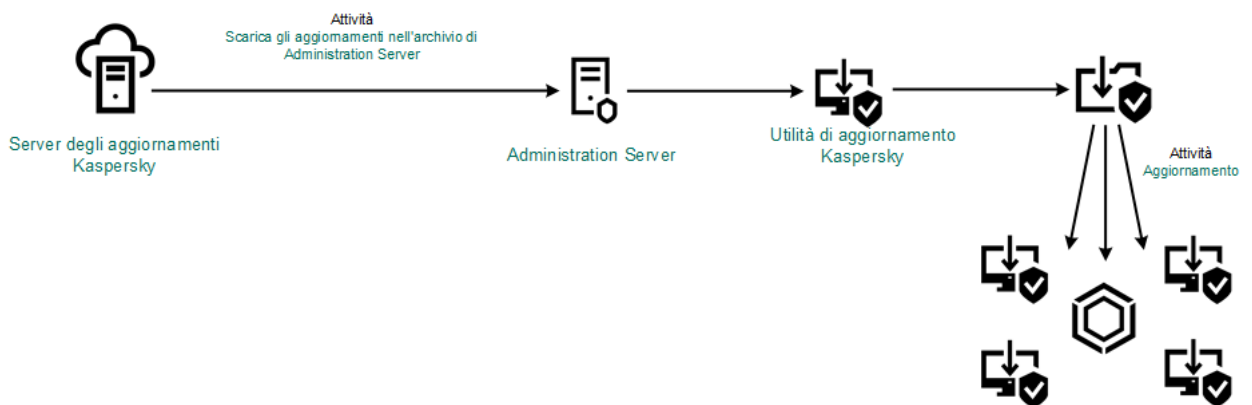
Il pacchetto di aggiornamenti viene distribuito ai computer client da parte dell'attività *Aggiornamento* di Kaspersky Endpoint Security. È possibile creare un numero illimitato di attività di aggiornamento per ogni gruppo di amministrazione.



Aggiornamento da un archivio server



Aggiornamento da una cartella condivisa



Aggiornamento tramite Kaspersky Update Utility

Per Web Console 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.

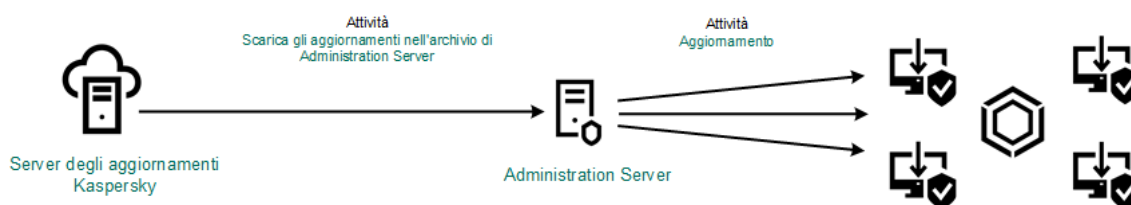
Gli aggiornamenti vengono scaricati dai server degli aggiornamenti Kaspersky o da altri server FTP o HTTP tramite i protocolli di rete standard. Se la connessione a un server proxy è necessaria per l'accesso alla sorgente degli aggiornamenti, [specificare le impostazioni del server proxy nel criterio 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 gli aggiornamenti nell'archivio di Administration Server*).
2. Configurare gli aggiornamenti dei database e dei moduli dell'applicazione dall'archivio server specificato negli altri computer della LAN aziendale (attività *Aggiornamento*).



Aggiornamento da un archivio server

Per configurare il download di un pacchetto di aggiornamenti nell'archivio server:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Attività**.
Viene aperto l'elenco delle attività.
2. Selezionare l'attività di Administration Server **Scarica aggiornamenti nell'archivio dell'Administration Server**.
Verrà visualizzata la finestra delle proprietà dell'attività.
L'attività di Administration Server *Scarica aggiornamenti nell'archivio dell'Administration Server* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center Web Console e può avere solo un'istanza.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Nel blocco **Altre impostazioni**, fare clic su **Configura**.
5. Nel campo **Cartella per l'archiviazione degli aggiornamenti**, specificare l'indirizzo del server FTP o HTTP, la cartella di rete o la cartella locale in cui Kaspersky Security Center copia il pacchetto degli aggiornamenti ricevuto dai server degli aggiornamenti Kaspersky.

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://dn1-01.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://<nome utente>:<password>@<nodo>:<porta>`.
- 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\AVP11\Update distribution\.

6. Salvare le modifiche.

Per configurare l'aggiornamento di Kaspersky Endpoint Security dall'archivio server specificato:

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

Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Aggiornamento** per Kaspersky Endpoint Security.

Verrà visualizzata la finestra delle proprietà dell'attività.

L'attività *Aggiornamento* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. Per creare l'attività *Aggiornamento*, installare il plug-in Web 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. Nel campo **Sorgente** 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 (vedere *le istruzioni riportate sopra*).

6. Nel blocco **Stato**, selezionare **Abilitato**.

7. Fare clic su **OK**.

8. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

9. Salvare le modifiche.

Se un aggiornamento non può essere eseguito dalla prima sorgente degli aggiornamenti, Kaspersky Endpoint Security passa automaticamente alla sorgente successiva.

Aggiornamento da una cartella condivisa

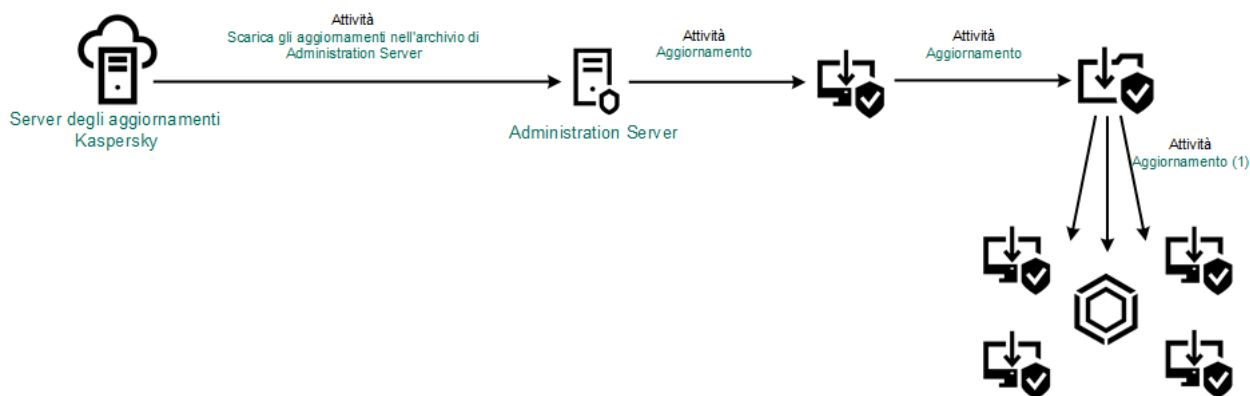
Per ridurre il traffico Internet, è possibile configurare gli aggiornamenti dei database e dei moduli dell'applicazione nei computer della LAN aziendale da una cartella condivisa. A tale scopo, uno dei computer della LAN aziendale deve ricevere i pacchetti degli aggiornamenti da Kaspersky Security Center 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 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. Abilitare la copia di un pacchetto di aggiornamento in una cartella condivisa in uno dei computer nella rete LAN aziendale (vedere le istruzioni di seguito).
3. Configurare gli aggiornamenti dei database e dei moduli dell'applicazione dalla cartella condivisa specificata negli altri computer della rete LAN aziendale (vedere le istruzioni di seguito).

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.



Aggiornamento da una cartella condivisa

Per abilitare la copia del pacchetto di aggiornamento nella cartella condivisa:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **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** per Kaspersky Endpoint Security.

Verrà visualizzata la finestra delle proprietà dell'attività.

L'attività *Aggiornamento* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. Per creare l'attività *Aggiornamento*, installare il plug-in Web 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\Share\Update distribution).

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\AVP11\Update distribution\.

7. Salvare le modifiche.

Per configurare gli aggiornamenti da una cartella condivisa:

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

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

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 **Selezionare i 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. Chiusura della procedura guidata.

Verrà visualizzata una nuova attività nella tabella delle attività.

6. Fare clic sulla nuova attività creata *Aggiornamento*.

Verrà visualizzata la finestra delle proprietà dell'attività.

7. Accedere alla sezione **Impostazioni applicazione**.

8. Selezionare la scheda **Modalità locale**.

9. Nel blocco **Sorgente degli aggiornamenti**, fare clic su **Aggiungi**.

10. Nel campo **Sorgente** 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*).

11. Fare clic su **OK**.

12. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.

13. Salvare le modifiche.

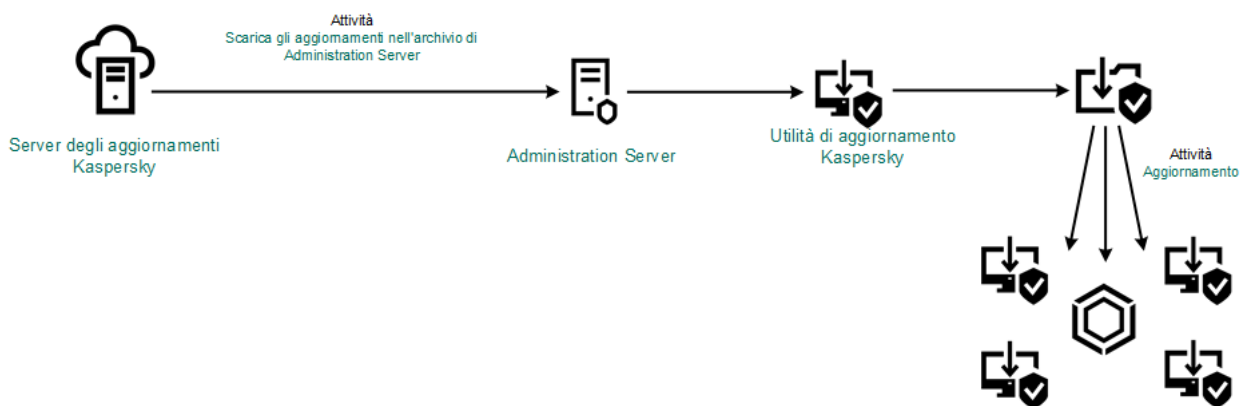
Aggiornamento tramite Kaspersky Update Utility

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 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.
4. Configurare gli aggiornamenti dei database e dei moduli dell'applicazione dalla cartella condivisa specificata negli altri computer della LAN aziendale.

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.



Aggiornamento tramite 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](#).

Per configurare gli aggiornamenti da una cartella condivisa:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Attività**. Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Aggiornamento** per Kaspersky Endpoint Security.

Verrà visualizzata la finestra delle proprietà dell'attività.

L'attività *Aggiornamento* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. Per creare l'attività *Aggiornamento*, installare il plug-in Web 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. Nel campo **Sorgente**, immettere il percorso UNC della cartella condivisa (ad esempio, \\Server\Share\Update distribution).

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**.

8. Salvare le modifiche.

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.

Per configurare le impostazioni di aggiornamento per la modalità mobile:

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

Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Aggiornamento** per Kaspersky Endpoint Security.

Verrà visualizzata la finestra delle proprietà dell'attività.

L'attività *Aggiornamento* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. Per creare l'attività *Aggiornamento*, installare il plug-in Web di Kaspersky Endpoint Security for Windows mentre è in esecuzione la procedura guidata.

Selezionare la scheda **Impostazioni applicazione** → **Modalità mobile**.

3. 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.

4. 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 **Aggiorna**.
2. Nel riquadro **Aggiornamento di database e moduli dell'applicazione**, fare clic sul pulsante **Aggiorna** 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 **Interrompere l'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 di Kaspersky Endpoint Security 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:

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiorna**.
2. Si apre l'elenco delle attività; selezionare l'attività di aggiornamento e fare clic su .
3. Fare clic su **Esegui aggiornamenti dei database con 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:

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiorna**.
2. Si apre l'elenco delle attività; selezionare l'attività di aggiornamento e fare clic su .
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.
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.

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 aggiungere una sorgente degli aggiornamenti:

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiorna**.
2. Si apre l'elenco delle attività; selezionare l'attività di aggiornamento e fare clic su .
3. Fare clic sul pulsante **Seleziona sorgente degli aggiornamenti**.
4. Nella finestra visualizzata, 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://dn1-01.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://<nome utente>:<password>@<nodo>:<porta>`.
- 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\AVP11\Update distribution\`.

6. Fare clic sul pulsante **Seleziona**.
7. Configurare le priorità delle sorgenti degli aggiornamenti utilizzando i pulsanti **Su** e **Giù**.
8. Salvare le modifiche.


Configurazione degli aggiornamenti 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 configurazione degli aggiornamenti dei database e dei moduli dell'applicazione da una cartella condivisa comprende i seguenti passaggi:

1. L'abilitazione della copia di un pacchetto di aggiornamento in una cartella condivisa in uno dei computer nella rete locale.
2. Configurare gli aggiornamenti dei database e dei moduli dell'applicazione dalla cartella condivisa specificata negli altri computer della LAN aziendale.

Per abilitare la copia del pacchetto di aggiornamento nella cartella condivisa:

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiorna**.
2. Si apre l'elenco delle attività; selezionare l'attività di aggiornamento e fare clic su .
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\Share\Update distribution).
5. Salvare le modifiche.


Per configurare gli aggiornamenti da una cartella condivisa:

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiorna**.
2. Si apre l'elenco delle attività; selezionare l'attività di aggiornamento e fare clic su .
3. Fare clic sul pulsante **Seleziona sorgente 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 sul pulsante **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. Per i dettagli su come tenere traccia degli aggiornamenti dei moduli delle applicazioni e su come confermare un aggiornamento in Kaspersky Security Center, consultare la [Guida di Kaspersky Security Center](#).

Dopo l'installazione di un aggiornamento dell'applicazione, potrebbe essere necessario riavviare il computer.


Per configurare gli aggiornamenti dei moduli dell'applicazione:

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiorna**.
2. Si apre l'elenco delle attività; selezionare l'attività di aggiornamento e fare clic su .
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 **Utilizza 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, selezionare **Dispositivi** → **Criteri e profili**.
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 **Impostazioni del server proxy**, selezionare **Ignora il server proxy per gli indirizzi locali**.
6. 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**.
3. Nella sezione **Server proxy**, fare clic sul collegamento **Impostazioni del server proxy**.
4. Nella finestra visualizzata, selezionare una delle seguenti opzioni per determinare l'indirizzo del server proxy:
 - **Rileva automaticamente le impostazioni del server proxy.**
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. Se si desidera abilitare l'autenticazione nel server proxy, selezionare la casella di controllo **Usa l'autenticazione per il server proxy** e fornire le credenziali dell'account utente.
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 primo aggiornamento dei database e dei moduli dell'applicazione, diventa disponibile la funzione di rollback dei database e dei moduli dell'applicazione alla versione precedente.

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. Il rollback dell'ultimo aggiornamento è ad esempio utile 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 rollback dell'ultimo aggiornamento:

1. Nella finestra principale dell'applicazione, andare alla sezione **Aggiorna**.
2. Nel riquadro **Rollback alla versione precedente del database**, fare clic sul pulsante **Esegui rollback**.

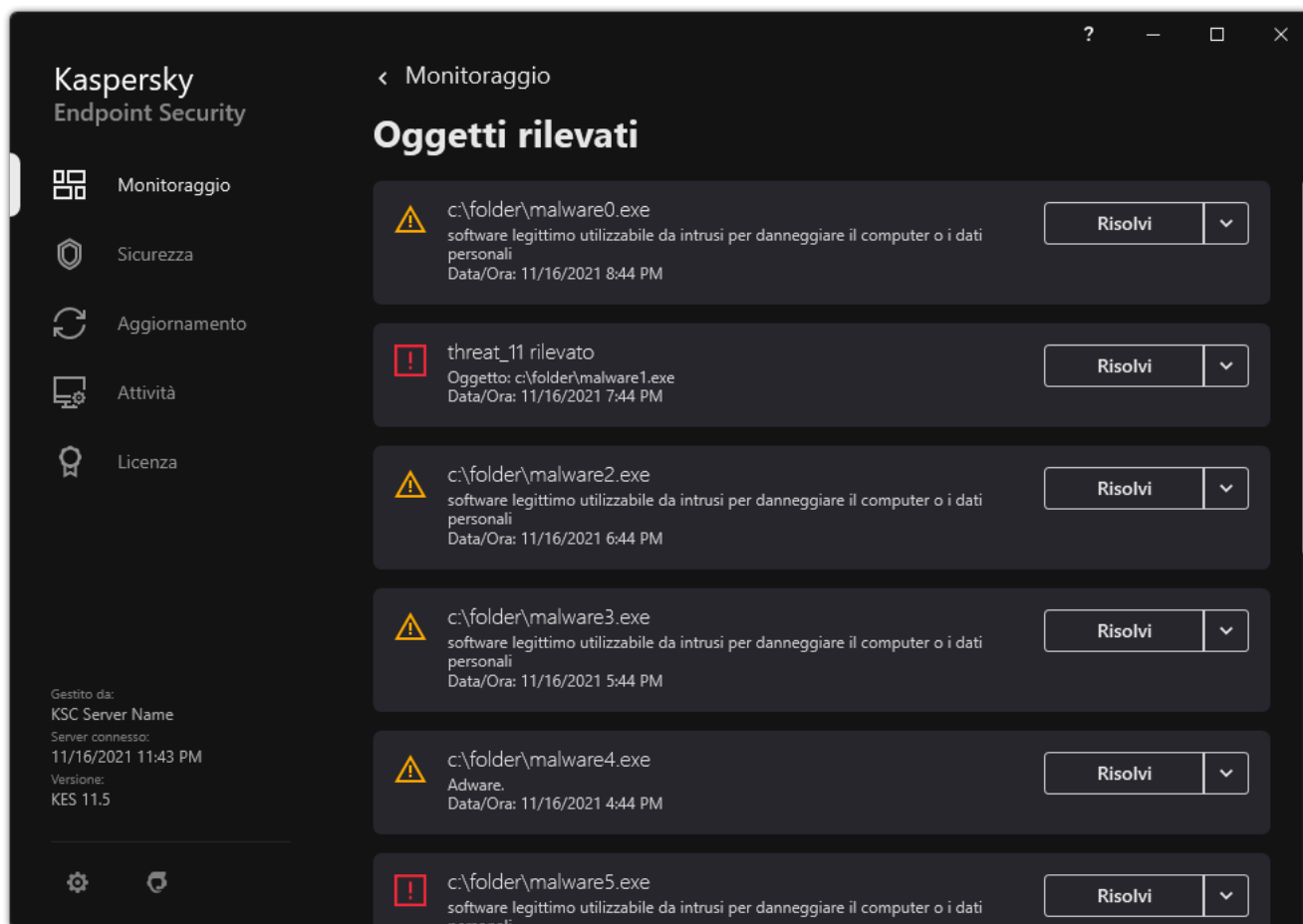
Kaspersky Endpoint Security inizierà a eseguire il rollback dell'ultimo aggiornamento del database. L'applicazione visualizzerà lo stato di avanzamento del rollback, la dimensione dei file scaricati e l'origine degli aggiornamenti. È possibile interrompere l'attività in qualsiasi momento facendo clic sul pulsante **Interrompere l'aggiornamento**.

Per avviare o arrestare un'attività di rollback 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 rollback non in esecuzione per avviarla.
 - Selezionare un'attività di rollback in esecuzione per interromperla.
 - Selezionare un'attività di rollback sospesa per riprenderla o riavviarla.

Utilizzo delle minacce attive

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). 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 virus](#) e nelle [impostazioni dell'applicazione](#).

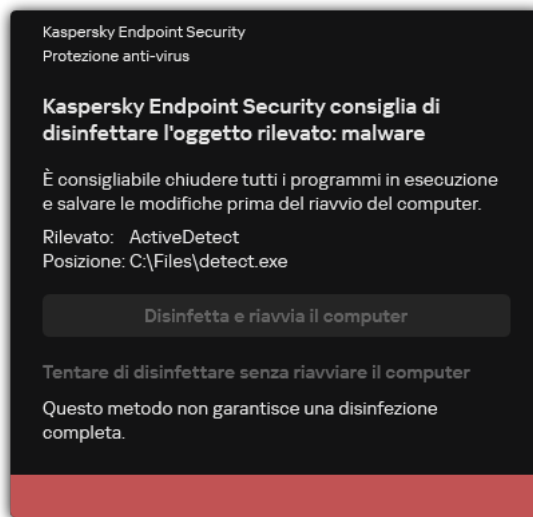


Un elenco di minacce attive

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 virus](#). 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 virus*.

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 virus*. Quindi, è necessario avviare l'attività *Scansione virus*.

Abilitazione o disabilitazione di Tecnologia Avanzata di Disinfezione

Se Kaspersky Endpoint Security non riesce ad arrestare l'esecuzione di un malware, è possibile utilizzare la tecnologia Disinfezione avanzata. Per impostazione predefinita, la tecnologia Disinfezione avanzata è disabilitata poiché utilizza una notevole quantità di risorse di elaborazione. Pertanto, è possibile abilitare Disinfezione avanzata solo quando [si devono contenere minacce attive](#).

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 virus*. Questo prerequisito non è necessario per utilizzare la tecnologia nelle workstation.


[Come abilitare o disabilitare la tecnologia Disinfezione avanzata 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Impostazioni generali** → **Impostazioni applicazione**.
6. Nel blocco **Modalità operativa**, selezionare o deselezionare la casella di controllo **Abilita la tecnologia Disinfezione avanzata** per abilitare o disabilitare la tecnologia Disinfezione avanzata.
7. Salvare le modifiche.

[Come abilitare o disabilitare la tecnologia Disinfezione avanzata in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 applicazione**.
5. Nel blocco **Modalità operativa**, selezionare o deselezionare la casella di controllo **Abilita la tecnologia Disinfezione avanzata** 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**.
3. Nel blocco **Modalità operativa**, 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 viene riavviato.



Elaborazione delle 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 virus](#), l'azione relativa al rilevamento delle minacce è impostata su **Notifica**. 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, accedere 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, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.
- **Elimina**.

[Come elaborare una minaccia in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **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, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.
- **Elimina.**

Come elaborare una minaccia nell'interfaccia dell'applicazione

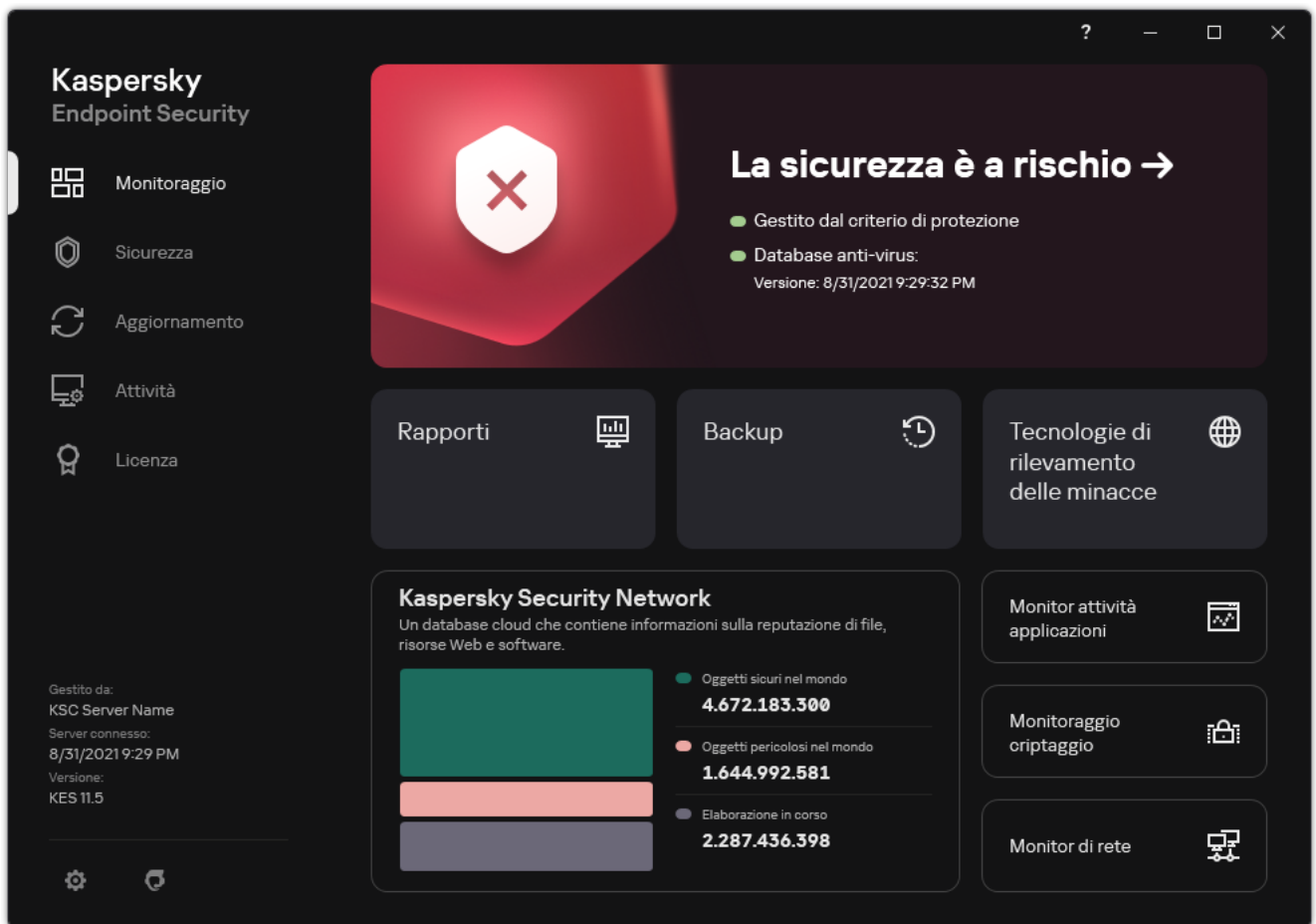
1. Nella finestra principale dell'applicazione, nella sezione **Monitoraggio**, fare clic sul riquadro **La protezione è a rischio**.

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, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.
- **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 dell'Enciclopedia dei Virus di Kaspersky](#). 



Finestra principale dell'applicazione quando viene rilevata una minaccia

Protezione del computer

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 nella RAM del computer. Il componente esegue la scansione dei file in tutte le unità del computer, nonché nelle unità connesse. 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 disinfecta 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 sono archiviati nel 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.

Per abilitare o disabilitare il 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. 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. I valori delle impostazioni per il livello di sicurezza consigliato sono specificati nella tabella seguente.

- **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 composti.
- Se si desidera configurare un livello di sicurezza personalizzato, fare clic sul pulsante **Impostazioni avanzate** e definire le proprie impostazioni del componente.
È possibile ripristinare i valori dei livelli di protezione preimpostati facendo clic sul pulsante **Ripristina il livello di sicurezza consigliato** nella parte superiore della finestra.

5. 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, Kaspersky Endpoint Security 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 composti.
Tecnologia iSwift	Attivato	Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalla scansione 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	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	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.


formati Microsoft Office		
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, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.

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, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.
 - **Disinfetta (se non è possibile, blocca)**. Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non è possibile, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive.
 - **Blocca**. Se questa opzione è selezionata, il componente Protezione minacce file blocca automaticamente tutti i file infetti senza tentare di disinfettarli.

Prima di tentare di disinfettare o eliminare un file infetto, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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. Selezionare un oggetto da aggiungere all'ambito della protezione.

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:
 - **Tecnologia iSwift**. Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalla scansione 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).
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 composti.

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. Nel blocco **Ottimizzazione della scansione**, selezionare la casella di controllo **Esamina solo i file nuovi e modificati**.
5. Salvare le modifiche.


Scansione dei file composti

Una tecnica comune per nascondere virus e altro malware è inserirli in file composti, come ad esempio archivi o database. Per rilevare i virus e il malware nascosti in questo modo, è necessario decomprimere il file composto, cosa che può rallentare la scansione. È possibile limitare i tipi di file composti da esaminare, velocizzando la scansione.

Il metodo elabora un file composto infetto (disinfezione o eliminazione) a seconda del tipo di file.

Il componente Protezione minacce file disinfetta i file composti 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 composti:

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 composti**, specificare i tipi di file composti di cui eseguire la scansione: archivi, pacchetto di distribuzione o file nei formati di 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 composti.

6. Configurare le impostazioni avanzate per la scansione dei file composti.

- **Non decomprimere i file composti di grandi dimensioni.**

Se la casella di controllo è selezionata, Kaspersky Endpoint Security non esegue la scansione dei file composti se la loro dimensione supera il valore specificato.

Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esamina i file composti 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 composti di grandi dimensioni** sia selezionata o meno.

- **Decomprimi file composti in background.**

Se la casella di controllo è selezionata, Kaspersky Endpoint Security consente di accedere ai file composti di dimensioni superiori al valore specificato prima della scansione dei file. In questo caso, Kaspersky Endpoint Security decompone ed esamina i file composti in background.

Kaspersky Endpoint Security consente di accedere ai file composti 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 composti 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.
- **Al momento dell'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.

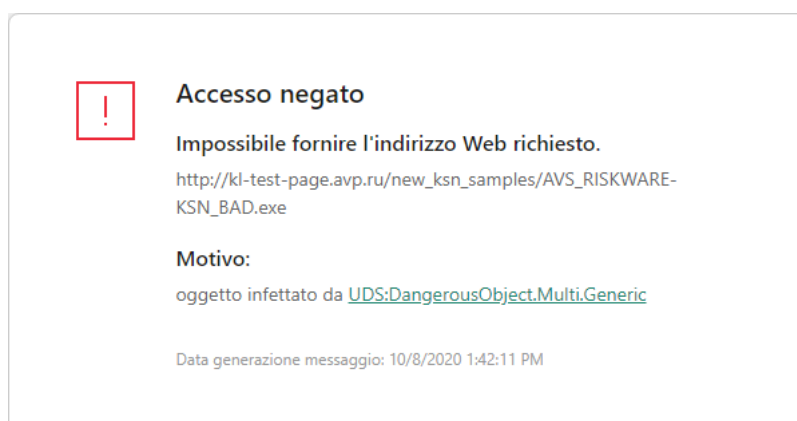
Protezione minacce Web

Il componente Protezione minacce Web impedisce il download di file dannosi da Internet e blocca inoltre i 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. È possibile [specificare le porte che verranno monitorate da Kaspersky Endpoint Security](#), oppure selezionare tutte le porte.

Per il monitoraggio del traffico HTTPS è necessario [abilitare la scansione delle connessioni criptate](#).

Quando un utente tenta di aprire un sito Web dannoso o di phishing, Kaspersky Endpoint Security bloccherà l'accesso e mostrerà un avviso (vedere la figura seguente).



Messaggio di accesso negato al sito Web

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, 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 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.
6. Utilizzare la casella di controllo **Protezione minacce Web** per abilitare o disabilitare il componente.
7. 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 protocolli 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 di Kaspersky Endpoint Security 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 Media.


Se si desidera configurare un livello di sicurezza personalizzato, fare clic sul pulsante **Impostazioni** e definire le proprie impostazioni del componente.

È possibile ripristinare i valori dei livelli di sicurezza preimpostati facendo clic sul pulsante **Predefinito** in **Livello di sicurezza**.
8. 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 il download**. 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.
 - **Avvisa**. 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.
9. Salvare le modifiche.

[Come abilitare o disabilitare il componente Protezione minacce Web in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 essenziale** → **Protezione minacce Web**.
5. Utilizzare l'interruttore **Protezione minacce Web** 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 il download**. 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.
 - **Avvisa**. 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](#)

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 protocolli 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 di Kaspersky Endpoint Security 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 Media.
 - Se si desidera configurare un livello di sicurezza personalizzato, fare clic sul pulsante **Impostazioni avanzate** e definire le proprie impostazioni del componente.
È possibile ripristinare i valori dei livelli di protezione preimpostati facendo clic sul pulsante **Ripristina il livello di sicurezza consigliato** nella parte superiore della finestra.
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 il download**. 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.
 - **Avvisa**. 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	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 e incluso nel pacchetto di installazione dell'applicazione e viene aggiornato durante gli aggiornamenti del database di Kaspersky Endpoint Security.

Web dannosi		
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.
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 il download	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 e incluso nel pacchetto di installazione dell'applicazione e viene aggiornato durante gli aggiornamenti del database di Kaspersky Endpoint Security.

Kaspersky Endpoint 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.
6. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
7. Viene visualizzata una finestra; in tale finestra, in **Metodi di scansione**, selezionare o deselegionare la casella di controllo **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.
8. 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. In **Metodi di scansione**, selezionare o deselegionare la casella di controllo **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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.
6. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
7. 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.
8. 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.
9. 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.
6. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
7. Viene visualizzata una finestra; in tale finestra, in **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 o 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.
8. 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](#).
9. 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 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.
6. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
7. Nella finestra visualizzata, selezionare la scheda **Indirizzi Web attendibili**.
8. Selezionare la casella di controllo **Non esaminare il traffico Web per gli URL attendibili**.
Se la casella 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.
9. 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](#).
10. Salvare le modifiche.

[Come aggiungere un indirizzo Web attendibile in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 essenziale** → **Protezione minacce Web**.
5. In **Indirizzi Web attendibili**, selezionare la casella di controllo **Non esaminare il traffico Web per gli indirizzi Web attendibili**.
Se la casella 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.
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 XML](#).
7. 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 per gli URL attendibili**.
Se la casella 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Protezione minacce Web**.
6. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
7. Nella finestra visualizzata, selezionare la scheda **Indirizzi Web attendibili**.
8. 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.
9. 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.
10. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 essenziale** → **Protezione minacce Web**.
5. Per esportare l'elenco delle esclusioni nella sezione **Indirizzi Web attendibili**:
 - a. Selezionare gli indirizzi Web attendibili 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 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.
6. Per importare l'elenco di esclusioni nella sezione **Indirizzi Web 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.
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
- Microsoft Outlook Express
- Windows Mail

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 operazioni con Outlook 2010, 2013, 2016 e 2019.


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 rinomina l'oggetto del messaggio come segue: [Il messaggio richiede la partecipazione dell'utente all'elaborazione] <oggetto del messaggio> o [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, Kaspersky Endpoint Security applica 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.

Per abilitare o disabilitare il 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. 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 di Kaspersky Endpoint Security 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.
È possibile ripristinare i valori dei livelli di protezione preimpostati facendo clic sul pulsante **Ripristina il livello di sicurezza consigliato** nella parte superiore della finestra.

5. 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	<p>L'<i>ambito della protezione</i> include gli oggetti che il componente controlla durante l'esecuzione: Messaggi in entrata e in uscita o Solo messaggi in entrata.</p> <p>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.</p>
Connetti estensione Microsoft Outlook	Attivato	<p>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.</p> <p>Se viene eseguita la scansione dei messaggi tramite l'estensione per Microsoft Outlook, è consigliabile utilizzare la modalità cache. Per informazioni più dettagliate sulla Modalità cache e per raccomandazioni sul relativo utilizzo, fare riferimento alla Microsoft Knowledge Base.</p>
Esamina gli archivi allegati	Attivato	Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. Kaspersky Endpoint Security esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato.
Esamina i file in formato Microsoft Office allegati	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.
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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security elimina l'oggetto infetto. Kaspersky Endpoint Security aggiunge informazioni sull'azione eseguita nell'oggetto del messaggio: [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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security elimina l'oggetto infetto. Kaspersky Endpoint Security aggiunge informazioni sull'azione eseguita nell'oggetto del messaggio: [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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security aggiunge un avviso all'oggetto del messaggio: [Il messaggio richiede la partecipazione dell'utente all'elaborazione] <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, Kaspersky Endpoint Security tenta di disinfettare l'oggetto rilevato. Se l'oggetto non può essere disinfettato, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security aggiunge un avviso all'oggetto del messaggio: [Il messaggio richiede la partecipazione dell'utente all'elaborazione] <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, Kaspersky Endpoint Security 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, deselegionare 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 composti allegati ai messaggi e-mail

È possibile abilitare o disabilitare la scansione degli allegati dei messaggi, limitare la dimensione massima degli allegati dei messaggi da esaminare e limitare la durata massima della scansione degli allegati dei messaggi.

Per configurare la scansione dei file composti 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 composti**, configurare le impostazioni di scansione:
 - **Esamina i file in formato Microsoft Office allegati.** Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE.
 - **Esamina gli archivi allegati.** Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. Kaspersky Endpoint Security esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato.

Se durante la scansione Kaspersky Endpoint Security 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.** 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.


5. Salvare le modifiche.

Filtraggio degli allegati dei messaggi e-mail

La funzionalità di filtro degli allegati non viene applicata 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.

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Protezione minacce di posta**.
6. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
7. Nella finestra visualizzata, selezionare la scheda **Filtro allegati**.
8. 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.
9. 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.
10. Salvare le modifiche.

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 essenziale** → **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.

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). Tale estensione consente di aprire le impostazioni del componente Protezione minacce di posta direttamente da Outlook e di specificare quando eseguire la scansione dei messaggi e-mail alla ricerca di virus e altre minacce. L'estensione di Protezione minacce di posta per Outlook può eseguire la scansione dei messaggi in entrata e in uscita trasmessi tramite i protocolli POP3, SMTP, NNTP, IMAP e MAPI. Kaspersky Endpoint Security supporta anche il funzionamento con altri client e-mail (inclusi Microsoft Outlook Express®, Windows Mail e Mozilla™ Thunderbird™).

L'estensione Protezione minacce di posta supporta le operazioni con Outlook 2010, 2013, 2016 e 2019.

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.

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.

I messaggi in uscita vengono prima esaminati dall'estensione di Protezione minacce di posta per Outlook e quindi dal componente Protezione minacce di posta.

Se viene eseguita la scansione dei messaggi tramite l'estensione Protezione minacce di posta per Outlook, è consigliabile utilizzare la modalità cache. Per informazioni più dettagliate sulla Modalità cache e per raccomandazioni sul relativo utilizzo, fare riferimento alla [Microsoft Knowledge Base](#).

Per configurare la modalità operativa dell'estensione di Protezione minacce di posta per Outlook tramite Kaspersky Security Center:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Protezione minacce di posta**.
6. Nel blocco **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
7. Nel blocco **Connettività**, fare clic sul pulsante **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. Salvare le modifiche.


Protezione minacce di rete

Il componente Protezione minacce di Rete esamina il traffico di rete in entrata alla ricerca di attività tipiche degli attacchi di rete. Quando Kaspersky Endpoint Security 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 di Kaspersky Endpoint Security 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. Se necessario, è possibile disabilitare Protezione minacce di Rete.


Per abilitare o disabilitare Protezione minacce di Rete:

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**.
3. Utilizzare l'interruttore **Protezione minacce di rete** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Di conseguenza, se Protezione minacce di rete è abilitato, Kaspersky Endpoint Security esamina il traffico di rete in entrata per rilevare eventuali attività tipiche degli attacchi di rete. Quando Kaspersky Endpoint Security rileva un tentativo di attacco di rete nel computer dell'utente, blocca la connessione di rete con il computer che ha originato l'attacco.

Blocco di un computer che ha originato l'attacco

Per bloccare un computer che ha originato l'attacco:

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**.
3. Selezionare la casella di controllo **Aggiungi il computer che ha originato l'attacco all'elenco dei computer bloccati per N minuti**.

Se la casella di controllo è selezionata, 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 32.768 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.


1. Impostare una durata di blocco diversa per un computer che ha originato l'attacco nel campo a destra della casella di controllo **Aggiungi il computer che ha originato l'attacco all'elenco dei computer bloccati per N min.**
2. 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.

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.

Per configurare gli indirizzi delle esclusioni dal blocco:

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**.
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.
6. Salvare le modifiche.

Di conseguenza, Kaspersky Endpoint Security non traccia le attività dei dispositivi nell'elenco delle esclusioni.

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Protezione minacce di rete**.
6. Nella sezione **Impostazioni Protezione minacce di rete** fare clic sul pulsante **Esclusioni**.
7. 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 collegamento **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.
8. 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.
9. Salvare le modifiche.

[Come esportare e importare un elenco di esclusioni in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 essenziale** → **Protezione minacce di rete**.
5. Nella sezione **Impostazioni Protezione minacce di rete** 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 su **Esporta**.
 - c. Confermare di voler esportare solo le esclusioni selezionate o esportare l'intero elenco di esclusioni.
 - d. 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.
 - e. Salvare il file.
Kaspersky Endpoint Security esporta l'intero elenco di esclusioni nel file XML.
7. 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.
8. Salvare le modifiche.

Configurazione della protezione dagli attacchi di rete per 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.

Per configurare la protezione dagli attacchi di rete per tipo:

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**.
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.
4. Utilizzare l'interruttore **Protezione dallo spoofing MAC**.
5. Nella sezione **Al rilevamento di un attacco di spoofing MAC** selezionare una delle seguenti opzioni:
 - **Invia solo notifica.**
 - **Invia notifica e blocca.**
6. Salvare le modifiche.

Firewall

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. Inserisce l'applicazione in uno dei *gruppi di attendibilità*: Attendibile, Restrizione bassa, Restrizione alta, Non attendibile.

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 come segue: una regola di rete per le applicazioni include regole di accesso basate sullo stato della rete: *pubblica*, *locale* o *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.

Stati delle connessioni di rete

Firewall consente di controllare l'attività di rete in base allo stato della connessione di rete. Kaspersky Endpoint Security riceve lo stato della connessione di rete dal sistema operativo del computer. Lo stato della connessione di rete nel sistema operativo viene impostato dall'utente durante la configurazione della connessione. È possibile [modificare lo stato della connessione di rete nelle impostazioni di Kaspersky Endpoint Security](#). Firewall monitorerà l'attività di rete in base allo stato della rete nelle impostazioni di Kaspersky Endpoint Security e non nel sistema operativo.

La connessione di rete può avere uno dei seguenti tipi di categoria:

- **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 la categoria *Rete pubblica*. Non è possibile modificare la categoria 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.

Abilitazione o disabilitazione di Firewall

Per impostazione predefinita, Firewall è abilitato e funziona in modalità ottimale.

Per abilitare o disabilitare Firewall:

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 esamina il traffico di rete in entrata alla ricerca di attività tipiche 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 della categoria della connessione di rete

Per impostazione predefinita, Firewall assegna a Internet la categoria *Rete pubblica*. Non è possibile modificare la categoria di Internet.

Per modificare la categoria 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 lo stato.
5. Nella colonna **Tipo di rete** selezionare lo stato della 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

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.

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.


[Come utilizzare lo strumento Monitor di rete per creare una regola per i pacchetti di rete nell'interfaccia dell'applicazione](#) 

1. Nella finestra dell'applicazione principale, nella sezione **Monitoraggio**, fare clic sul riquadro **Monitor di rete**.
2. Selezionare la 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. Fare clic su **Aggiungi**.
Verranno visualizzate le proprietà delle regole di rete.
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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Firewall**.
6. Nella sezione **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.
7. Selezionare la scheda **Regole per i pacchetti di rete**.
Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.
8. Fare clic su **Aggiungi**.
Verranno visualizzate le proprietà delle regole per i pacchetti.
9. Immettere manualmente il nome del servizio di rete nel campo **Nome**.
10. 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.
11. Se si desidera che le azioni della regola di rete vengano registrate nel [rapporto](#), selezionare la casella di controllo **Registra eventi**.
12. Salvare la nuova regola di rete.
13. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.
14. 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, deselegionare la casella di controllo accanto all'oggetto.

[Come creare una regola per i pacchetti di rete in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
 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 **Protezione minacce essenziale** → **Firewall**.
 5. Nella sezione **Impostazioni di Firewall** fare clic sul collegamento **Regole per i pacchetti di rete**.
Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.
 6. Fare clic sul pulsante **Aggiungi**.
Verranno visualizzate le proprietà delle regole per i pacchetti.
 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 collegamento **Seleziona modello**. 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 **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. Utilizzare l'interruttore nella colonna **Stato** per abilitare o disabilitare la regola per i pacchetti.


Impostazioni delle regole per i pacchetti di rete

Parametro	Descrizione
Azione	<p>Consenti.</p> <p>Blocca.</p> <p>In base alle regole dell'applicazione. Se questa opzione è selezionata, Firewall applica le regole di rete dell'applicazione alla connessione di rete.</p>
Protocollo	<p>Controlla le attività di rete tramite il protocollo selezionato: TCP, UDP, ICMP, ICMPv6, IGMP e GRE.</p> <p>Se come protocollo è selezionato ICMP o ICMPv6, è possibile definire il codice e il tipo di pacchetto ICMP.</p> <p>Se come tipo di protocollo è selezionato TCP o UDP, è possibile specificare i numeri di porta (separati da virgole) del computer locale e remoto tra cui monitorare la connessione.</p>
Direzione	<p>In entrata (pacchetto). Firewall applica la regola di rete a tutti i pacchetti di rete in entrata.</p>

	<p>In entrata. Firewall applica la regola di rete a tutti i pacchetti di rete inviati tramite una connessione avviata da un computer remoto.</p> <p>In entrata/In uscita. Firewall applica la regola di rete ai pacchetti di rete in entrata e in uscita, indipendentemente dal fatto che sia stato il computer dell'utente o un computer remoto ad avviare la connessione di rete.</p> <p>In uscita (pacchetto). Firewall applica la regola di rete a tutti i pacchetti di rete in uscita.</p> <p>In uscita. Firewall applica la regola di rete a tutti i pacchetti di rete inviati tramite una connessione avviata dal computer dell'utente.</p>
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)	Limitare il controllo dei pacchetti di rete in base al Time to live (TTL).
Indirizzo remoto	<p>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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security supporta i nomi DNS a partire dalla versione 11.7.0. Se si specifica un nome DNS per la versione 11.6.0 o precedente, Kaspersky Endpoint Security può applicare la regola pertinente a tutti gli indirizzi.</p> </div>
Indirizzo locale	<p>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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security supporta i nomi DNS a partire dalla versione 11.7.0. Se si specifica un nome DNS per la versione 11.6.0 o precedente, Kaspersky Endpoint Security può applicare la regola pertinente a tutti gli indirizzi.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>A volte l'indirizzo locale non può essere ottenuto per le applicazioni. In tal caso, questo parametro viene ignorato.</p> </div>

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Firewall**.
6. Nella sezione **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.
7. Selezionare la scheda **Regole per i pacchetti di rete**.
8. 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.
9. 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.
10. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 **Protezione minacce essenziale** → **Firewall**.
5. Fare clic sul collegamento **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.
 - 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 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.

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 dell'applicazione principale, nella sezione **Monitoraggio**, fare clic sul riquadro **Monitor di rete**.
2. Selezionare la 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Protezione minacce essenziale** → **Firewall**.
6. Nella sezione **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.
7. Selezionare la scheda **Regole di rete dell'applicazione**.
8. Fare clic su **Aggiungi**.
9. 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.
10. Fare clic sul pulsante **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.
11. Selezionare l'applicazione desiderata.
12. 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.
13. 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.
14. Selezionare la scheda **Regole di rete**.
Verrà visualizzato l'elenco delle regole di rete predefinite impostate da Firewall.
15. Fare clic sul pulsante **Aggiungi**.
Verranno visualizzate le proprietà delle regole di rete.
16. Immettere manualmente il nome del servizio di rete nel campo **Nome**.
17. 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.

18. Se si desidera che le azioni della regola di rete vengano registrate nel [rapporto](#), selezionare la casella di controllo **Registra eventi**.
19. Salvare la nuova regola di rete.
20. Utilizzare i pulsanti **Su** / **Giù** per impostare la priorità della regola di rete.
21. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 **Protezione minacce essenziale** → **Firewall**.
5. Nella sezione **Impostazioni di Firewall** fare clic sul collegamento **Regole di rete dell'applicazione**.
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 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 di **Applicazione**. Fare clic sul pulsante **Avanti**.
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 facendo clic su **OK**.
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 sul pulsante **Aggiungi**.
Verranno visualizzate le proprietà delle regole delle applicazioni.
15. Immettere manualmente il nome del servizio di rete nel campo **Nome**.
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**. 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 **Su** / **Giù** per impostare la priorità della regola di rete.


20. Salvare le modifiche.

Impostazioni delle regole di rete delle applicazioni

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 (separati da virgole) del computer locale e remoto tra cui monitorare la connessione.
Direzione	In entrata. In entrata/In uscita. In uscita.
Indirizzo remoto	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. Kaspersky Endpoint Security supporta i nomi DNS a partire dalla versione 11.7.0. Se si specifica un nome DNS per la versione 11.6.0 o precedente, Kaspersky Endpoint Security può applicare la regola pertinente a tutti gli indirizzi.
Indirizzo locale	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. <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">Kaspersky Endpoint Security supporta i nomi DNS a partire dalla versione 11.7.0. Se si specifica un nome DNS per la versione 11.6.0 o precedente, Kaspersky Endpoint Security può applicare la regola pertinente a tutti gli indirizzi.</div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">A volte l'indirizzo locale non può essere ottenuto per le applicazioni. In tal caso, questo parametro viene ignorato.</div>

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 dell'applicazione principale, 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 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 della 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.

Il componente Prevenzione Attacchi BadUSB non è installato per impostazione predefinita. Se è necessario il componente Prevenzione Attacchi BadUSB, è possibile aggiungere il componente nelle proprietà del [pacchetto di installazione](#) prima di installare l'applicazione o [modificare i componenti dell'applicazione disponibili](#) dopo l'installazione dell'applicazione.




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.

Per abilitare o disabilitare Prevenzione Attacchi BadUSB:


1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Prevenzione Attacchi BadUSB**.
3. Utilizzare l'interruttore **Prevenzione Attacchi BadUSB** per abilitare o disabilitare il componente.
4. Nel blocco **Autorizzazione tastiera USB alla connessione**, modificare le impostazioni di sicurezza per l'immissione del codice di autorizzazione:
 - **Numero massimo di tentativi di autorizzazione del dispositivo.** 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 5 tentativi di immissione del codice di autorizzazione, il dispositivo USB viene bloccato dopo il quinto tentativo non riuscito. Kaspersky Endpoint Security mostra la durata del blocco per il dispositivo USB. Trascorso questo tempo, è possibile compiere 5 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, i lettori di codici a barre). Non è consigliabile utilizzare la Tastiera sullo schermo per l'autorizzazione di dispositivi USB sconosciuti.

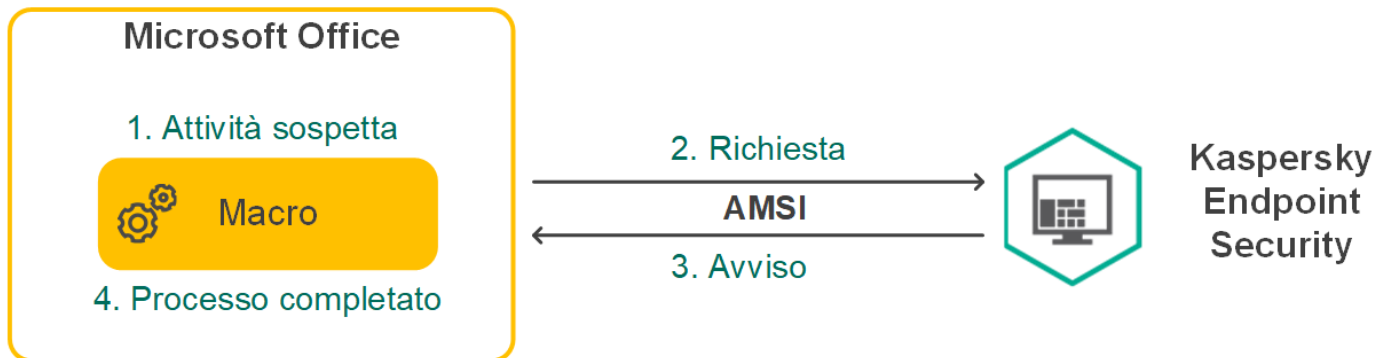
Per autorizzare o impedire l'utilizzo di Tastiera sullo schermo per l'autorizzazione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce essenziale** → **Prevenzione Attacchi BadUSB**.
3. 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.
4. Salvare le modifiche.

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 terze parti 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 terze parti 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 terze parti della minaccia rilevata. Dopo la ricezione di una notifica di minaccia, l'applicazione di terze parti non consente di eseguire 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 terze parti, 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 terze parti ad Administration Server. Il componente Protezione AMSI non nega le richieste provenienti dalle applicazioni di terze parti 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;
- Windows 11;
- Windows Server 2016 Essentials/Standard/Datacenter;
- Windows Server 2019 Essentials/Standard/Datacenter;
- Windows Server 2022.

Abilitazione e disabilitazione di Protezione AMSI

Per impostazione predefinita, Protezione AMSI è abilitato.

Per abilitare o disabilitare Protezione AMSI:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione selezionare **Protezione minacce essenziale** → **Protezione AMSI**.


3. Utilizzare l'interruttore **Protezione AMSI** per abilitare o disabilitare il componente.

4. Salvare le modifiche.

Utilizzo di Protezione AMSI per eseguire la scansione dei file composti

Una tecnica comune per nascondere virus e altro malware è inserirli in file composti, come gli archivi. Per rilevare i virus e il malware nascosti in questo modo, è necessario decomprimere il file composto, cosa che può rallentare la scansione. È possibile limitare i tipi di file composti da esaminare, velocizzando la scansione.

Per configurare le scansioni di Protezione AMSI dei file composti:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione selezionare **Protezione minacce essenziale** → **Protezione AMSI**.
3. Nel blocco **Scansione dei file composti**, specificare i tipi di file composti 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 composti di grandi dimensioni, selezionare la casella di controllo **Non decomprimere i file composti di grandi dimensioni**, quindi specificare il valore desiderato nel campo **Dimensione massima file**. Il componente Protezione AMSI non decomprimerà i file composti di dimensioni superiori al valore specificato.
 - Per consentire al componente Protezione AMSI di decomprimere i file composti di grandi dimensioni, deselegionare la casella di controllo **Non decomprimere i file composti 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 composti di grandi dimensioni** sia selezionata o meno.

5. Salvare le modifiche.


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.

Abilitazione e disabilitazione di Prevenzione Exploit

Prevenzione Exploit è abilitato per impostazione predefinita e viene eseguito nella modalità consigliata dagli esperti Kaspersky. Se necessario, è possibile disabilitare Prevenzione Exploit.

Per abilitare o disabilitare Prevenzione Exploit:


1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Prevenzione Exploit**.
3. Utilizzare l'interruttore **Prevenzione Exploit** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Di conseguenza, se Prevenzione Exploit è abilitato, Kaspersky Endpoint Security monitorerà i file eseguibili eseguiti da 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.

Selezione di un'azione da eseguire quando viene rilevato un exploit

Per impostazione predefinita, al rilevamento di un exploit Kaspersky Endpoint Security blocca i tentativi di operazioni dell'exploit.


Per scegliere un'azione da eseguire quando viene rilevato un exploit:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Prevenzione Exploit**.
3. Selezionare l'azione richiesta nella sezione **Al rilevamento di exploit**:
 - **Blocca operazione**. 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.
 - **Notifica**. 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](#).
4. Salvare le modifiche.

Protezione della memoria dei processi di sistema

Per impostazione predefinita, la protezione della memoria dei processi di sistema è abilitata.

Per abilitare e disabilitare la protezione della memoria dei processi di sistema:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Prevenzione Exploit**.

3. Utilizzare l'interruttore **Abilita protezione della memoria dei processi di sistema** per abilitare o disabilitare questa funzionalità.

4. Salvare le modifiche.

Di conseguenza, Kaspersky Endpoint Security bloccherà i processi esterni che tentano di accedere ai 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 (Behavior Stream Signature) 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 assicura una difesa proattiva del computer.

Abilitazione e disabilitazione di Rilevamento del Comportamento

Rilevamento del Comportamento è abilitato per impostazione predefinita e viene eseguito nella modalità consigliata dagli esperti Kaspersky. Se necessario, è possibile disabilitare Rilevamento del Comportamento.

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.


Per abilitare o disabilitare Rilevamento del Comportamento:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Rilevamento del Comportamento**.
3. Utilizzare l'interruttore **Rilevamento del comportamento** per abilitare o disabilitare il componente.
4. 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.

Selezione dell'azione da intraprendere se viene rilevata un'attività malware

Per selezionare l'azione da eseguire in caso di rilevamento di attività dannose in un'applicazione, eseguire le seguenti operazioni:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Rilevamento del Comportamento**.

3. Selezionare l'azione attinente nella sezione **Se viene rilevata un'attività malware**:

- **Elimina file.** 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.
- **Termina l'applicazione.** Se si seleziona questo elemento, Kaspersky Endpoint Security termina l'applicazione al momento del rilevamento dell'attività dannosa.
- **Notifica.** 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.

4. Salvare le modifiche.

Protezione delle cartelle condivise dal criptaggio esterno

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.

La protezione delle cartelle condivise dal criptaggio esterno fornisce l'analisi delle attività nelle cartelle condivise. Se questa attività corrisponde a una firma BSS tipica del criptaggio esterno, Kaspersky Endpoint Security esegue l'azione selezionata.


Per impostazione predefinita, la protezione delle cartelle condivise dal criptaggio esterno è disabilitata.

In seguito all'installazione di Kaspersky Endpoint Security, la protezione delle cartelle condivise dal criptaggio esterno sarà limitata fino al riavvio del computer.

Abilitazione e disabilitazione della protezione delle cartelle condivise dal criptaggio esterno


In seguito all'installazione di Kaspersky Endpoint Security, la protezione delle cartelle condivise dal criptaggio esterno sarà limitata fino al riavvio del computer.

Per abilitare o disabilitare la protezione delle cartelle condivise dal criptaggio esterno:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Rilevamento del Comportamento**.
3. Utilizzare il pulsante **Abilita la protezione delle cartelle condivise dal criptaggio esterno** per abilitare o disabilitare il rilevamento delle attività tipiche del criptaggio esterno.
4. Salvare le modifiche.

Selezione dell'azione da eseguire se viene rilevato criptaggio esterno delle cartelle condivise

Per selezionare l'azione da eseguire al rilevamento di criptaggio esterno delle cartelle condivise:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Rilevamento del Comportamento**.
3. Selezionare l'azione attinente nella sezione **Protezione delle cartelle condivise dal criptaggio esterno**:
 - **Blocca connessione per N min. (da 1 a 43800)**. Se questa opzione è selezionata e 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 sull'interfaccia dell'applicazione locale](#).
 - Invia 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.

 - **Notifica**. Se questa opzione è selezionata e Kaspersky Endpoint Security rileva un tentativo di modifica dei file nelle cartelle condivise, vengono eseguite le seguenti azioni:
 - Aggiunge una voce ai [rapporti sull'interfaccia dell'applicazione locale](#).
 - Aggiunge una voce all'elenco delle minacce attive.
 - Invia informazioni sull'attività dannosa rilevata a Kaspersky Security Center.
4. Salvare le modifiche.

Creazione di un'esclusione per la protezione delle cartelle condivise dal criptaggio esterno

L'esclusione di una cartella 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.

[Come creare un'esclusione per la protezione delle cartelle condivise 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 **Criteri**.
4. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni**.
6. Nel blocco **Esclusioni dalla scansione e applicazioni attendibili**, fare clic sul pulsante **Impostazioni**.
7. Nella finestra visualizzata, selezionare la scheda **Esclusioni dalla scansione**.
Verrà visualizzata una finestra contenente un elenco di esclusioni.
8. 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.
9. Selezionare la casella di controllo **Consenti l'utilizzo delle applicazioni attendibili 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.
10. Fare clic su **Aggiungi**.
11. Nel blocco **Proprietà**, selezionare la casella di controllo **File o cartella**.
12. Fare clic sul collegamento **seleziona file o cartella** nel blocco **Descrizione dell'esclusione dalla scansione (fare clic sugli elementi sottolineati per modificarli)** per aprire la finestra **Nome del file o della cartella**.
13. Fare clic su **Sfoggia** e selezionare la cartella condivisa.

È inoltre possibile inserire manualmente il percorso. 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 cartella, ad eccezione della cartella 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 **Cartella** con l'estensione TXT e un nome composto da tre caratteri.

14. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.
15. Fare clic sul collegamento **qualsiasi** nel blocco **Descrizione dell'esclusione dalla scansione (fare clic sugli elementi sottolineati per modificarli)** per attivare il collegamento **selezionare i componenti**.
16. Fare clic sul collegamento **selezionare i componenti** per visualizzare la finestra **Componenti della protezione**.
17. Selezionare la casella di controllo accanto al componente **Rilevamento del Comportamento**.
18. Salvare le modifiche.

[Come creare un'esclusione per la protezione delle cartelle condivise tramite Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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. Accedere a **Impostazioni generali** → **Esclusioni**.
5. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Esclusioni dalla scansione**.
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 applicazioni attendibili 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.
8. Fare clic sul pulsante **Aggiungi**.
9. Selezionare le modalità di aggiunta dell'esclusione **File or folder**.
10. Fare clic su **Sfoglia** e selezionare la cartella condivisa.


È inoltre possibile inserire manualmente il percorso. 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 cartella, ad eccezione della cartella 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 Cartella con l'estensione TXT e un nome composto da tre caratteri.
11. Nel blocco **Componenti della protezione**, selezionare il componente **Rilevamento del Comportamento**.
12. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.

13. Selezionare lo stato **Attivo** per l'esclusione.

È possibile utilizzare l'interruttore per [interrompere un'esclusione](#) in qualsiasi momento.

14. Salvare le modifiche.

[Come creare un'esclusione per la protezione delle cartelle condivise nell'interfaccia dell'applicazione](#)

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

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

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 inserire manualmente il percorso. 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 cartella, ad eccezione della cartella 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 Cartella con l'estensione TXT e un nome composto da tre caratteri.

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.

Configurazione degli indirizzi delle esclusioni dalla protezione delle cartelle condivise dal criptaggio esterno

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.

Per escludere i computer remoti che eseguono il criptaggio esterno delle cartelle condivise:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Protezione minacce avanzata** → **Rilevamento del Comportamento**.
3. Nella sezione **Esclusioni** fare clic sul collegamento **Configurare gli indirizzi delle esclusioni**.
4. Se si desidera aggiungere un indirizzo IP o un nome computer all'elenco delle esclusioni, fare clic sul pulsante **Aggiungi**.
5. Immettere l'indirizzo IP o il nome del computer da cui non devono essere gestiti gli attacchi di criptaggio esterno.
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 \(MMC\) !\[\]\(c694a3ff3b077d76910920a6a1593ab4_img.jpg\)](#)

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Rilevamento del Comportamento**.
6. Nella sezione **Impostazioni Protezione minacce di rete** fare clic sul pulsante **Esclusioni**.
7. 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 collegamento **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.
8. 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.
9. Salvare le modifiche.

[Come esportare e importare un elenco di esclusioni in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **Rilevamento del Comportamento**.
5. Per esportare l'elenco delle esclusioni nella sezione **Esclusioni**:
 - a. Selezionare le esclusioni che si desidera esportare.
 - b. Fare clic su **Esporta**.
 - c. Confermare di voler esportare solo le esclusioni selezionate o esportare l'intero elenco di esclusioni.
 - d. 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.
 - e. Salvare il file.
Kaspersky Endpoint Security esporta l'intero elenco di esclusioni nel file XML.
6. Per importare l'elenco delle esclusioni nella sezione **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.
7. 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 da [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. Inserisce l'applicazione in uno dei *gruppi di attendibilità*: Attendibile, Restrizione bassa, Restrizione alta, Non attendibile.

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
6. Utilizzare la casella di controllo **Prevenzione Intrusioni Host** per abilitare o disabilitare il componente.
7. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **Prevenzione Intrusioni Host**.
5. Utilizzare l'interruttore **Prevenzione Intrusioni Host** 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 a cui Kaspersky Endpoint Security deve [assegnare automaticamente tutte le applicazioni sconosciute](#). Le applicazioni che sono state avviate prima di Kaspersky Endpoint Security vengono spostate automaticamente nel gruppo di attendibilità [specificato nelle impostazioni del componente 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
6. 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.
7. Selezionare la scheda **Diritti applicazione**.
8. Fare clic su **Aggiungi**.
9. Nella finestra visualizzata, immettere i criteri per cercare l'applicazione di cui si 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.
10. Fare clic sul pulsante **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.
11. Selezionare l'applicazione desiderata.
12. Nell'elenco a discesa **Aggiungi l'applicazione selezionata al gruppo di attendibilità**, selezionare il gruppo di attendibilità necessario per l'applicazione.
13. Salvare le modifiche.

[Come modificare il gruppo di attendibilità di un'applicazione in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **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 di **Applicazione**. Fare clic sul pulsante **Avanti**.
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 facendo clic su **OK**.
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 sul pulsante **Gestisci applicazioni**.
Verrà visualizzato l'elenco delle applicazioni installate.
4. Selezionare l'applicazione desiderata.
5. Nel menu di scelta rapida dell'applicazione, fare 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
6. 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.
7. Selezionare la scheda **Diritti applicazione**.
8. Selezionare il gruppo di attendibilità necessario.
9. Nel menu di scelta rapida del gruppo di attendibilità, selezionare **Diritti del gruppo**.
Verranno visualizzate le proprietà del gruppo di attendibilità.
10. 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 la scheda **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 la scheda **Diritti**.

L'attività di rete delle applicazioni è controllata da [Firewall](#) mediante le *regole di rete*.

11. 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** (⊗).
12. 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.
13. Salvare le modifiche.


[Come modificare i diritti del gruppo di attendibilità in Web Console e Cloud Console](#) ?

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **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. 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 da [Firewall](#) mediante le *regole di rete*.


9. Per la risorsa opportuna, nella colonna dell'azione corrispondente selezionare l'opzione necessaria: **Eredita, Consenti** (✓) o **Vieta** (✗).
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 sul pulsante **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 la scheda **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 la scheda **Diritti**.

L'attività di rete delle applicazioni è controllata da [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** , **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 utente*) 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
6. Nel blocco **Diritti dell'applicazione e risorse protette**, fare clic sul pulsante **Modifica**.
7. Per l'impostazione **Gruppo di attendibilità per le applicazioni avviate prima dell'esecuzione di Kaspersky Endpoint Security for Windows**, selezionare il [gruppo di attendibilità](#) appropriato.
8. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **Prevenzione Intrusioni Host**.
5. Per l'impostazione **Gruppo di attendibilità per le applicazioni avviate prima dell'esecuzione di Kaspersky Endpoint Security for Windows**, 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 dell'esecuzione di Kaspersky Endpoint Security for Windows**, 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
6. Nella sezione **Regole di elaborazione delle applicazioni**, utilizzare l'elenco a discesa **Gruppo di attendibilità per le applicazioni che non potevano essere aggiunte ai gruppi esistenti** 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.
7. 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.
8. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **Prevenzione Intrusioni Host**.
5. Nella sezione **Regole di elaborazione delle applicazioni**, utilizzare l'elenco a discesa **Gruppo di attendibilità per le applicazioni che non potevano essere aggiunte ai gruppi esistenti** 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 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.
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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
6. 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 Attendibili 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](#).
7. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **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 Attendibili 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 Attendibili 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
6. 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.
7. Selezionare la scheda **Diritti applicazione**.
8. Fare clic su **Aggiungi**.
9. Nella finestra visualizzata, immettere i criteri per cercare l'applicazione di cui si 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.
10. Fare clic sul pulsante **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.
11. Selezionare l'applicazione desiderata.
12. 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.
13. Selezionare l'applicazione opportuna, quindi selezionare **Diritti applicazione** dal menu di scelta rapida dell'applicazione.
Verranno visualizzate le proprietà dell'applicazione.
14. 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 la scheda **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 la scheda **Diritti**.

L'attività di rete delle applicazioni è controllata da [Firewall](#) mediante le *regole di rete*.

15. 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** (⊘).

16. 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.

17. Salvare le modifiche.





[Come modificare i diritti dell'applicazione in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
 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 avanzata** → **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 di **Applicazione**. Fare clic sul pulsante **Avanti**.
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 facendo clic su **OK**.
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 da [Firewall](#) mediante le *regole di rete*.
14. Per la risorsa opportuna, nella colonna dell'azione corrispondente selezionare l'opzione necessaria: **Eredita**, **Consenti** (✔) o **Vieta** (✘).
 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 sul pulsante **Gestisci applicazioni**.
Verrà visualizzato l'elenco delle applicazioni installate.
4. Selezionare l'applicazione desiderata.
5. Nel 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 la scheda **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 la scheda **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** , **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	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 l'attività dell'applicazione	Kaspersky Endpoint Security non monitorerà l'attività file e rete dell'applicazione nel sistema operativo. Le attività dell'applicazione vengono monitorate dai seguenti componenti: Rilevamento del Comportamento , Prevenzione Exploit , Prevenzione Intrusioni Host , Motore di Remediation e Firewall .
Non ereditare le restrizioni del processo principale (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 l'attività	Kaspersky Endpoint Security non monitorerà l'attività file o l'attività di rete delle applicazioni avviate dall'applicazione.

dell'applicazione secondaria	
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 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.

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.

Per proteggere le risorse del sistema operativo ubicate nel Registro di sistema `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet`, è necessario aggiungere le chiavi del Registro di sistema ubicate in `\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet???`. Ad esempio, `\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet???\services*\`. Questo è dovuto alle specifiche di funzionamento del Registro di sistema di Windows.



[Come aggiungere una risorsa protetta 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
6. 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.
7. Selezionare la 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.
8. 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**.
9. 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**.
10. 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.
11. Salvare le modifiche.

[Come aggiungere una risorsa protetta in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **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 **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 sul pulsante **Aggiungi**.
Verrà avviata la creazione guidata della nuova risorsa.
8. Fare clic sul collegamento **Nome gruppo** per 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 facendo clic su **OK**.
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 sul pulsante **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  **Disabilita 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Prevenzione Intrusioni Host**.
6. Nella sezione **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** 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**.


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.

7. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **Prevenzione Intrusioni Host**.
5. Nella sezione **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** 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**.
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. Nella sezione **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** 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**.

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

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 controlla l'accesso delle applicazioni al flusso audio e al flusso video come segue:

- Le applicazioni delle categorie Attendibili e Restrizione bassa possono ricevere il flusso audio e video dai dispositivi per impostazione predefinita.
- Le applicazioni delle categorie Restrizione alta e Non attendibili non possono ricevere il flusso audio e video dai dispositivi per impostazione predefinita.

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.

Motore di Remediation

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 virus](#).


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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Protezione minacce avanzata** → **Motore di Remediation**.
6. Utilizzare la casella di controllo **Motore di Remediation** per abilitare o disabilitare il componente.
7. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **Motore di Remediation**.
5. Utilizzare l'interruttore **Motore di Remediation** per abilitare o disabilitare il componente.
6. Salvare le modifiche.

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.

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 l'utente sta partecipando a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla categoria e sulla reputazione dei file esaminati, nonché informazioni sulla reputazione degli indirizzi Web esaminati.

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.

Per ridurre il carico sui server KSN, gli esperti di Kaspersky possono rilasciare aggiornamenti dell'applicazione che disabilitano temporaneamente o limitano parzialmente le richieste a Kaspersky Security Network. In tal caso, lo stato della connessione a KSN nell'interfaccia locale dell'applicazione è *Abilitato con restrizioni*.

Infrastruttura KSN

Kaspersky Endpoint Security supporta le seguenti soluzioni infrastrutturali KSN:

- *KSN Globale* è la soluzione utilizzata dalla maggior parte delle applicazioni Kaspersky. I partecipanti KSN ricevono le informazioni da Kaspersky Security Network 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 di Kaspersky Security Network.

- *KSN Privato* 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 Security Network e ad altri dati statistici senza inviare dati a KSN dai propri computer. KSN Privato 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 impostazione predefinita, Kaspersky Security Center utilizza KSN Globale. È possibile configurare l'uso di KSN Privato in Administration Console (MMC), in Kaspersky Security Center Web Console e nella [riga di comando](#). Non è possibile configurare l'utilizzo di KSN Privato in Kaspersky Security Center Cloud Console.

Per ulteriori dettagli su KSN Privato, consultare la documentazione relativa a Kaspersky Private Security Network.

Abilitazione e disabilitazione dell'utilizzo di Kaspersky Security Network

Per abilitare o disabilitare l'utilizzo di Kaspersky Security Network:

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.

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.
4. Se necessario, disattivare l'interruttore **Abilita modalità KSN estesa**.
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 KSN Privato

KSN Privato (di seguito denominato anche KPSN) 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 attendibile" nel database di reputazione locale ma ha una reputazione "attendibile" in KSN/KPSN, Kaspersky Endpoint Security rileverà il file come "non attendibile" 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](#).

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.

Per abilitare o disabilitare la modalità cloud per i componenti della protezione:

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 con KSN tramite il servizio Proxy KSN.

Il servizio Proxy KSN 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 proxy KSN 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 proxy KSN come segue: abilitare o disabilitare il proxy KSN e configurare la porta per la connessione. A tale scopo, è necessario aprire le proprietà di Administration Server. Per informazioni dettagliate sulla configurazione del proxy KSN, consultare la Guida di Kaspersky Security Center. È inoltre possibile abilitare o disabilitare il proxy KSN per i singoli computer nel criterio di Kaspersky Endpoint Security.

[Come abilitare o disabilitare il proxy KSN in Administration Console \(MMC\)](#)

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. Nel blocco **Impostazioni proxy KSN**, utilizzare la casella di controllo **Usa Proxy KSN** per abilitare o disabilitare il proxy KSN.
4. Se necessario, selezionare la casella di controllo **Usa i server KSN quando il proxy KSN non è disponibile**.
Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza i server KSN quando il servizio proxy KSN non è disponibile. I server KSN possono essere gestiti sia da Kaspersky (quando si utilizza KSN Globale) che da terze parti (quando si utilizza KSN Privato).
5. Salvare le modifiche.

[Come abilitare o disabilitare il proxy KSN in Web Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 avanzata** → **Kaspersky Security Network**.
5. Utilizzare la casella di controllo **Usa Proxy KSN** per abilitare o disabilitare il proxy KSN.
6. Se necessario, selezionare la casella di controllo **Usa i server KSN quando il proxy KSN non è disponibile**.
Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza i server KSN quando il servizio proxy KSN non è disponibile. I server KSN possono essere gestiti sia da Kaspersky (quando si utilizza KSN Globale) che da terze parti (quando si utilizza KSN Privato).
7. Salvare le modifiche.

L'indirizzo del proxy KSN corrisponde all'indirizzo di Administration Server. Quando il nome di dominio di Administration Server viene modificato, è necessario aggiornare manualmente l'indirizzo del proxy KSN.

Per configurare l'indirizzo del proxy KSN:

1. In Administration Console accedere alla cartella **Administration Server** → **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.
2. Nel menu di scelta rapida della cartella **Pacchetti di installazione**, selezionare **Proprietà**.
3. Nella scheda **Generale** nella finestra aperta, specificare il nuovo indirizzo del server proxy KSN.
4. Salvare le modifiche.

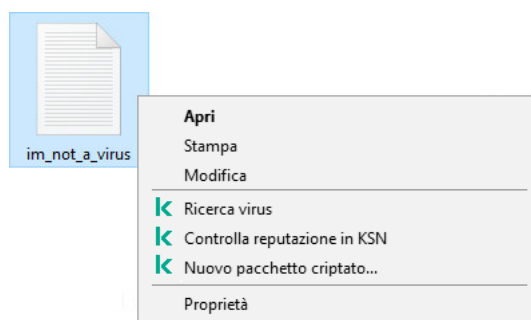
Controllo della reputazione di un file in Kaspersky Security Network

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)**. La maggior parte degli utenti di Kaspersky Security Network ha confermato che il file è attendibile.

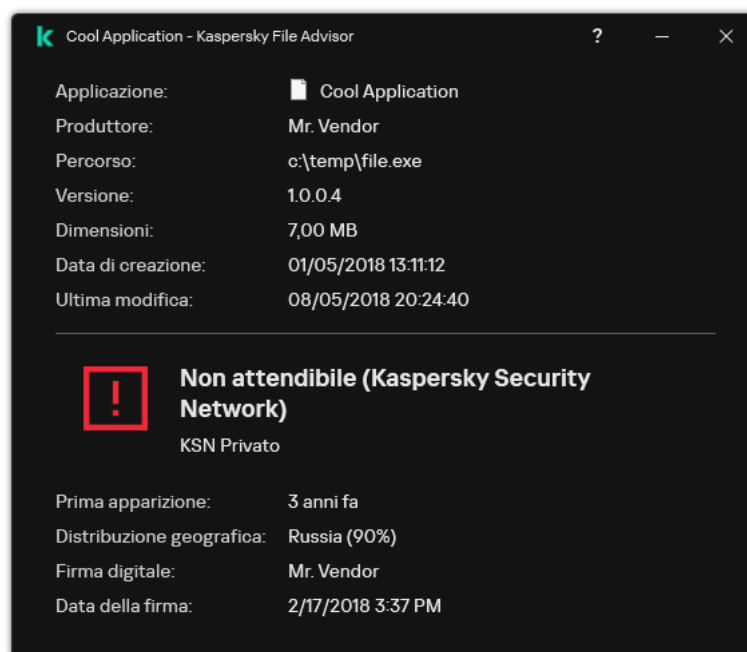
⚠ **Software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali**. Benché non presentino funzioni pericolose, le applicazioni di questo tipo possono essere sfruttate dagli utenti malintenzionati. Per ulteriori dettagli sul software legittimo utilizzabile da utenti malintenzionati 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: *KSN Globale* o *KSN Privato*.

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](#) e [Protezione minacce Web](#) 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 abilitare la scansione delle connessioni criptate:

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 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 file, 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).
6. Salvare le modifiche.

Parametro	Descrizione
Certificati radice attendibili	<p>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.</p>
Quando si visita un dominio con un certificato non attendibile	<ul style="list-style-type: none"> • 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 <i>Non attendibile</i>. 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 connessione. 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.
Quando si verificano errori durante la scansione delle connessioni criptate	<ul style="list-style-type: none"> • Blocca connessione. Se questo elemento è selezionato, quando si verifica un errore di scansione delle connessioni criptate, Kaspersky Endpoint Security blocca la connessione di rete. • Aggiungi dominio alle esclusioni. Se questo elemento è selezionato, quando 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 connessione. Kaspersky Endpoint Security genera anche un evento per l'errore di scansione della connessione criptata.
Blocca le connessioni SSL 2.0 (opzione consigliata)	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security blocca le connessioni di rete stabilite tramite il protocollo SSL 2.0.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non blocca le connessioni di rete stabilite tramite il protocollo SSL 2.0 e non monitora il traffico di rete trasmesso mediante queste connessioni.</p>
Decripta una connessione criptata con il sito Web	<p>I certificati EV (Extended Validation) 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.</p>

che utilizza il certificato EV

Se la casella di controllo è selezionata, Kaspersky Endpoint Security decripta e monitora le connessioni criptate con siti Web che utilizzano un certificato EV.

Se la casella di controllo è deselezionata, Kaspersky Endpoint Security 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Impostazioni generali** → **Impostazioni di rete**.
6. Nel blocco **Certificati radice attendibili**, fare clic su **Aggiungi**.
7. Viene visualizzata una finestra, che consente di selezionare un certificato radice attendibile.
Kaspersky Endpoint Security supporta certificati con estensioni PEM, DER e CRT.
8. Salvare le modifiche.

[Come installare i certificati radice attendibili in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 su **Mostra certificati**.
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 su **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.

- 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Impostazioni generali** → **Impostazioni di rete**.
6. Nel blocco **Scansione delle connessioni criptate**, fare clic sul pulsante **Impostazioni avanzate**.
7. Viene visualizzata una finestra; in tale finestra, selezionare la modalità operativa dell'applicazione quando si visita un dominio con un certificato non attendibile: **Consenti connessione** o **Blocca connessione**.
8. Salvare le modifiche.

[Come configurare la scansione delle connessioni criptate con un certificato non attendibile in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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**, selezionare la modalità operativa dell'applicazione quando si visita un dominio con un certificato non attendibile: **Consenti connessione** o **Blocca connessione**.
6. 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. In **Scansione delle connessioni criptate**, selezionare la modalità operativa dell'applicazione quando si visita un dominio con un certificato non attendibile: **Consenti connessione** o **Blocca connessione**.
4. Salvare le modifiche.



Visita di un dominio con un certificato non attendibile

La connessione non è sicura. Gli utenti malintenzionati possono tentare di intercettare i dati privati. È consigliabile non utilizzare più il sito Web.

revoked.badssl.com

Motivo:

L'attendibilità per questo certificato o uno dei certificati nella catena è stata revocata.

[Visualizza certificato](#)

[Comprendo i rischi ma desidero procedere](#)

Scansione delle connessioni criptate in Firefox e Thunderbird


Dopo l'installazione, Kaspersky Endpoint Security aggiunge un certificato Kaspersky all'archivio di sistema per i certificati attendibili (archivio certificati Windows). Per impostazione predefinita, Firefox e Thunderbird utilizzano il proprio archivio certificati proprietario Mozilla invece dell'archivio certificati di 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 in Firefox e Thunderbird per analizzare il traffico di queste applicazioni. Se un criterio non viene applicato al computer, è possibile scegliere l'archivio certificati che verrà utilizzato dalle applicazioni Mozilla. Se è stato selezionato l'archivio certificati Mozilla, aggiungere manualmente un certificato Kaspersky. 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, Kaspersky Endpoint Security non esamina il traffico nel browser Mozilla Firefox e nel client di posta Thunderbird.

Prima di aggiungere un certificato all'archivio Mozilla, esportare il certificato Kaspersky dal Pannello di controllo di Windows (proprietà del browser). Per ulteriori dettagli sull'esportazione del certificato Kaspersky, consultare la [Knowledge Base dell'Assistenza tecnica](#). Per i dettagli relativi all'aggiunta di un certificato all'archivio, visitare il [sito Web del supporto tecnico 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 in Firefox e Thunderbird:

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 **Mozilla Firefox e Thunderbird**, selezionare la casella di controllo **Utilizza l'archivio certificati selezionato per eseguire la scansione delle connessioni criptate nelle applicazioni Mozilla**.
4. Selezionare un archivio certificati:
 - **Usa archivio certificati Windows (consigliato)**. Il certificato radice di Kaspersky viene aggiunto a questo archivio durante l'installazione di Kaspersky Endpoint Security.
 - **Usa archivio certificati Mozilla**. 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.
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*. 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.

Per escludere un indirizzo Web dalle scansioni delle connessioni criptate:

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 **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 le maschere per gli indirizzi IP. È possibile immettere un intervallo di indirizzi IP nell'interfaccia dell'applicazione locale (ad esempio 198.51.100.0/24). Non è possibile immettere un intervallo di indirizzi IP in Kaspersky Security Center Console.


Esempi:

- - 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).
- - Il record comprende i seguenti indirizzi: <https://subdomain.domain.com>, <https://subdomain.domain.com/page123>. Il record è esclusivo del dominio 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.

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 **Dispositivi** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

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 **Selezionare i 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. Chiusura della procedura guidata.

Verrà visualizzata una nuova attività nell'elenco delle attività.

6. Fare clic sull'attività **Cancella dati** per 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 a mente che i dipendenti possono spegnere il computer prima di andare in vacanza. In tal caso, il periodo di mancata connessione può essere superato e i dati verranno eliminati. 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 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 sul pulsante **Esegui**.

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).

Kaspersky Endpoint Security monitora solo il traffico HTTP e HTTPS.

Per il monitoraggio del traffico HTTPS è necessario [abilitare la scansione delle connessioni criptate](#).

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 grafiche. 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 "File di immagini".

- **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 "File di 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.



Impossibile fornire la pagina Web richiesta.


Indirizzo: <http://kaspersky.ru/>.

La pagina Web è stata bloccata dalla regola kasp.

Motivo: la risorsa Web appartiene alle categorie di contenuti Non determinato e alle categorie di tipo di dati Non determinato.

Questa risorsa Web non è consentita a livello di azienda. Se si ritiene che il blocco sia stato applicato per errore o è necessario accedere a questa risorsa Web, contattare l'amministratore della rete aziendale locale ([Richiedi accesso](#)).

Data generazione messaggio: 10/14/2020 1:31:27 AM



La pagina Web richiesta potrebbe essere non protetta o non consentita dal criterio aziendale.

Indirizzo: <http://kaspersky.ru/>.

La pagina Web è stata bloccata dalla regola kasp.

Motivo: la risorsa Web appartiene alle categorie di contenuti Non determinato e alle categorie di tipo di dati Non determinato.

Per aprire la pagina Web richiesta, fare clic sul collegamento <http://kaspersky.ru/>.

Per ottenere l'accesso all'intero contenuto del sito Web a cui appartiene la pagina Web richiesta, fare clic sul collegamento http://kaspersky.ru/*.

Per ottenere l'accesso a tutti i domini esistenti di livello pari o inferiore a quello contrassegnato da "*", fare clic sul collegamento */*.kaspersky.ru/*.

L'accesso alle risorse Web elencate in precedenza verrà concesso per la durata della sessione corrente dell'applicazione.

Nel caso l'avviso sia stato visualizzato per errore, contattare l'amministratore della rete aziendale locale ([Richiedi accesso](#)).


Data generazione messaggio: 10/14/2020 1:31:50 AM

Messaggi di Controllo Web

Abilitazione e disabilitazione di Controllo Web

Controllo Web è abilitato per impostazione predefinita.

Per abilitare o disabilitare Controllo Web:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo Web**.
3. Utilizzare l'interruttore **Controllo Web** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Azioni con le regole di accesso alle risorse Web

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. Sono preimpostate due regole:

- La regola Script e fogli di stile, che consente a tutti gli utenti di accedere in qualsiasi momento alle risorse Web i cui indirizzi contengono nomi di file con le estensioni CSS, JS o VBS. Ad esempio:
`http://www.example.com/style.css`, `http://www.example.com/style.css?mode=normal`.
- Regola predefinita. 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.

Aggiunta di una regola di accesso alle risorse Web

Per aggiungere o modificare una regola 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**.
3. Nella sezione **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. Nella sezione **Azione** selezionare l'opzione opportuna:
 - **Consenti**. Se questo valore è selezionato, Kaspersky Endpoint Security consente l'accesso alle risorse Web che corrispondono ai parametri della regola.
 - **Blocca**. Se questo valore è selezionato, Kaspersky Endpoint Security blocca l'accesso alle risorse Web che corrispondono ai parametri della regola.
 - **Avvisa**. Se questo valore è selezionato, Kaspersky Endpoint Security visualizza un avviso che segnala che una risorsa Web è indesiderata quando l'utente tenta di accedere alle risorse Web che corrispondono alla regola. Utilizzando i collegamenti nel messaggio di avviso, l'utente può ottenere l'accesso alla risorsa Web richiesta.
8. Nella sezione **Contenuto 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 *Immagini grafiche*).

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 **Indirizzi** selezionare il filtro per gli indirizzi delle risorse Web attinente:
 - **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. Per creare un elenco di indirizzi delle risorse Web:

a. Fare clic sul pulsante **Aggiungere un indirizzo** o **Aggiungi gruppo di indirizzi**.

b. Nella finestra visualizzata, creare un elenco di indirizzi di 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](#).

c. Tornare alla finestra per la configurazione della regola di accesso alle risorse Web.

Se la [Scansione delle connessioni criptate è disabilitata](#), per il protocollo HTTPS è possibile filtrare solo in base al nome del server.

10. 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 le risorse Web solo per utenti specifici. Per creare un elenco di utenti a cui applicare la regola:

a. Fare clic su **Aggiungi**.

b. Nella finestra visualizzata, selezionare gli utenti o il gruppo 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.

11. 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.


12. Salvare le modifiche.

Assegnazione di priorità alle 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. 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.


È possibile assegnare le priorità alle regole nell'elenco disponendo le regole in un determinato ordine.

Per assegnare una priorità a una regola 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**.
3. Nella sezione **Impostazioni** fare clic sul pulsante **Regola di accesso alle risorse Web**.
4. Nella finestra visualizzata, selezionare la regola di cui si desidera modificare la priorità.
5. Utilizzare i pulsanti **Su** e **Giù** per spostare la regola nella posizione desiderata nell'elenco delle regole di accesso alle risorse Web.
6. Salvare le modifiche.

Abilitazione e disabilitazione di una regola di accesso alle risorse Web

Per abilitare o disabilitare una regola 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**.
3. Nella sezione **Impostazioni** fare clic sul pulsante **Regola di accesso alle risorse Web**.
4. Nella finestra visualizzata selezionare la regola che si desidera abilitare o disabilitare.
5. Nella colonna **Stato** eseguire le seguenti operazioni:
 - Per abilitare l'utilizzo della regola, selezionare il valore **Attivato**.
 - Per disabilitare l'utilizzo della regola, selezionare il valore **Disattivato**.
6. Salvare le modifiche.

Esportazione e importazione dell'elenco degli indirizzi Web attendibili

È possibile esportare l'elenco delle regole di Controllo Web in un file XML. 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri, selezionare **Controlli di sicurezza** → **Controllo Web**.
6. 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.
7. 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.
8. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 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.
6. Per importare l'elenco delle regole, nella sezione **Elenco di 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.
7. Salvare le modifiche.

Verifica delle regole di accesso alle risorse Web

È possibile verificare la coerenza delle regole di Controllo Web. A tale scopo, il componente Controllo Web include una funzione Diagnostica regole.

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**.
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** e 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 dell'elenco di indirizzi delle risorse 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 con estensione txt. 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.

Per importare o esportare un elenco di indirizzi di risorse Web in un file:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo Web**.
3. Nella sezione **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 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.
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 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.




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 è compatibile con altri browser.


Kaspersky Endpoint Security crea i seguenti eventi sulle attività Internet degli utenti:

- Bloccare il sito Web (stato *Eventi critici* .
- Visitare un sito Web non consigliato (stato *Avvisi* .
- Visitare un sito Web consentito (stato *Messaggi informativi* .

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](#).

Per inoculare lo script per l'interazione con le pagine Web nel traffico Web:


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 **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](#).

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 **Impostazioni di notifica**.
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> e <http://www.example.com/gallery>, Kaspersky Endpoint Security invierà un solo evento con l'oggetto <http://www.example.com>.

Per abilitare la registrazione degli eventi per visitare 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**.
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**.
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, 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.

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. È possibile modificarne il contenuto.

Per modificare il modello per i messaggi di Controllo Web:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **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.

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 di indirizzi `example.com` include 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.

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.

Migrazione delle regole di accesso alle risorse Web da versioni precedenti dell'applicazione

Quando si esegue l'upgrade di Kaspersky Endpoint Security 10 Service Pack 2 for Windows o di una versione precedente dell'applicazione a Kaspersky Endpoint Security for Windows 11.9.0, viene eseguita la migrazione delle regole di accesso alle risorse Web basate sulle categorie di contenuti delle risorse Web nel modo seguente:

- Le regole di accesso alle risorse Web basate su una o più categorie di contenuti delle risorse Web negli elenchi "Chat, forum, IM", "E-mail basata sul Web" e "Social network" vengono migrate alla categoria di contenuti delle risorse Web "Comunicazioni di rete".
- Le regole di accesso alle risorse Web basate su una o più categorie di contenuti delle risorse Web negli elenchi "Acquisti online" e "Sistemi di pagamento" vengono migrate alla categoria di contenuti delle risorse Web "Acquisti online, banche, sistemi di pagamento".
- Le regole di accesso alle risorse Web basate sulla categoria di contenuti delle risorse Web "Gioco d'azzardo" vengono migrate alla categoria di contenuti "Gioco d'azzardo, lotterie, scommesse".
- Le regole di accesso alle risorse Web basate sulla categoria di contenuti delle risorse Web "Giochi tramite browser" vengono migrate alla categoria di contenuti "Giochi per computer".
- Le regole di accesso alle risorse Web basate su categorie di contenuti delle risorse Web non menzionate nell'elenco precedente vengono migrate senza modifiche.

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.

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 – ⓧ.
 - Dipende dal bus di connessione (eccetto per il 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). Di conseguenza è possibile limitare la connessione di tutti i dispositivi, ad esempio tramite 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.

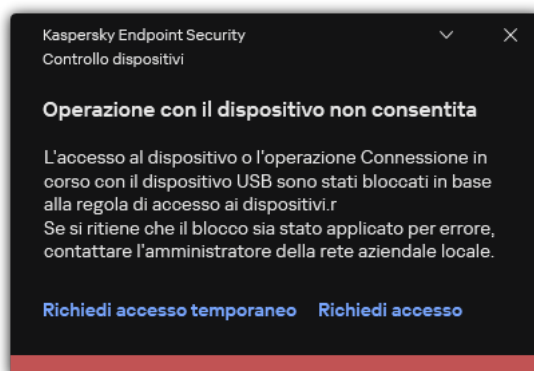
È possibile aggiungere dispositivi attendibili in base ai seguenti dati:

- **Dispositivi per ID.** Ogni dispositivo ha un identificatore univoco (ID hardware o HWID). È possibile visualizzare l'ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. ID dispositivo di esempio: 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 ID fornitore (VID) e un ID prodotto (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.

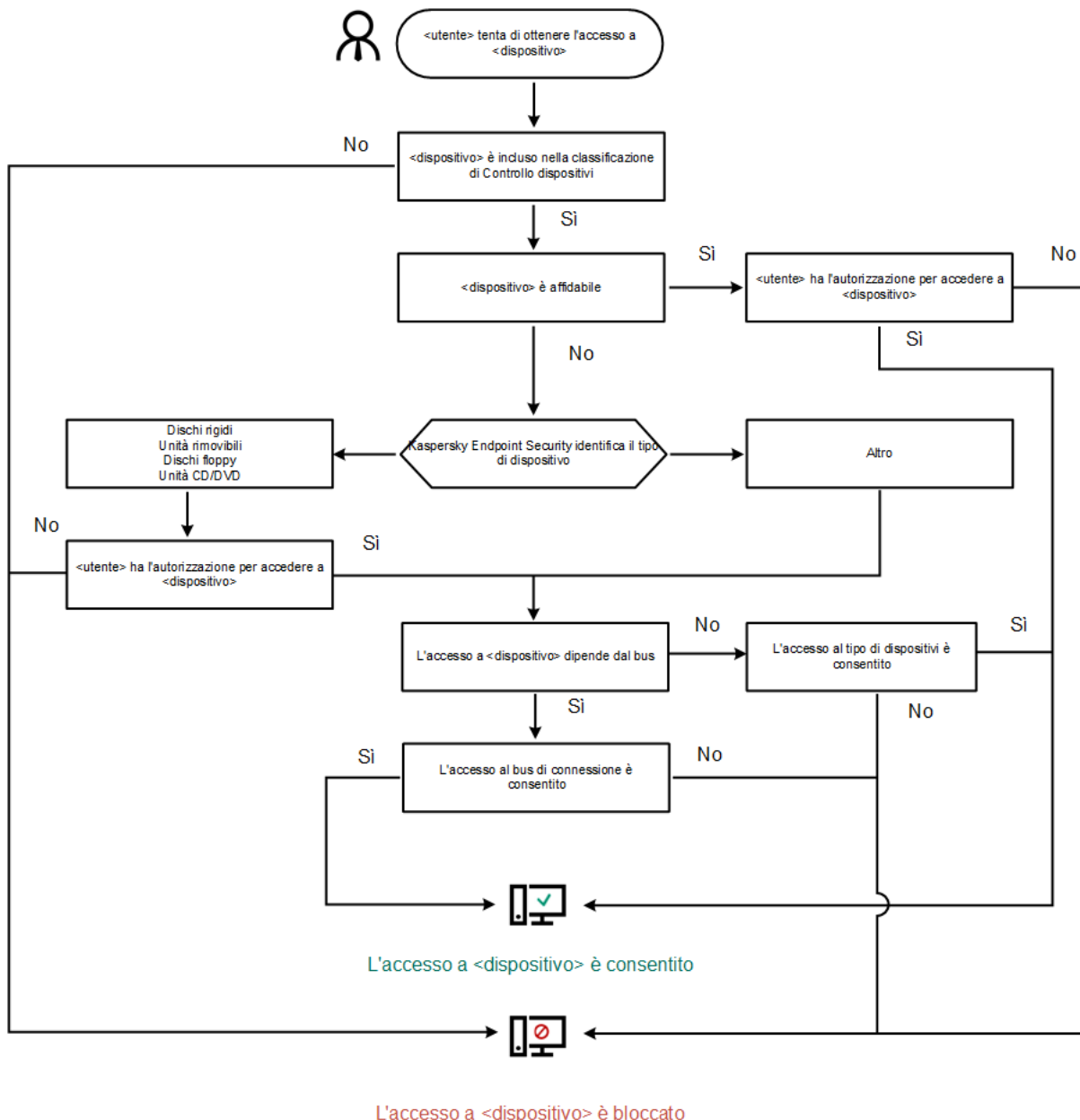
Quando un dispositivo bloccato da Controllo dispositivi viene connesso al computer, Kaspersky Endpoint Security bloccherà l'accesso e mostrerà una notifica (vedere la figura seguente).



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).



L'accesso a <dispositivo> è bloccato

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](#).

Abilitazione e disabilitazione di Controllo dispositivi

Controllo dispositivi è abilitato per impostazione predefinita.

Per abilitare o disabilitare Controllo dispositivi:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Controlli di sicurezza** → **Controllo dispositivi**.

3. Utilizzare l'interruttore **Controllo dispositivi** per abilitare o disabilitare il componente.

4. Salvare le modifiche.

Di conseguenza, 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** → **Archivio** → **Hardware**.

Informazioni sulle regole di accesso

Le *regole di accesso* comprendono un gruppo di impostazioni che determinano quali utenti possono accedere ai dispositivi installati o connessi al computer. 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	✓	✓	✓	✓	✓
Stampanti	✓	–	–	–	–
Dischi floppy	✓	✓	✓	✓	✓
Unità CD/DVD	✓	✓	✓	✓	✓
Modem	✓	–	–	–	–
Dispositivi a nastro	✓	–	–	–	–
Dispositivi multifunzione	✓	–	–	–	–
Lettori di smart card	✓	–	–	–	–
Dispositivi ActiveSync USB Windows CE	✓	–	–	–	–
Schede di rete esterne	✓	–	–	–	–
Dispositivi portatili (MTP)	✓	✓	✓	✓	✓
Bluetooth	✓	–	–	–	–


Fotocamere e scanner	✓	–	–	–	–
----------------------	---	---	---	---	---

Regole di accesso ai dispositivi mobili




I dispositivi mobili che eseguono Android o iOS sono categorizzati come dispositivi portatili (MTP). Quando un dispositivo mobile è connesso al computer, il sistema operativo determina il tipo di dispositivo. Se nel computer sono installati ADB (Android Debug Bridge), 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.

Tenere presenti le seguenti considerazioni speciali relative all'accesso ai dispositivi ADB o iTunes:



- Non è possibile configurare una pianificazione di accesso ai dispositivi. Se l'accesso ai dispositivi è limitato dalle regole (hanno lo stato ) , i dispositivi ADB e iTunes sono sempre accessibili.
- Non è possibile configurare l'accesso ai dispositivi per singoli utenti o configurare le autorizzazioni di accesso (lettura/scrittura). Se l'accesso ai dispositivi è limitato dalle regole (hanno lo stato ) , i dispositivi ADB e iTunes sono accessibili a tutti gli utenti con tutte le autorizzazioni.
- Non è possibile configurare l'accesso ai dispositivi ADB o iTunes attendibili per singoli utenti. Se il dispositivo è attendibile, i dispositivi ADB e iTunes sono accessibili a tutti gli utenti.
- 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 impostazione predefinita, le regole di accesso consentono a tutti gli utenti di accedere in modo completo ai dispositivi in qualsiasi momento, se è consentito l'accesso ai bus di connessione per i tipi di dispositivi corrispondenti (stato ) .

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

Le regole di accesso ai bus di connessione determinano se la connessione dei dispositivi è consentita (stato ) o vietata (stato ) . Per impostazione predefinita, vengono create regole che consentono l'accesso a tutti i bus di connessione presenti nella classificazione del componente Controllo dispositivi.

Modifica di una regola di accesso ai dispositivi

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.

Per modificare una regola di accesso ai dispositivi:

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 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 ai dispositivi di archiviazione** selezionare la regola di accesso che si desidera modificare. La sezione contiene dispositivi che dispongono di un file system per il quale è possibile configurare ulteriori impostazioni di accesso. Per impostazione predefinita, una regola di accesso ai dispositivi consente agli utenti l'accesso completo al tipo di dispositivi specificato in qualsiasi momento.

a. Nella colonna **Accesso**, selezionare l'opzione di accesso al dispositivo appropriata:

- **Consenti.**

- **Blocca.**

- **Dipende dal bus di connessione.**

Per bloccare o consentire l'accesso a un dispositivo, [configurare l'accesso al bus di connessione](#).

- **Limita in base alle regole.**

Questa opzione consente di configurare i diritti utente, le autorizzazioni e una pianificazione per l'accesso al dispositivo.

b. Nella sezione **Diritti degli utenti** fare clic sul pulsante **Aggiungi**.

Verrà visualizzata una finestra per l'aggiunta di una nuova regola di accesso al dispositivo.

c. Assegnare una priorità alla *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.

d. Selezionare lo stato **Abilitato** per la regola di accesso al dispositivo.

e. Configurare le autorizzazioni di accesso al dispositivo degli utenti: lettura e/o scrittura.


f. Selezionare gli utenti o il gruppo di utenti al quale si desidera applicare la regola di accesso al dispositivo.

g. Configurare una pianificazione di accesso al dispositivo per gli utenti.

- h. Fare clic sul pulsante **Aggiungi**.
5. Nella sezione **Accesso ai dispositivi esterni**, selezionare la regola e configurare l'accesso: **Consenti**, **Blocca** o **Dipende dal bus di connessione**. Se necessario, [configurare l'accesso al bus di connessione](#).
6. Nella sezione **Accesso alle reti Wi-Fi**, fare clic sul collegamento **Wi-Fi** e configurare l'accesso: **Consenti**, **Blocca** o **Blocca con eccezioni**. Se necessario, [aggiungere le reti Wi-Fi all'elenco delle reti attendibili](#).
7. Salvare le modifiche.

Modifica di una regola di accesso ai 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**.
6. Salvare le modifiche.

Aggiunta di una rete Wi-Fi all'elenco delle reti attendibili

È possibile consentire agli utenti di connettersi alle reti Wi-Fi che si considerano sicure, ad esempio una rete Wi-Fi aziendale. A tale scopo, è necessario aggiungere la rete all'elenco delle reti Wi-Fi attendibili. Controllo dispositivi bloccherà l'accesso a tutte le reti Wi-Fi tranne quelle specificate nell'elenco delle reti attendibili.

Per aggiungere una rete Wi-Fi all'elenco delle reti 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. Nella sezione **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.
5. Nel blocco **Accesso**, selezionare **Blocca con eccezioni**.
6. Nel blocco **Reti Wi-Fi attendibili**, fare clic sul pulsante **Aggiungi**.

7. Nella finestra visualizzata, procedere come segue:

- a. Nel campo **Nome della rete** specificare il nome della rete Wi-Fi che si desidera aggiungere all'elenco delle reti attendibili.
- b. Nell'elenco a discesa **Tipo di autenticazione** selezionare il tipo di autenticazione utilizzato per la connessione alla rete Wi-Fi attendibile.
- c. Nell'elenco a discesa **Tipo di criptaggio** selezionare il tipo di criptaggio utilizzato per proteggere il traffico della rete Wi-Fi attendibile.
- d. Nel campo **Commento** è possibile specificare qualsiasi informazione sulla rete Wi-Fi aggiunta.

Una rete Wi-Fi viene considerata attendibile se le relative impostazioni corrispondono a tutte le impostazioni specificate nella regola.

8. Salvare le modifiche.


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. Nella sezione **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 ai dispositivi di archiviazione**, selezionare **Unità rimovibili**.
5. Nella finestra visualizzata, selezionare la scheda **Generazione di log**.
6. Attivare l'interruttore **Generazione di log**.
7. Nel blocco **Operazioni sui file**, selezionare le operazioni che si desidera monitorare: **Scrittura**, **Eliminazione**.
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
- Verdetto di 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\environment]
 - Per i sistemi operativi a 32 bit:
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\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 1000 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 *Informativo*.


Kaspersky Endpoint Security presenta le seguenti limitazioni durante l'utilizzo dei dispositivi attendibili:

- Le versioni 11.0.0–11.2.0 dei plug-in di amministrazione di Kaspersky Endpoint Security non possono funzionare con un elenco di dispositivi attendibili creato nelle versioni 11.3.0 e 11.4.0 di Kaspersky Endpoint Security. Per utilizzare un elenco di dispositivi attendibili creato in queste versioni, è necessario eseguire l'upgrade del plug-in di amministrazione alla versione 11.3.0 e 11.4.0 rispettivamente.
- Le versioni 11.3.0 e 11.4.0 dei plug-in di amministrazione di Kaspersky Endpoint Security non possono funzionare con un elenco di dispositivi attendibili creato in Kaspersky Endpoint Security 11.2.0 o in una versione precedente. Affinché queste versioni funzionino con un elenco di dispositivi attendibili, è necessario eseguire l'upgrade dell'applicazione rispettivamente alla versione 11.3.0 e 11.4.0. È inoltre possibile inviare una richiesta contenente una descrizione della situazione all'Assistenza tecnica tramite [Kaspersky CompanyAccount](#) ².
- Per eseguire la migrazione di un elenco di dispositivi attendibili da Kaspersky Endpoint Security versione 11.2.0 alla versione 11.3.0, inviare una richiesta contenente una descrizione della situazione all'Assistenza tecnica tramite [Kaspersky CompanyAccount](#) ².

Aggiunta di un dispositivo all'elenco Attendibili dall'interfaccia dell'applicazione

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).

Per aggiungere un dispositivo all'elenco Attendibili dall'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.
6. Nel campo **Commento** è possibile fornire qualsiasi informazione pertinente sul dispositivo attendibile.
7. Selezionare gli utenti o il gruppo di utenti per i quali si desidera consentire l'accesso ai dispositivi attendibili.
8. Salvare le modifiche.

Aggiunta di un dispositivo all'elenco Attendibili da Kaspersky Security Center

Kaspersky Security Center riceve informazioni sui dispositivi se Kaspersky Endpoint Security è installato nei computer e [Controllo Dispositivi è abilitato](#). 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.

È possibile aggiungere un dispositivo all'elenco dei dispositivi attendibili in base ai seguenti dati:

- **Dispositivi per ID.** Ogni dispositivo ha un identificatore univoco (ID hardware o HWID). È possibile visualizzare l'ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. ID dispositivo di esempio: `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 ID fornitore (VID) e un ID prodotto (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_*`.

Per aggiungere i dispositivi all'elenco dei dispositivi attendibili:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Controlli di sicurezza** → **Controllo dispositivi**.
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 sul pulsante **Aggiungi** e selezionare un metodo per aggiungere un dispositivo all'elenco dei dispositivi attendibili.
9. Per filtrare i dispositivi, selezionare un tipo di dispositivo dall'elenco a discesa **Tipo di dispositivo** (ad esempio **Unità rimovibili**).
10. 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 **Aggiorna**. Per visualizzare correttamente l'elenco dei dispositivi, è possibile aggiungere dispositivi tramite la maschera dell'ID del dispositivo.

11. Per filtrare i dispositivi, nel campo **Nome 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.

12. Fare clic sul pulsante **Aggiorna**.

La tabella visualizza un elenco dei dispositivi che soddisfano i criteri di filtro definiti.

13. Selezionare le caselle di controllo accanto ai nomi dei dispositivi da aggiungere all'elenco dei dispositivi attendibili.
14. Nel campo **Commento** immettere una descrizione del motivo dell'aggiunta di dispositivi all'elenco dei dispositivi attendibili.
15. Fare clic sul pulsante **Seleziona** a destra del campo **Consenti a utenti e/o gruppi di utenti**.
16. Selezionare un utente o un gruppo in Active Directory e confermare la selezione.
Per impostazione predefinita, l'accesso ai dispositivi attendibili è consentito per il gruppo Tutti.
17. 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.

Se il computer dispone già di un elenco di dispositivi attendibili, Kaspersky Endpoint Security richiederà di eliminare l'elenco esistente o di aggiungere nuove voci dal file XML.

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 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.

3. 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.

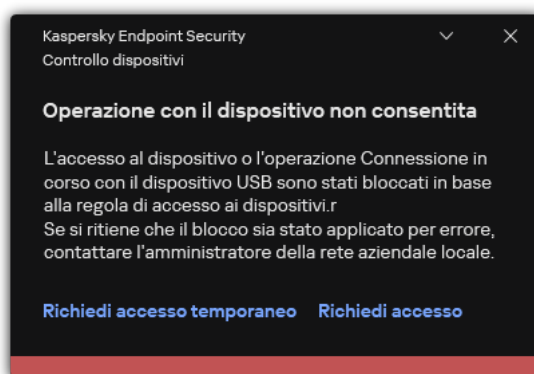
Kaspersky Endpoint Security mostrerà una notifica in cui viene indicato che l'accesso al dispositivo è bloccato (vedere la figura di seguito).

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**.

L'amministratore riceverà un messaggio contenente una richiesta di accesso, ad esempio tramite e-mail. Per ulteriori dettagli sull'elaborazione delle richieste degli utenti, consultare la [Guida di Kaspersky Security Center](#). Dopo l'[aggiunta del dispositivo all'elenco dei dispositivi attendibili](#) e dopo l'aggiornamento delle impostazioni di Kaspersky Endpoint Security nel computer, l'utente otterrà l'accesso al dispositivo.



Notifica Controllo dispositivi

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 richiesta di accesso temporaneo** deve essere selezionata.

Un utente richiede l'accesso a un dispositivo bloccato nel seguente modo:

1. Connettere il dispositivo al computer.

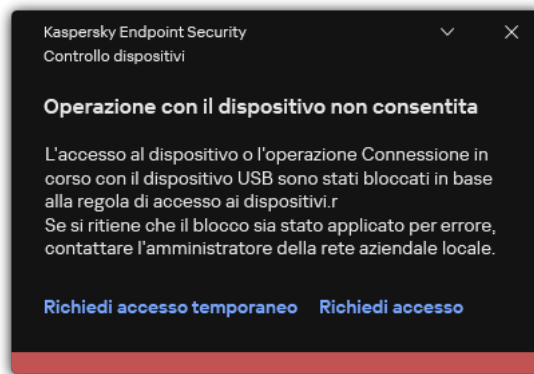
Kaspersky Endpoint Security mostrerà una notifica in cui viene indicato che l'accesso al dispositivo è bloccato (vedere la figura di seguito).

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 desiderato.
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. Nella finestra visualizzata, 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, selezionare **Dispositivi** → **Dispositivi gestiti**.
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 **Sfoggia** 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. 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.

Sono disponibili modelli per i messaggi relativi all'accesso bloccato ai dispositivi o alle operazioni vietate con il contenuto dei dispositivi e per il messaggio inviato all'amministratore. È possibile modificare i modelli dei messaggi.

Per modificare i modelli per i messaggi di Controllo dispositivi:

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 **Modelli di messaggi**, configurare i modelli per i messaggi di Controllo dispositivi:
 - **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.
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 tenere traccia dei comportamenti inusuali (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 **Attivazione delle regole con stato Smart Training**.

2. Analisi del rapporto sull'attivazione delle regole.

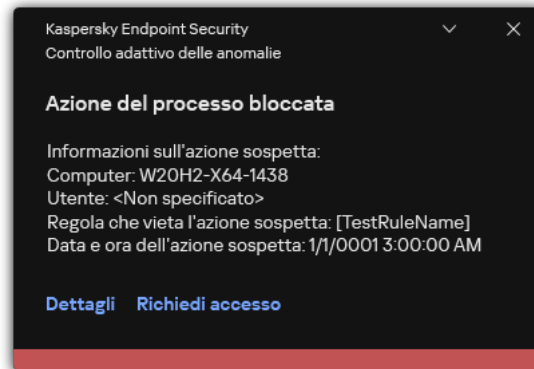
L'amministratore analizza il [rapporto sull'attivazione delle regole](#) o i contenuti dell'archivio **Attivazione delle regole con stato Smart Training**. L'amministratore può quindi selezionare il comportamento di Controllo adattivo delle anomalie quando viene attivata la regola, scegliendo se bloccarla 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. Controllo adattivo delle anomalie viene configurato 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 **Attivazione delle regole con stato Smart Training**. È consigliabile consultare il rapporto sull'attivazione delle regole e i contenuti dell'archivio **Attivazione delle regole con stato Smart Training**.

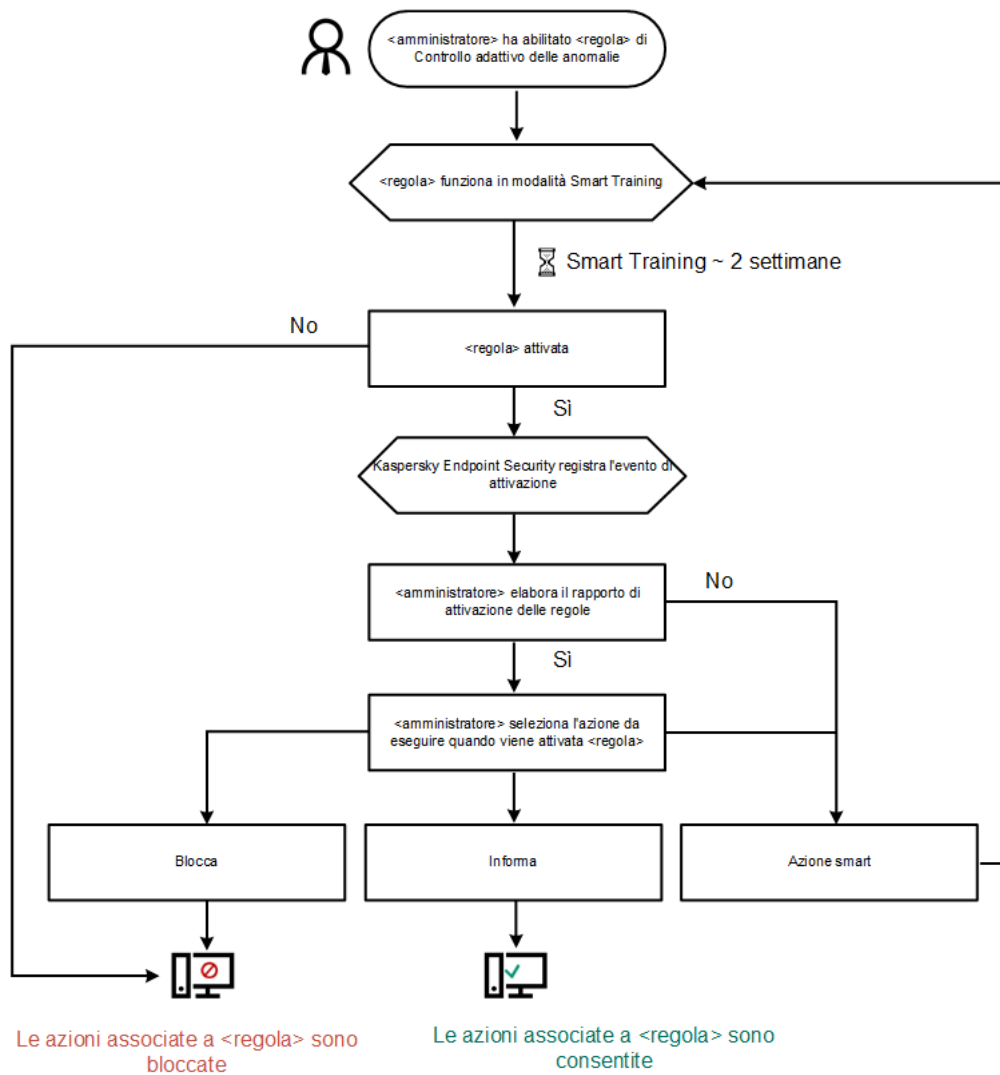
Quando un'applicazione dannosa tenta di eseguire un'azione, Kaspersky Endpoint Security blocca l'azione e visualizza una notifica (vedere la figura seguente).



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

Abilitazione e disabilitazione di Controllo adattivo delle anomalie

Controllo adattivo delle anomalie è abilitato per impostazione predefinita.

Per abilitare o disabilitare 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. Utilizzare l'interruttore **Controllo adattivo delle anomalie** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Di conseguenza, Controllo adattivo delle anomalie passerà alla modalità di addestramento. Durante l'addestramento, Controllo adattivo delle anomalie monitora l'attivazione delle regole. Al termine dell'addestramento, Controllo adattivo delle anomalie inizia a bloccare le azioni che non sono tipiche dei computer nella rete di un'azienda.

Se l'organizzazione ha iniziato a utilizzare alcuni nuovi strumenti e Controllo adattivo delle anomalie blocca le azioni di tali strumenti, è possibile reimpostare i risultati della modalità di addestramento e ripetere l'addestramento. A tale scopo, è necessario [modificare l'azione intrapresa quando viene attivata la regola](#) (ad esempio, impostarla su **Notifica**). Quindi è necessario riattivare la modalità di addestramento (impostare il valore **Azione smart**).


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. Nella sezione **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 *Avvia Windows PowerShell dalle applicazioni 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. Nella sezione **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 **Attivazione delle regole con 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.
- **Notifica.** 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. Nella sezione **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 **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.

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.** Codice hash 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://<oggetto>`, dove <oggetto> si riferisce al nome dell'oggetto, ad esempio `object://esempio.sito.web.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. È inoltre possibile utilizzare le maschere, ad esempio `object://*C:\Windows\temp*`.

- **Hash oggetto origine.** Codice hash 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.** Codice hash file.
- **Oggetto di destinazione.** Il comando per avviare il processo di destinazione. Specificare il comando utilizzando il modello seguente `object://<comando>`, 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.** Codice hash 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. Nella sezione **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 regole:
 - 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. Nella sezione **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 il messaggio sul blocco delle azioni potenzialmente dannose e per il messaggio da inviare all'amministratore. È possibile modificare i modelli dei messaggi.

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.
4. Salvare le modifiche.

Visualizzazione dei rapporti di Controllo adattivo delle anomalie

Per visualizzare i rapporti di Controllo adattivo delle anomalie:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio, selezionare **Controlli di sicurezza** → **Controllo adattivo delle anomalie**.
Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo adattivo delle anomalie.
6. Eseguire una delle seguenti operazioni:
 - Se si desidera visualizzare un rapporto sulle impostazioni delle regole di Controllo adattivo delle anomalie, fare clic su **Rapporto sullo stato delle regole di Controllo adattivo delle anomalie**.
 - Se si desidera visualizzare un rapporto sull'attivazione delle regole di Controllo adattivo delle anomalie, fare clic su **Rapporto sulle regole attivate di Controllo adattivo delle anomalie**.
7. Verrà avviato il processo di generazione del rapporto.

Il rapporto viene visualizzato in una nuova finestra.

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*), hash file, fornitore dell'applicazione e altri criteri.

2. [Gestione 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.

3. [Selezione della modalità di Controllo applicazioni](#).

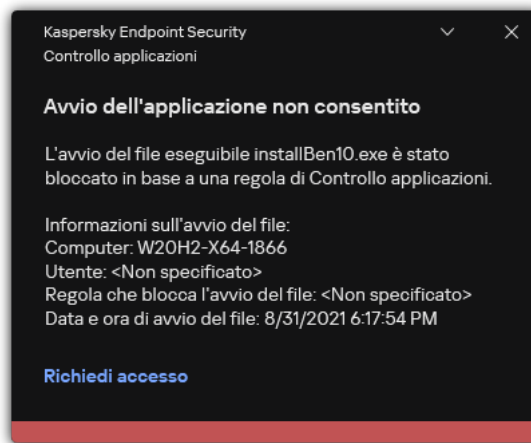
L'amministratore sceglie la modalità per l'utilizzo delle applicazioni che non sono incluse in nessuna delle regole: (lista vietati e lista consentiti delle applicazioni).

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.
- **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.

Questa modalità di Controllo applicazioni è abilitata per impostazione predefinita.

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.

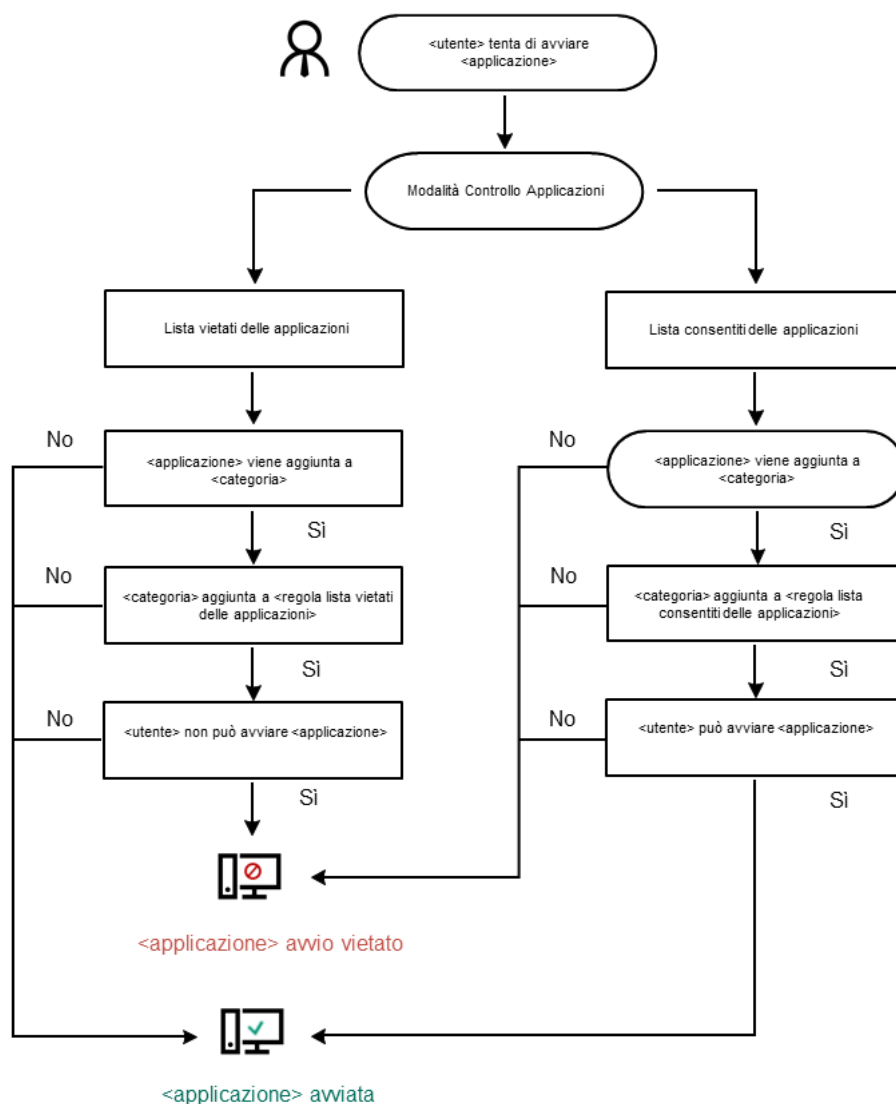
Tuttavia, Kaspersky Security Center offre strumenti che non sono disponibili nell'interfaccia locale di Kaspersky Endpoint Security, come gli strumenti necessari per le seguenti attività:

- [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.
- Quando viene eseguito l'upgrade della versione dell'applicazione, l'importazione delle impostazioni del componente Controllo applicazioni è supportata solo se viene eseguito l'upgrade di Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive a Kaspersky Endpoint Security 11.9.0 for Windows.

Quando viene eseguito l'upgrade di versioni dell'applicazione diverse da Kaspersky Endpoint Security 10 Service Pack 2 for Windows, le impostazioni di Controllo Applicazioni devono essere configurate nuovamente per ripristinare il componente allo stato operativo.

- 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 **Altre applicazioni \ 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.

Abilitazione e disabilitazione di Controllo applicazioni

Controllo applicazioni è disabilitato per impostazione predefinita.


Per abilitare o disabilitare 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. Utilizzare l'interruttore **Controllo applicazioni** per abilitare o disabilitare il componente.
4. Salvare le modifiche.

Di conseguenza, se Controllo applicazioni è abilitato, l'applicazione inoltra le informazioni sui file eseguibili a Kaspersky Security Center. È possibile visualizzare l'elenco dei file eseguibili in esecuzione in Kaspersky Security Center nella cartella **File eseguibili**. Per ricevere informazioni su tutti i file eseguibili anziché sui soli file eseguibili in esecuzione, eseguire l'[attività Inventario](#).

Selezione della modalità di Controllo applicazioni

Per selezionare la modalità 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. Nella sezione **Modalità Controllo avvio applicazioni** 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.

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.

Tutte le regole create nella modalità selezionata vengono salvate dopo la modifica della modalità, in modo da poterle riutilizzare. Per tornare a utilizzare queste regole, è sufficiente selezionare la modalità necessaria.

4. Nel blocco **Azione all'avvio delle applicazioni bloccate**, selezionare l'azione che deve essere eseguita dal componente quando un utente tenta di avviare un'applicazione bloccata dalle regole di Controllo applicazioni.
5. Selezionare la casella di controllo **Controlla caricamento moduli DLL** se si desidera che Kaspersky Endpoint Security monitori il caricamento dei moduli DLL quando le applicazioni vengono avviate dagli utenti.

Le informazioni sul modulo e sull'applicazione che lo ha caricato saranno salvate in un rapporto.

Kaspersky Endpoint Security monitora solo i moduli DLL e i driver caricati dal momento che è stata selezionata la casella di controllo. Riavviare il computer dopo aver selezionato la casella di controllo se si desidera che Kaspersky Endpoint Security monitori tutti i moduli DLL e i driver, compresi quelli caricati prima dell'avvio di Kaspersky Endpoint Security.

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 "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.

È consigliabile attivare la [protezione tramite password](#) per la configurazione delle impostazioni dell'applicazione, in modo che sia possibile disattivare le regole che bloccano l'avvio di moduli DLL e driver critici, senza modificare le impostazioni del criterio di Kaspersky Security Center.

6. Salvare le modifiche.

Utilizzo delle regole di Controllo applicazioni nell'interfaccia dell'applicazione

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 dal componente 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 di attivazione della regola ha la seguente correlazione: "tipo di condizione - criterio condizione - valore 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.
- **Test in corso.** 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 regola di Controllo applicazioni

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. Compilare o modificare un elenco di utenti e/o gruppi di utenti a cui è consentito o meno avviare le applicazioni che soddisfano le condizioni di attivazione della regola. A tale scopo, fare clic sul pulsante **Aggiungi** nella tabella **Soggetti e relativi diritti**.
Per impostazione predefinita, il valore **Tutti** viene aggiunto all'elenco degli utenti. La regola si applica a tutti gli utenti.

Se nella tabella non è specificato alcun utente, la regola non può essere salvata.

- d. Nella tabella **Soggetti 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 **Soggetti e relativi diritti** e non sono membri dei gruppi di utenti nella tabella **Soggetti 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 **Soggetti e relativi diritti** e che non appartengono ai gruppi di utenti specificati nella tabella **Soggetti 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** [creare](#) o modificare l'elenco delle condizioni di inclusione per l'attivazione della regola.


7. Nella scheda **Esclusioni** 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.

Aggiunta di una condizione di attivazione per una regola di Controllo applicazioni

Per aggiungere una nuova condizione di attivazione per 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. 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** o la scheda **Esclusioni** 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** o **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** o **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** o **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 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** 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**.

Modifica dello stato di una regola di Controllo applicazioni

Per modificare lo stato di 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. 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.
 - **Test in corso**. 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.

Gestione delle regole di Controllo applicazioni in Kaspersky Security Center

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 dal componente 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 di attivazione della regola ha la seguente correlazione: "tipo di condizione - criterio condizione - valore 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.
- **Test in corso.** 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.

Ricezione delle informazioni sulle applicazioni installate nei computer degli utenti

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.

Le informazioni sulle applicazioni utilizzate nei computer della rete LAN aziendale sono disponibili nella cartella **Registro delle applicazioni** e nella cartella **File eseguibili**. Le cartelle **Registro delle applicazioni** e **File eseguibili** sono contenute nella cartella **Gestione applicazioni** nella struttura di Kaspersky Security Center Administration Console.

La cartella **Registro delle applicazioni** contiene l'elenco delle applicazioni rilevate dal [Network Agent](#) installato nei computer client.

La cartella **File eseguibili** contiene un elenco di tutti i file eseguibili avviati nei computer client o rilevati durante l'attività di inventario di Kaspersky Endpoint Security.

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**.

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**.

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 la cartella **Avanzate** → **Gestione applicazioni** → **File eseguibili**.
3. Selezionare un file eseguibile.
4. Dal menu di scelta rapida del file eseguibile selezionare **Proprietà**.

Creazione delle categorie di 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:

1. Aprire Kaspersky Security Center Administration Console.
2. Nella struttura di Administration Console, selezionare la cartella **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 delle categorie utente.

Passaggio 1. Selezione del tipo di categoria

In questo passaggio selezionare uno dei seguenti tipi di categorie di applicazioni:

- **Categoria con contenuto aggiunto manualmente.** Se si seleziona questo tipo di categoria, durante il passaggio "Configurazione delle condizioni per l'inclusione di applicazioni in una categoria" e il passaggio "Configurazione delle condizioni per l'esclusione di applicazioni da una categoria" 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.** 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.** Se si seleziona questo tipo di categoria, durante il passaggio "Cartella archivi" sarà possibile specificare una cartella da cui i file eseguibili verranno inclusi automaticamente nella categoria.

Quando si crea una categoria con contenuti aggiunti 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

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 eseguibili.** 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 **Identificazione personale 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'applicazione.** Selezionare una cartella nel dispositivo client. Kaspersky Security Center aggungerà i file eseguibili di questa cartella alla categoria personalizzata.
- **Seleziona certificato 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 **Identificazione personale certificato** specificato.

- **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 eseguibili.** 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 compresi 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 compresi 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'applicazione.** Selezionare una cartella nel dispositivo client. Kaspersky Security Center aggiungerà i file eseguibili di questa cartella alla categoria personalizzata.
- **Seleziona certificato 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 SHA-256 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).**
- 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.

- Campo **Periodo di scansione (ore)**. In questo campo è possibile specificare il periodo di tempo (in ore) al termine del quale Kaspersky Security Center deselecta la categoria di applicazioni e la aggiunge a tutti i file eseguibili dei computer specificati presenti nella cartella **File eseguibili**.

Il campo è disponibile se la casella di controllo **Sincronizza i dati con l'archivio dell'Administration Server** è selezionata.

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:

- 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.

- 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 SHA-256 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).**

- 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 deselectata, 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.

- Campo **Periodo di scansione (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.

Questo campo è disponibile se è selezionata la casella di controllo **Forza scansione delle modifiche nella cartella**.

Passaggio 7. Creazione di una categoria personalizzata

Chiusura della procedura guidata.

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 la cartella **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 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 la versione Kaspersky Endpoint Security 10 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 la versione Kaspersky Endpoint Security 10 Service Pack 1)**.
8. Salvare le modifiche.

Aggiunta e modifica di una regola di Controllo applicazioni tramite Kaspersky Security Center

Per aggiungere o modificare una regola di Controllo applicazioni tramite Kaspersky Security Center:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo applicazioni.

6. Eseguire una delle seguenti operazioni:

- Per aggiungere una regola, fare clic sul pulsante **Aggiungi**.
- Per modificare una regola esistente, selezionarla nell'elenco di regole e fare clic sul pulsante **Modifica**.

Verrà visualizzata la finestra **Regola di Controllo applicazioni**.

7. 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 delle categorie utente.
 - 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.

8. Nella tabella **Soggetti e relativi diritti** fare clic sul pulsante **Aggiungi**.

9. Nella finestra visualizzata, specificare l'elenco degli utenti e/o dei gruppi di utenti per cui configurare l'autorizzazione per l'avvio delle applicazioni della categoria selezionata.

10. Nella tabella **Soggetti 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 **Nega** nelle righe corrispondenti.

11. Selezionare la casella di controllo **Nega per gli altri utenti** se si desidera impedire a tutti gli utenti che non compaiono nella colonna **Soggetto** e che non fanno parte del gruppo di utenti specificati nella colonna **Soggetto** di avviare le applicazioni che appartengono alla categoria selezionata.

12. 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.

13. 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:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo applicazioni.
6. 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 di Controllo applicazioni.
 - **Disattivato**. Questo stato indica che la regola viene ignorata durante l'esecuzione di 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.

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
6. 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.
7. Per esportare 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.
8. 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, selezionare **Dispositivi** → **Criteri e profili**.
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 applicazioni**.
5. Fare clic sul collegamento **Impostazioni elenchi per le regole**.
6. Selezionare un elenco di regole: lista vietati e lista consentiti per le applicazioni.
7. Per esportare l'elenco delle regole di Controllo applicazioni:
 - 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.
8. Per esportare 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.
9. Salvare le modifiche.

Verifica delle regole di Controllo applicazioni tramite Kaspersky Security Center

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.

Per abilitare o disabilitare il test delle regole di Controllo applicazioni in Kaspersky Security Center:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Controlli di sicurezza** → **Controllo applicazioni**.
Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo applicazioni.
6. 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.
7. 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**.
8. Salvare le modifiche.

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**.

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 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. Durante il passaggio **Selezione del tipo di modello di rapporto**, selezionare **Altro** → **Rapporto sulle applicazioni proibite in modalità di 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'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 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. Durante il 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

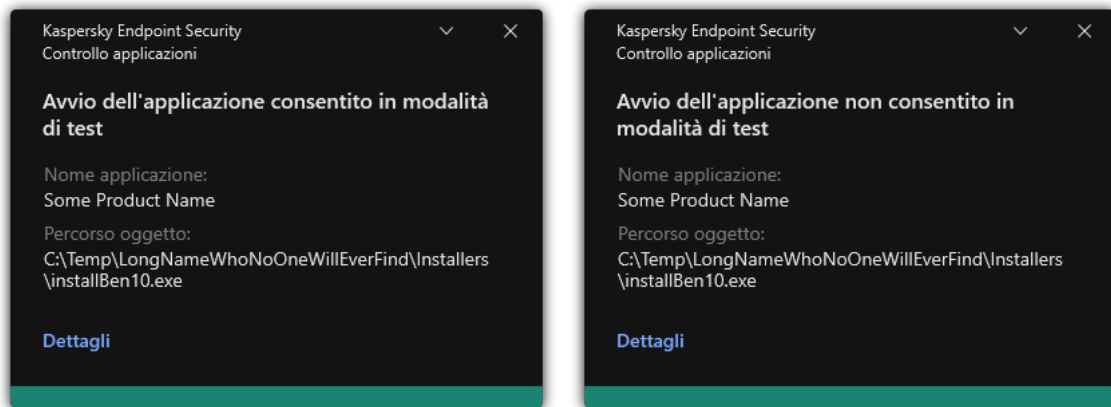
Per garantire che le regole di Controllo applicazioni non blocchino le applicazioni necessarie per le attività lavorative, è consigliabile abilitare la verifica delle regole di Controllo applicazioni e analizzare il relativo funzionamento dopo la creazione di nuove regole.

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 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 **Test in corso**.
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

Monitor attività applicazioni

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 dell'applicazione principale, 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** visualizza le informazioni su tutte le applicazioni installate nel computer.
- La scheda **In esecuzione** visualizza 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** consente di visualizzare 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Impostazioni generali** → **Interfaccia**.
6. Utilizzare la casella di controllo **Nascondi sezione Monitor attività applicazioni** per concedere o revocare l'accesso allo strumento.
7. 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, selezionare **Dispositivi** → **Criteri e profili**.
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** → **Interfaccia**.
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 `Cartella` con l'estensione `TXT` e un nome composto da tre caratteri.

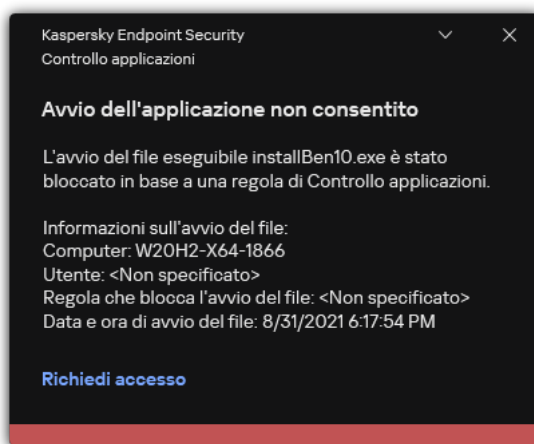
Modifica dei modelli dei messaggi di Controllo applicazioni

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. 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.

Sono disponibili speciali modelli per il messaggio visualizzato quando viene bloccato l'avvio di un'applicazione e per il messaggio inviato all'amministratore. È possibile modificare i modelli dei messaggi.

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 applicazioni**.
3. Nel blocco **Modelli di messaggi sul blocco delle applicazioni**, configurare i modelli per i messaggi di controllo 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. La notifica di un'applicazione bloccata è mostrata nella figura seguente.
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. 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.
4. Salvare le modifiche.



Notifica di Controllo applicazioni

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 **Soggetto** 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](#) e [Protezione minacce web](#) 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.


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**.
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 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 **Monitorare 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Impostazioni generali** → **Impostazioni di rete**.
6. Nel blocco **Porte monitorate**, selezionare **Monitora solo le porte di rete selezionate**.
7. 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.
8. 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.
9. Per esportare l'elenco delle applicazioni le cui porte sono monitorate da Kaspersky Endpoint Security:
 - a. Selezionare la casella di controllo **Monitorare 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.
10. 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.

11. 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.

12. Salvare le modifiche.

[Come esportare/importare gli elenchi delle porte monitorate in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 **N porte selezionate**.
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 **Monitorare tutte le porte per le applicazioni specificate**.
 - b. Fare clic sul collegamento **N applicazioni selezionate**.
 - 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.

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.

- 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.

Quando un utente tenta di eseguire un'azione protetta da password, Kaspersky Endpoint Security richiede all'utente nome utente e password o la password provvisoria (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.

The screenshot shows a Kaspersky dialog box titled "Modificare le impostazioni?". It contains the following elements:

- Label: "Nome utente:" followed by a text input field.
- Text below the field: "Il valore predefinito del nome utente: KLAdmin."
- Label: "Immettere la password:" followed by a text input field.
- Label: "Non richiedere conferma per i prossimi:" followed by a dropdown menu.
- Dropdown menu content: "Non selezionato" with a downward arrow.
- Text below the dropdown: "Per passare da una lingua di input all'altra, utilizzare ALT+MAI" followed by a blue button labeled "ENU".
- Two buttons at the bottom: "Conferma" (highlighted with a blue border) and "Annulla".

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 di dominio. Protezione tramite password supporta i seguenti account:

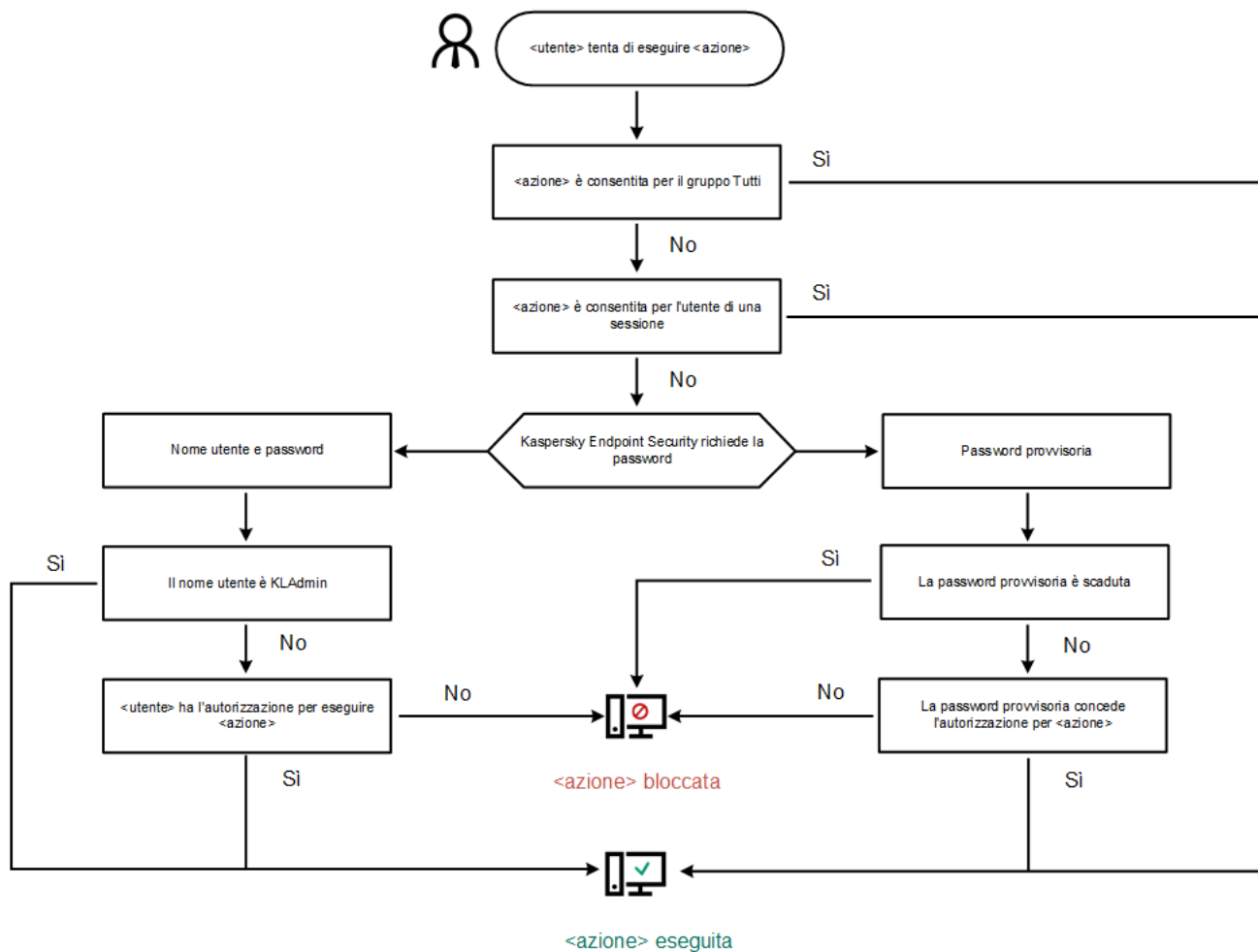
- **KLAdmin.** Account amministratore con accesso illimitato a Kaspersky Endpoint Security. L'account KLAdmin ha il diritto di eseguire qualsiasi azione protetta da password. Le autorizzazioni per l'account KLAdmin non possono essere revocate. Quando si abilita la protezione tramite password, Kaspersky Endpoint Security richiede di impostare una password per l'account KLAdmin.
- **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.

Algoritmo operativo della protezione tramite password

Kaspersky Endpoint Security decide se consentire o bloccare un'azione protetta da password in base al seguente algoritmo (vedere la figura seguente).




Algoritmo operativo della protezione tramite password

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).

Per abilitare la protezione tramite password:

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

È possibile concedere l'accesso a Kaspersky Endpoint Security a singoli utenti o gruppi. 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](#).

Per concedere autorizzazioni a singoli utenti o gruppi:

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. Nella finestra visualizzata, fare clic sul pulsante **Seleziona utente o gruppo**.
Verrà visualizzata la finestra di dialogo Selezionare utenti o gruppi standard.

5. Selezionare un utente o un gruppo in Active Directory e confermare la selezione.

6. 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.

7. 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

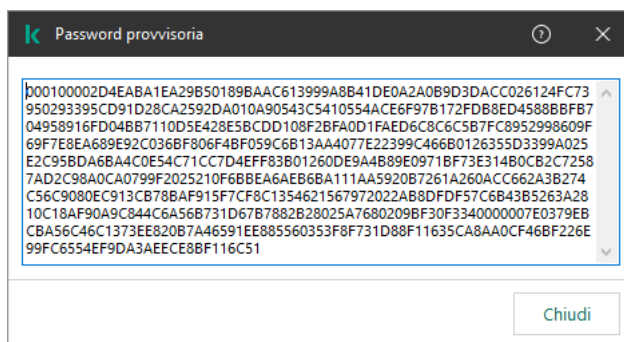
È possibile utilizzare una password provvisoria per concedere l'accesso provvisorio a Kaspersky Endpoint Security per un singolo computer all'esterno della rete aziendale. Questo è necessario per consentire all'utente di eseguire un'azione bloccata senza ottenere le credenziali dell'account KLAdmin. 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** e fare doppio clic per aprire le proprietà dell'applicazione.
Nella finestra delle impostazioni dell'applicazione selezionare **Impostazioni generali** → **Interfaccia**.
7. Nel blocco **Protezione tramite password**, fare clic sul pulsante **Impostazioni**.
8. Nel blocco **Password provvisoria**, fare clic sul pulsante **Impostazioni**.
9. Verrà visualizzata la finestra **Crea password provvisoria**.
10. Nel campo **Data di scadenza** specificare la data di scadenza della password provvisoria.
11. 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.
12. Fare clic su **Genera**.
Verrà visualizzata una finestra contenente la password provvisoria (vedere la figura seguente).
13. 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, selezionare **Dispositivi** → **Dispositivi gestiti**.
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 **Protezione tramite password**, fare clic sul pulsante **Password provvisoria**.
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

Caratteristiche speciali delle autorizzazioni di Protezione tramite password

Le autorizzazioni di protezione tramite password hanno alcuni aspetti e limitazioni importanti da tenere in considerazione.


Impostazioni 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 KLAdmin 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 KLAdmin di disabilitare i componenti della protezione, [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 consentite, 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 nelle unità criptate

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.

Visualizzazione dei rapporti

Non sono presenti considerazioni o limitazioni speciali.

Ripristina da Backup

Non sono presenti considerazioni o limitazioni speciali.

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 \(MMC\)](#) ²

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Impostazioni generali** → **Interfaccia**.
6. Nel blocco **Protezione tramite password**, fare clic sul pulsante **Impostazioni**.
7. Viene visualizzata una finestra; in tale finestra, deselezionare la casella di controllo **Protezione tramite password**.
8. Salvare le modifiche.
9. Selezionare di nuovo la casella di controllo **Protezione tramite password**.
10. Fare clic su **OK**.
Viene verrà visualizzata la finestra Password amministratore.
11. Specificare la nuova password dell'account KLAdmin e confermarla.
12. Salvare le modifiche.

[Come reimpostare la password dell'account KLAdmin in Web Console e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Dispositivi gestiti**.
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**.
Verranno visualizzate le impostazioni locali dell'applicazione.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Passare a **Impostazioni generali** → **Interfaccia**.
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.

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.

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. 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](#).

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 di scansione](#).

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 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio, selezionare **Impostazioni generali** → **Esclusioni e tipi di oggetti rilevati**.
6. Nel blocco **Esclusioni dalla scansione e applicazioni attendibili**, fare clic sul pulsante **Impostazioni**.
7. Nella finestra visualizzata, selezionare la scheda **Esclusioni dalla scansione**.
Verrà visualizzata una finestra contenente un elenco di esclusioni.
8. 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.
9. Selezionare la casella di controllo **Consenti l'utilizzo delle applicazioni attendibili 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.
10. Fare clic su **Aggiungi**.
11. Per escludere un file o una cartella dalla scansione:
 - a. Nella sezione **Proprietà** selezionare la casella di controllo **File o cartella**.
 - b. Fare clic sul collegamento **seleziona file o 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**.
 - c. 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 **Sfoggia**.
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 **cartella**, ad eccezione della

cartella 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 Cartella con l'estensione TXT e un nome composto da tre caratteri.

d. Salvare le modifiche.

12. Per escludere dalla scansione oggetti con un nome specifico:

- Nella sezione **Proprietà** selezionare la casella di controllo **Nome oggetto**.
- Fare clic sul collegamento **inserire il nome dell'oggetto** nel blocco **Descrizione dell'esclusione dalla scansione (fare clic sui termini sottolineati per modificarli)** per aprire la finestra **Nome 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.

d. Salvare le modifiche.

13. Se si desidera escludere un singolo file dalle scansioni:

- Nella sezione **Proprietà** selezionare la casella di controllo **Hash dell'oggetto**.
- Fare clic sul collegamento della voce dell'hash dell'oggetto per aprire la finestra **Hash dell'oggetto**.
- Immettere l'hash del file o selezionare il file facendo clic sul pulsante **Sfoggia**.
Se il file viene modificato, verrà modificato anche l'hash del file. In tal caso, il file modificato non verrà aggiunto alle esclusioni.

d. Salvare le modifiche.

14. Se necessario, nel campo **Commento** immettere un breve commento dell'esclusione dalla scansione.

15. Specificare i componenti di Kaspersky Endpoint Security da cui verrà utilizzata l'esclusione dalla scansione:

- Fare clic sul collegamento **qualsiasi** nel blocco **Descrizione dell'esclusione dalla scansione (fare clic sui termini sottolineati per modificarli)** per attivare il collegamento **selezionare i componenti**.
- Fare clic sul collegamento **selezionare i componenti** per visualizzare la finestra **Componenti della protezione**.
- Selezionare le caselle di controllo accanto ai componenti a cui deve essere applicata l'esclusione dalla scansione.

d. Salvare le modifiche.

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.

16. È possibile utilizzare la casella di controllo per [interrompere un'esclusione](#) in qualsiasi momento.

17. Salvare le modifiche.

[Come creare un'esclusione dalla scansione in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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** → **Esclusioni e tipi di oggetti rilevati**.
5. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili**, fare clic sul collegamento **Esclusioni dalla scansione**.
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 applicazioni attendibili 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.
8. Fare clic sul pulsante **Aggiungi**.
9. Selezionare le modalità di aggiunta dell'esclusione: **File o cartella**, **Nome oggetto** o **Hash dell'oggetto**.
10. Se si desidera escludere un file o una cartella dalle scansioni, selezionare il file o la cartella facendo clic sul pulsante **Sfoggia**.
È inoltre possibile inserire manualmente il percorso. 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 cartella, ad eccezione della cartella 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 Cartella con l'estensione TXT e un nome composto da tre caratteri.
11. Se si desidera escludere un tipo specifico di oggetto dalle scansioni, nel campo **Nome 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 **Componenti della protezione** 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. È possibile utilizzare l'interruttore per [interrompere un'esclusione](#) in qualsiasi momento.

16. 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**.
4. Fare clic su **Aggiungi**.

5. Se si desidera escludere un file o una cartella dalle scansioni, selezionare il file o la cartella facendo clic sul pulsante **Sfoggia**.

È inoltre possibile inserire manualmente il percorso. 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 cartella, ad eccezione della cartella 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 Cartella con l'estensione TXT e un nome composto da tre caratteri.

6. Se si desidera escludere un tipo specifico di oggetto dalle scansioni, nel campo **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.

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.

È possibile utilizzare l'interruttore per [interrompere un'esclusione](#) in qualsiasi momento.

11. Salvare le modifiche.

Esempi di maschera del percorso:

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 nella cartella 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\.

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.

Abilitazione e disabilitazione di un'esclusione dalla scansione


Per abilitare o disabilitare un'esclusione dalla scansione:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Minacce ed esclusioni**.
3. Nella sezione **Esclusioni** fare clic sul collegamento **Gestisci esclusioni**.

4. Selezionare l'esclusione desiderata nell'elenco delle esclusioni dalla scansione.
5. Utilizzare l'interruttore accanto a un oggetto per includere o escludere questo oggetto dall'ambito della scansione.
6. Salvare le modifiche.

Selezione dei tipi di oggetti rilevabili

Per selezionare i tipi di oggetti rilevabili:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Minacce ed esclusioni**.
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:

- [Virus e worm](#) 

Sottocategoria: virus e worm (Viruses_and_Worms)

Livello di pericolosità: 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 sovrascrittura* 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 parassiti* 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 collegamento*, *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	Penetrano nei computer attraverso le Internet Relay Chat, sistemi utilizzati

Worm	di chat Internet	<p>per comunicare con altre persone in tempo reale via Internet.</p> <p>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.</p>
Net-Worm	Worm di rete	<p>Questi worm si propagano tramite le reti di computer.</p> <p>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.</p>
P2P-Worm	Worm di file sharing	<p>Si propagano attraverso le reti peer-to-peer di file sharing.</p> <p>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.</p> <p>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.</p>
Worm	Altri tipi di worm	<p>Gli altri tipi di worm includono:</p> <ul style="list-style-type: none"> • 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 pericolosità: 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: <ul style="list-style-type: none">• 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

		<p>specificati nei file del sistema operativo.</p> <p>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.</p>
Trojan-Downloader	Trojan downloader	<p>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.</p>
Trojan-Dropper	Trojan dropper	<p>Contengono altri programmi Trojan che copiano nel disco rigido e quindi installano nel computer.</p> <p>Gli intrusi possono utilizzare i Trojan dropper per:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>
Trojan-Proxy	Trojan proxy	<p>Consentono all'intruso di accedere in modo anonimo alle pagine Web utilizzando il computer dell'utente e vengono spesso utilizzati per inviare posta spam.</p>
Trojan-PSW	Password-stealing-ware	<p>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.</p> <p>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).</p>
Trojan-Spy	Programmi Trojan per lo spionaggio dell'utente	<p>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.</p>

Trojan-DDoS	Programmi Trojan per l'esecuzione di attacchi di rete	<p>Invidano 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.</p> <p>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.</p>
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	Invisano 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 <i>exploit</i> 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	Invisano 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.
Spoofers	Strumenti di spoofing	Inviano messaggi e richieste di rete con l'indirizzo di un mittente fittizio. Gli spoofers 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 nascondere 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 pericolosità: 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 legale utilizzabile da utenti 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.
Dialer	Auto-Dialer	Questi programmi sono in grado di stabilire connessioni telefoniche nascoste tramite un modem.
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	Inviando 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.

- [Rileva altro software utilizzabile da intrusi per danneggiare il computer o i dati personali](#) 

Sottocategoria: software legale utilizzabile da utenti 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.
Dialer	Auto-Dialer	Questi programmi sono in grado di stabilire connessioni telefoniche nascoste tramite un modem.
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	<p>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.</p> <p>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.</p>
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	Invisano 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](#) 

Kaspersky Endpoint Security esamina gli oggetti compressi e il modulo dell'utilità di decompressione contenuti negli archivi autoestraenti.

Per nascondere i programmi pericolosi ai software anti-virus, gli hacker li comprimono utilizzando appositi programmi di compressione o creano file con compressione multipla.

Gli analisti anti-virus di Kaspersky hanno identificato i programmi di compressione più diffusi tra gli hacker.

Se Kaspersky Endpoint Security rileva un programma di compressione di questo tipo in un file, è probabile che il file contenga un'applicazione dannosa o che potrebbe essere utilizzata da utenti malintenzionati per danneggiare il computer o i dati personali.

Kaspersky Endpoint Security identifica i seguenti tipi di programmi:

- *File compressi potenzialmente pericolosi* – utilizzati per la compressione di malware, come virus, worm e programmi Trojan.
- *File con compressione multipla* (livello di pericolosità medio) – oggetti compressi tre volte con uno o più programmi di compressione.

- [Oggetti con compressione multipla](#) 

Kaspersky Endpoint Security esamina gli oggetti compressi e il modulo dell'utilità di decompressione contenuti negli archivi autoestraenti.

Per nascondere i programmi pericolosi ai software anti-virus, gli hacker li comprimono utilizzando appositi programmi di compressione o creano file con compressione multipla.

Gli analisti anti-virus di Kaspersky hanno identificato i programmi di compressione più diffusi tra gli hacker.

Se Kaspersky Endpoint Security rileva un programma di compressione di questo tipo in un file, è probabile che il file contenga un'applicazione dannosa o che potrebbe essere utilizzata da utenti malintenzionati per danneggiare il computer o i dati personali.

Kaspersky Endpoint Security identifica i seguenti tipi di programmi:

- *File compressi potenzialmente pericolosi* – utilizzati per la compressione di malware, come virus, worm e programmi Trojan.
- *File con compressione multipla* (livello di pericolosità medio) – oggetti compressi tre volte con uno o più programmi di compressione.

4. Salvare le modifiche.

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 esamina 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. Tuttavia, un'applicazione che è stata aggiunta all'elenco delle applicazioni attendibili viene esclusa dalle scansioni da parte di Kaspersky Endpoint Security.

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. Durante la scansione verranno ignorati gli oggetti utilizzati da questa applicazione.

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.

L'esclusione dalla scansione delle applicazioni attendibili consente di evitare problemi di compatibilità tra Kaspersky Endpoint Security e altri programmi, ad esempio il problema della doppia scansione del traffico di rete di un computer di terze parti da parte di Kaspersky Endpoint Security e di un'altra applicazione anti-virus, nonché di migliorare le prestazioni del computer, aspetto di fondamentale importanza quando si utilizzano applicazioni server.

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 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Impostazioni generali** → **Esclusioni**.
6. Nel blocco **Esclusioni dalla scansione e applicazioni attendibili**, fare clic sul pulsante **Impostazioni**.
7. Nella finestra visualizzata, selezionare la scheda **Applicazioni attendibili**.
Verrà visualizzata una finestra contenente un elenco di applicazioni attendibili.
8. 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.
9. 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.
10. Fare clic su **Aggiungi**.
11. Nella finestra visualizzata, immettere il percorso 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 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.
12. Configurare le impostazioni avanzate per l'applicazione attendibile (vedere la tabella seguente).
13. È possibile utilizzare la casella di controllo per [escludere un'applicazione dall'area attendibile](#) in qualsiasi momento.
14. Salvare le modifiche.



1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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. Accedere a **Impostazioni generali** → **Esclusioni**.
5. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Applicazioni attendibili**.
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.
8. Fare clic su **Aggiungi**.
9. Nella finestra visualizzata, immettere il percorso 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 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. È possibile utilizzare la casella di controllo per [escludere un'applicazione dall'area attendibile](#) in qualsiasi momento.
12. Salvare le modifiche.

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Minacce ed esclusioni**.
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 attendibile.

È inoltre possibile inserire manualmente il percorso. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri  e  durante l'immissione di una maschera.

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 (vedere la tabella seguente).
7. È possibile utilizzare l'interruttore per [escludere un'applicazione dall'area attendibile](#) in qualsiasi momento.
8. Salvare le modifiche.


Impostazioni delle applicazioni attendibili

Parametro	Descrizione
Non esaminare i file prima dell'apertura	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 l'attività dell'applicazione	Kaspersky Endpoint Security non monitorerà l'attività file e rete dell'applicazione nel sistema operativo. Le attività dell'applicazione vengono monitorate dai seguenti componenti: Rilevamento del Comportamento , Prevenzione Exploit , Prevenzione Intrusioni Host , Motore di Remediation e Firewall .
Non ereditare le restrizioni dal processo principale (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 l'attività	Kaspersky Endpoint Security non monitorerà l'attività file o l'attività di rete delle applicazioni avviate dall'applicazione.

dell'applicazione secondaria	
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 di protezione AMSI	Kaspersky Endpoint Security non monitorerà le richieste dell'applicazione attendibile per gli oggetti che verranno esaminati dal componente Protezione AMSI .
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.
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: <ul style="list-style-type: none"> • Lo stato Attivo indica che l'applicazione si trova nell'area attendibile. • Lo stato Inattivo indica che l'applicazione è esclusa dall'area attendibile.

Abilitazione e disabilitazione delle regole dell'area attendibile per un'applicazione nell'elenco delle applicazioni attendibili


Per abilitare o disabilitare l'azione delle regole dell'area attendibile applicata a un'applicazione nell'elenco delle applicazioni attendibili:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Minacce ed esclusioni**.
3. Nella sezione **Esclusioni**, fare clic sul collegamento **Specifica applicazioni attendibili**.
4. Nell'elenco delle applicazioni attendibili selezionare l'applicazione attendibile desiderata.
5. Utilizzare l'interruttore nella colonna **Stato** per includere o escludere un'applicazione attendibile dall'ambito della scansione.
6. Salvare le modifiche.

Utilizzo dell'archivio di certificati di sistema attendibili

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*.

Per iniziare a utilizzare l'archivio di certificati di sistema attendibili:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Minacce ed esclusioni**.
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.

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\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, selezionare **Impostazioni generali** → **Rapporti e archivi**.
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, selezionare **Impostazioni generali** → **Rapporti e archivi**.
3. Se si desidera limitare la dimensione di Backup, selezionare la casella di controllo **Limita la dimensione del Backup a N MB** nella sezione **Backup**. Specificare la dimensione massima di Backup.
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 *Infetto*, 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 disinfettare al riavvio del computer* non possono essere ripristinati. Dopo il riavvio del computer lo stato del file diventerà *Disinfettato* o *Eliminato*. 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 Microsoft Windows 8 (per informazioni dettagliate su come ripristinare un'applicazione Windows Store, consultare i *file della Guida di Microsoft Windows 8*).

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 dell'applicazione principale, 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.

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 dell'applicazione principale, 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.

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 **Impostazioni di notifica**.

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 Applicazione.

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 **Impostazioni di notifica**.

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 **Impostazioni delle 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.


Kaspersky Endpoint Security supporta solo l'autenticazione SMTP di base. Le impostazioni dell'applicazione non consentono di configurare l'uso di TLS. È possibile configurare le notifiche e-mail nelle proprietà di Kaspersky Security Center Administration Server. Kaspersky Security Center supporta l'uso di TLS per il server SMTP.



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 i 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\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.

 **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**.

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, selezionare **Impostazioni generali** → **Rapporti e archivi**.


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, selezionare **Impostazioni generali** → **Rapporti e archivi**.
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 soprattutto 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**.
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, selezionare **Impostazioni generali** → **Rapporti e archivi**.
3. Nella sezione **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).


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: <ul style="list-style-type: none">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 applicazioni di amministrazione remota, ad esempio TeamViewer o RemotelyAnywhere, di accedere a Kaspersky Endpoint Security.	✓	– (ad eccezione di Windows 7)

Abilitazione e disabilitazione di Auto-difesa

Il meccanismo Auto-Difesa di Kaspersky Endpoint Security è abilitato per impostazione predefinita.

Per abilitare o disabilitare Auto-Difesa:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
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.

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.

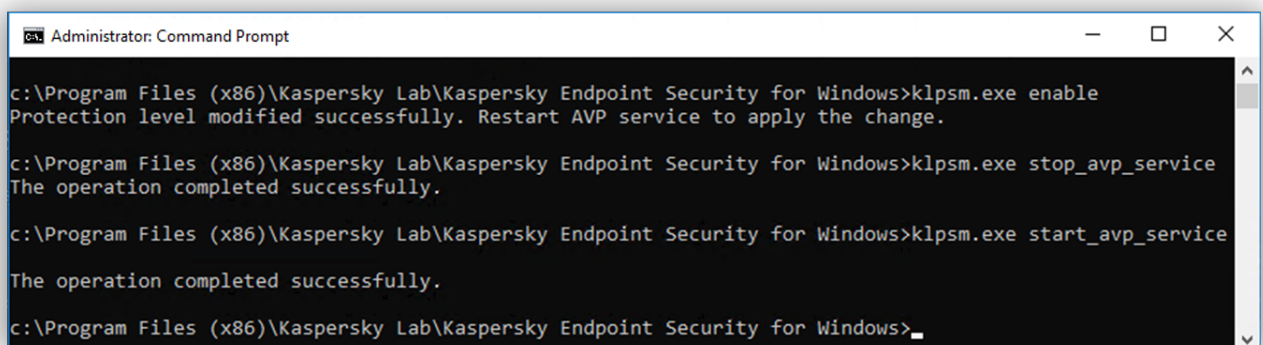
3. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

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.](#)



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```

Abilitazione del supporto della tecnologia AM-PPL


Abilitazione e disabilitazione della difesa gestione esterna

La difesa dalla gestione esterna impedisce alle applicazioni di amministrazione remota, ad esempio TeamViewer o RemotelyAnywhere, di accedere a Kaspersky Endpoint Security. Questa tecnologia include le seguenti funzionalità di difesa dalla gestione esterna:

- Protezione contro la modifica delle impostazioni di Kaspersky Endpoint Security.
- Protezione dei servizi Kaspersky Endpoint Security (ad esempio il servizio avp).
- Protezione dei processi delle applicazioni.

La protezione contro la gestione esterna è disponibile solo per i computer in cui vengono eseguiti sistemi operativi a 32 bit, ad eccezione di Windows 7. Per Windows 7, la tecnologia è disponibile per sistemi operativi a 32 bit e a 64 bit.

Per abilitare o disabilitare la protezione dalla gestione esterna:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
3. Utilizzare la casella di controllo **Consenti la gestione delle impostazioni di Kaspersky Endpoint Security tramite le applicazioni di controllo remoto** per abilitare o disabilitare la difesa dalla gestione esterna.
Se la casella di controllo è selezionata, è possibile utilizzare applicazioni di amministrazione remota per configurare Kaspersky Endpoint Security e gestirne servizi e processi.
Se la casella di controllo è deselezionata, la difesa dalla gestione esterna impedisce alle applicazioni di amministrazione remota di accedere a Kaspersky Endpoint Security. È possibile consentire la configurazione di Kaspersky Endpoint Security utilizzando applicazioni di amministrazione remota specifiche. A tale scopo, è necessario [aggiungere l'applicazione di amministrazione remota all'elenco di applicazioni attendibili](#). In questo caso, la difesa dall'amministrazione remota impedirà comunque all'applicazione di amministrazione remota di accedere ai servizi e ai processi di Kaspersky Endpoint Security.
4. Utilizzare la casella di controllo **Abilita gestione esterna dei servizi di sistema** per abilitare o disabilitare la protezione dei servizi di Kaspersky Endpoint Security dalla gestione esterna.

Per chiudere l'applicazione dalla riga di comando, disabilitare la protezione dei servizi di Kaspersky Endpoint Security dalla gestione esterna.


5. Salvare le modifiche.

Di conseguenza, quando la difesa dalla gestione esterna è abilitata, Kaspersky Endpoint Security impedisce al puntatore del mouse di accedere alla finestra dell'applicazione. Quando un utente remoto tenta di chiudere un servizio dell'applicazione, viene visualizzata una finestra di sistema con un messaggio di errore.

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** → **Minacce ed esclusioni**.
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 inserire manualmente il percorso. Kaspersky Endpoint Security supporta le variabili di ambiente e i caratteri e durante l'immissione di una maschera.
6. Selezionare la casella di controllo **Non monitorare l'attività dell'applicazione**.
7. Salvare le modifiche.

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 di aggiornamento;
- 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 da parte di Kaspersky Endpoint Security durante la scansione del computer può aumentare il carico sui sottosistemi della CPU e del disco rigido, nonché influenzare le prestazioni di altre applicazioni. 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 attiva per i server e avviare un'attività di gruppo *Scansione virus* in un momento appropriato per gli utenti del server.

Abilitazione o disabilitazione della modalità di risparmio energetico

Per abilitare o disabilitare la modalità di risparmio energetico:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
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.

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:


- Attività di aggiornamento;
- Attività Scansione completa;
- Attività Scansione delle aree critiche;
- Attività Scansione personalizzata;
- Attività Controllo integrità.

4. Salvare le modifiche.

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 concedere risorse ad altre applicazioni.

Per abilitare o disabilitare la concessione di risorse ad altre applicazioni:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
3. Nel blocco **Prestazioni**, utilizzare la casella di controllo **Concedi risorse alle 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.

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 virus sulle workstation

Si consiglia di abilitare [Scansione in background](#) per la scansione virus delle workstation. *Scansione in background* è una modalità di scansione di Kaspersky Endpoint Security che non visualizza 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 virus 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 virus* in base ai seguenti suggerimenti:

1. [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 alla fine della giornata, è possibile configurare l'attività di scansione come segue:

- Abilitare la funzionalità di riattivazione LAN. La funzionalità di riattivazione LAN consente di accendere il computer da remoto inviando un segnale speciale sulla rete locale. Per utilizzare questa funzionalità, è necessario abilitare la riattivazione LAN nelle impostazioni BIOS. È inoltre possibile spegnere automaticamente il computer al termine della scansione.
- Disabilitare la funzionalità "Esegui attività non effettuate". Kaspersky Endpoint Security ignorerà le attività non effettuate quando l'utente accende il computer. L'esecuzione di attività dopo l'accensione del computer può causare disagi all'utente perché la scansione richiede una notevole quantità di risorse.

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.

2. [Definire un ambito di scansione.](#)

Selezionare i seguenti oggetti da esaminare:

- Memoria del kernel
- Processi in esecuzione e oggetti di avvio
- Settori di avvio
- Unità di sistema (%systemdrive%).

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 dalla scansione 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.](#)

Scansione virus nei server

Configurare l'attività *Scansione virus* in base ai seguenti suggerimenti:

1. [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.

2. [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 dalla scansione 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.

3. [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.](#)

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 l'utente sta partecipando a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla categoria e sulla reputazione dei file esaminati, nonché informazioni sulla reputazione degli indirizzi Web esaminati.

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 KSN privato.

KSN Privato 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 Security Network e ad altri dati statistici senza inviare dati a KSN 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.

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 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 [Gestire gli account per l'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 archivarli 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.

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 connesse tramite bus: SCSI, ATA, IEEE1394, 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 Think Center 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 100
- 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 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 il 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 per l'Agente di Autenticazione](#) è destinata alla configurazione delle impostazioni di autenticazione dell'utente. 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
6. 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.

7. 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](#).

8. Configurare le opzioni avanzate di Criptaggio disco Kaspersky (vedere la tabella seguente).
9. Salvare le modifiche.

[Come eseguire Criptaggio disco Kaspersky tramite Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.

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. Accedere a **Criptaggio dei dati** → **Criptaggio dell'intero disco**.

5. In **Gestire il criptaggio**, selezionare **Criptaggio disco Kaspersky**.

6. Fare clic sul collegamento **Criptaggio disco Kaspersky**.

Viene aperta la finestra delle impostazioni di Criptaggio disco Kaspersky.

La tecnologia Criptaggio disco Kaspersky non può essere utilizzata se il computer dispone di dischi rigidi criptati tramite BitLocker.

7. 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.

Se è necessario escludere alcuni dischi rigidi dal criptaggio, [creare un elenco di tali dischi rigidi](#).

8. Configurare le opzioni avanzate di Criptaggio disco Kaspersky (vedere la tabella seguente).

9. 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](#).

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 gli 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	Se questa casella di controllo è selezionata, l'applicazione controlla le informazioni sugli

<p>automaticamente gli account dell'Agente di Autenticazione per tutti gli utenti di questo computer al momento dell'accesso</p>	<p>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 <i>Gestire gli account per l'Agente di Autenticazione</i> per i computer con unità già criptate.</p>
<p>Salva il nome utente immesso nell'Agente di Autenticazione</p>	<p>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.</p>
<p>Cripta solo lo spazio su disco utilizzato (riduce i tempi di criptaggio)</p>	<p>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.</p> <div data-bbox="427 730 1493 954" style="border: 1px solid black; padding: 10px;"> <p>L'abilitazione o la disabilitazione della funzionalità Cripta solo lo spazio su disco utilizzato (Windows 8 e versioni successive) 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.</p> </div> <p>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.</p> <p>Se la casella di controllo è deselezionata, viene criptato l'intero disco rigido, inclusi i frammenti residui dei file precedentemente eliminati e modificati.</p> <div data-bbox="427 1227 1493 1417" style="border: 1px solid black; padding: 10px;"> <p>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.</p> </div> <p>Questa casella di controllo è deselezionata per impostazione predefinita.</p>
<p>Usa Legacy USB Support (opzione non consigliata)</p>	<p>Questa casella di controllo consente di abilitare o disabilitare la funzione Legacy USB Support. <i>Legacy USB Support</i> 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.</p> <p>Se la casella di controllo è selezionata, il supporto dei dispositivi USB durante l'avvio iniziale del computer sarà abilitato.</p> <div data-bbox="427 1839 1493 2029" style="border: 1px solid black; padding: 10px;"> <p>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.</p> </div>

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
6. 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.

7. Per aggiungere dischi rigidi all'elenco dei dischi rigidi esclusi dal criptaggio:
 - a. Fare clic su **Aggiungi**.
 - b. Viene verrà visualizzata una finestra; in tale finestra, modificare le impostazioni **Nome dispositivo**, **Nome computer**, **Tipo di disco**, **Criptaggio disco Kaspersky**.
 - c. Fare clic sul pulsante **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**.

8. 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.



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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
6. 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**.
7. 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 collegamento **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.
8. Per importare l'elenco delle regole:
 - 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.
9. Salvare le modifiche.

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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. Accedere a **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
5. Selezionare la tecnologia **Criptaggio disco Kaspersky** e seguire il collegamento per configurare le impostazioni.
Vengono aperte le impostazioni di criptaggio.
6. Fare clic sul collegamento **Esclusioni**.
7. Per esportare l'elenco delle regole:
 - a. Selezionare le esclusioni che si desidera esportare.
 - b. Fare clic su **Esporta**.
 - c. Confermare di voler esportare solo le esclusioni selezionate o esportare l'intero elenco di esclusioni.
 - d. 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.
 - e. Salvare il file.
Kaspersky Endpoint Security esporta l'intero elenco di esclusioni nel file XML.
8. Per importare l'elenco delle regole:
 - 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.
9. 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.

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.

La tecnologia Single Sign-On è incompatibile con i fornitori di credenziali dell'account di terze parti.

Come abilitare l'uso della tecnologia Single Sign-On 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Impostazioni di criptaggio generali**.
6. Nella sezione **Impostazioni password** fare clic sul pulsante **Impostazioni**.
7. Nella finestra visualizzata, nella scheda **Agente di Autenticazione** selezionare la casella di controllo **Utilizza la tecnologia SSO (Single Sign-On)**.
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.

Come abilitare l'utilizzo di Single Sign-On in Web Console

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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. Accedere a **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
5. Selezionare la tecnologia **Criptaggio disco Kaspersky** e seguire il collegamento per configurare le impostazioni.
Vengono aperte le impostazioni di criptaggio.
6. Nel blocco **Impostazioni password**, selezionare la casella di controllo **Utilizza la tecnologia SSO (Single Sign-On)**.
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.

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. Successivamente, Kaspersky Endpoint Security sostituisce la password dell'account Agente di Autenticazione con la password dell'account Windows.

Gestione degli account per l'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 gli account per l'Agente di Autenticazione* è destinata alla configurazione delle impostazioni di autenticazione dell'utente. 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 gli account per l'Agente di Autenticazione*. È inoltre impossibile interrompere forzatamente un'attività.

[Come creare l'attività Gestisci gli account per l'Agente di Autenticazione in Administration Console \(MMC\)](#) 

1. In Administration Console accedere alla cartella **Administration Server** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)** → **Gestisci gli account per l'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 per l'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

Chiusura della 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.

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

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

2. Nell'elenco a discesa **Tipo di attività** selezionare **Gestisci gli account per l'Agente di Autenticazione**.

3. Nel campo **Nome attività** immettere una breve descrizione, ad esempio *Account amministratore*.

4. Nel blocco **Selezionare i dispositivi a cui assegnare l'attività**, selezionare l'ambito dell'attività.

Passaggio 2. Gestione degli account per l'agente di autenticazione

Generare un elenco di comandi di gestione degli account per l'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

Chiusura della 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 gli account per l'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 gli account per l'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 gli account per l'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 *Gestire gli account per l'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.

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

Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Gestisci gli account per l'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 dell'Agente di Autenticazione fare clic sul pulsante **Aggiungi**.

Viene avviata la procedura guidata per la gestione degli account dell'Agente di Autenticazione.

5. Selezionare il tipo di comando **Aggiungi**.

6. 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 (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.

7. Configurare le impostazioni degli account dell'Agente di Autenticazione.

- **Crea un nuovo account per l'Agente di Autenticazione in sostituzione dell'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 l'autenticazione basata sulla 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 l'autenticazione basata sul 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**.

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 gli account per l'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 gli account per l'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 gli account per l'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 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 **Dispositivi** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sull'attività **Gestisci gli account per l'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 dell'Agente di Autenticazione fare clic sul pulsante **Aggiungi**.

Viene avviata la procedura guidata per la gestione degli account dell'Agente di Autenticazione.

5. Selezionare il tipo di comando **Modifica**.

6. 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 (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.

7. Selezionare le caselle di controllo accanto alle impostazioni che si desidera modificare.

8. Configurare le impostazioni degli account dell'Agente di Autenticazione.

- **Crea un nuovo account per l'Agente di Autenticazione in sostituzione dell'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 l'autenticazione basata sulla 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 l'autenticazione basata sul 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.

9. Salvare le modifiche.

10. 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 gli account per l'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 gli account per l'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 gli account per l'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 **Dispositivi** → **Attività**.
Viene aperto l'elenco delle attività.
2. Fare clic sull'attività **Gestisci gli account per l'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 dell'Agente di Autenticazione fare clic sul pulsante **Aggiungi**.
Viene avviata la procedura guidata per la gestione degli account dell'Agente di Autenticazione.
5. Selezionare il tipo di comando **Elimina**.
6. Selezionare un account utente. È possibile selezionare un account dall'elenco degli account di dominio o inserire manualmente il nome dell'account.
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, 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 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 **Attività**.
6. Nell'elenco delle attività, selezionare **Gestisci account per l'Agente di Autenticazione** e aprire le proprietà dell'attività facendo doppio clic.
7. 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.

[Come visualizzare un elenco degli account dell'Agente di Autenticazione tramite Web Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Dispositivi gestiti**.
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. Nell'elenco delle attività, selezionare **Gestisci gli account per l'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 gli account per l'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 terze parti 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 attiva che consente il criptaggio dei dati.

Per decriptare i dischi rigidi:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
6. Nell'elenco a discesa **Tecnologia di criptaggio** selezionare la tecnologia con cui sono stati criptati i dischi rigidi.
7. 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.

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](#).

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.

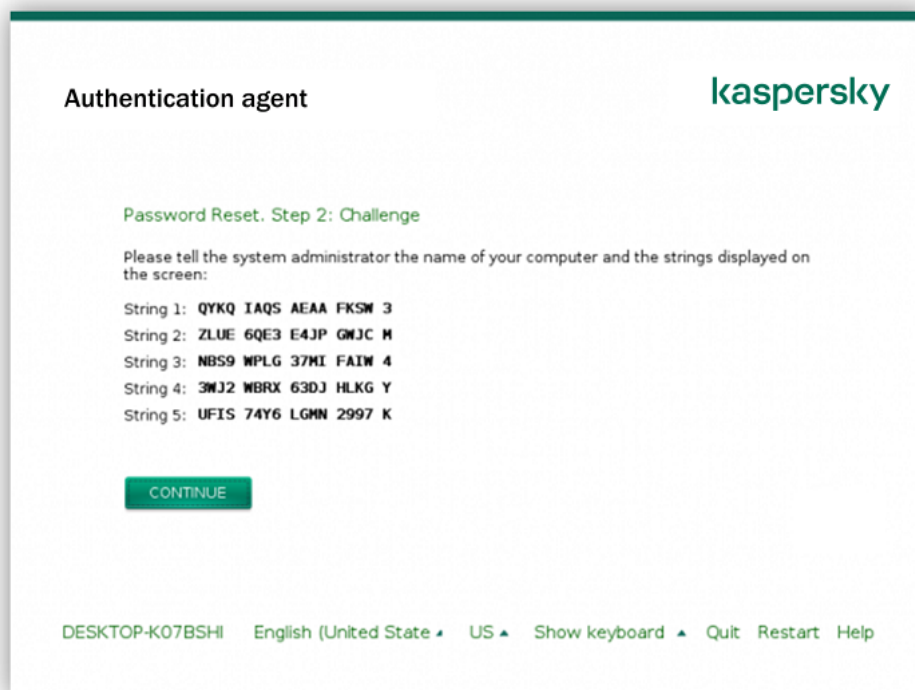
Ripristino dell'accesso a un'unità protetta dalla tecnologia Criptaggio disco Kaspersky

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 **Password dimenticata** 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 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. 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.
5. Nel menu di scelta rapida selezionare **Concedi l'accesso in modalità offline**.
6. Nella finestra visualizzata selezionare la scheda **Agente di Autenticazione**.
7. 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: *Criptaggio avanzato (AES256)* o *Criptaggio superficiale (AES56)*. La libreria di criptaggio AES viene installata insieme all'applicazione.
8. 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.
9. Nell'elenco a discesa **Disco rigido** selezionare il disco rigido criptato per cui è necessario ripristinare l'accesso.
10. 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.

[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, selezionare **Dispositivi** → **Dispositivi gestiti**.
2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso all'unità.
3. Fare clic sul pulsante **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 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. 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.
5. Nel menu di scelta rapida selezionare **Concedi l'accesso in modalità offline**.
6. Nella finestra visualizzata selezionare la scheda **Criptaggio dei dati**.
7. Nella scheda **Criptaggio dei dati** fare clic sul pulsante **Sfoglia**.
8. 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.

[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, selezionare **Dispositivi** → **Dispositivi gestiti**.
2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso ai dati.
3. Fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.
4. Selezionare la sezione **Criptaggio dei dati**.
5. Fare clic sul pulsante **Selezionare un 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 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 **Attività**.
6. Nell'elenco delle attività, selezionare **Gestisci account per l'Agente di Autenticazione** e aprire le proprietà dell'attività facendo doppio clic.
7. Nella finestra delle proprietà dell'attività, selezionare la sezione **Impostazioni**.
8. Nell'elenco degli account, selezionare l'account di servizio di Agente di Autenticazione (ad esempio, WIN10-USER\ServiceAccount).
9. Nell'elenco a discesa **Azione**, selezionare **Visualizza account**.
10. Nelle proprietà dell'account, selezionare la casella di controllo **Mostra password originale**.
11. 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, selezionare **Dispositivi** → **Dispositivi gestiti**.
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. Nell'elenco delle attività, selezionare **Gestisci gli account per l'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 originale**.
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.

Per informazioni dettagliate sull'aggiornamento sicuro del sistema operativo, consultare la [Knowledge Base dell'Assistenza tecnica](#).

L'aggiornamento automatico del sistema operativo è disponibile alle seguenti condizioni:

1. Il sistema operativo viene aggiornato tramite WSUS (Windows Server Update Services).
2. Nel computer è installato Windows 10 1607 (RS1) o versione successiva.
3. Kaspersky Endpoint Security 11.2.0 o versioni successive è installato nel computer.

Se tutte le condizioni sono soddisfatte, è possibile aggiornare il sistema operativo come di consueto.

Se si utilizza la tecnologia Criptaggio disco Kaspersky (FDE) e nel computer è installato Kaspersky Endpoint Security for Windows versione 11.1.0 o 11.1.1, non è necessario decriptare i dischi rigidi per aggiornare Windows 10.

Per aggiornare il sistema operativo è necessario eseguire le seguenti operazioni:

1. Prima di aggiornare il sistema, copiare i driver denominati cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf e klfdefsf.sys in una cartella locale. Ad esempio C:\fde_drivers.
2. Eseguire l'installazione dell'aggiornamento di sistema con l'interruttore `/ReflectDrivers` e specificare la cartella contenente i driver salvati:

```
setup.exe /ReflectDrivers C:\fde_drivers
```

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 11.9.0.

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.](#)

Selezione del livello di traccia per l'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 selezionare il livello di traccia per l'agente di autenticazione:

1. 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.
2. Selezionare il livello di traccia nella finestra delle impostazioni dell'agente di autenticazione:
 - **Disable debug logging (default).** Se questa opzione è selezionata, l'applicazione non registra le informazioni sugli eventi dell'agente di autenticazione nel file di traccia.
 - **Enable debug logging.** 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.
 - **Enable verbose logging.** 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 **Enable debug logging**. Un livello elevato di dettaglio delle voci può rallentare l'avvio dell'agente di autenticazione e del sistema operativo.

- **Enable debug logging and select serial port.** 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.

- **Enable verbose debug logging and select serial port.** 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 **Enable debug logging and select serial port**. Un livello elevato di dettaglio delle voci può rallentare l'avvio dell'agente di autenticazione e del sistema operativo.

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.

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Impostazioni di criptaggio generali**.
6. Nel blocco **Modelli**, fare clic sul pulsante **Guida**.
7. 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.
8. 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.

9. 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 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 Kaspersky Security Center. 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](#).

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 di un'unità, BitLocker crea una chiave master. Kaspersky Endpoint Security invia la chiave master a Kaspersky Security Center in modo da poter [ripristinare l'accesso al disco](#), se ad esempio un utente ha dimenticato la password.

Se un utente cripta un disco utilizzando BitLocker, Kaspersky Endpoint Security invierà [informazioni sul criptaggio del disco a Kaspersky Security Center](#). Tuttavia, Kaspersky Endpoint Security non invierà la chiave master a Kaspersky Security Center, pertanto sarà impossibile ripristinare l'accesso al disco utilizzando Kaspersky Security Center. Per il corretto funzionamento di BitLocker con Kaspersky Security Center, [decriptare l'unità](#) e [criptarla nuovamente](#) utilizzando un criterio. È possibile decriptare un'unità in locale o utilizzando un criterio.

Dopo il criptaggio del disco rigido di sistema, l'utente deve eseguire l'autenticazione BitLocker per avviare il sistema operativo. Dopo la procedura di autenticazione, BitLocker consentirà agli utenti di accedere. BitLocker non supporta la tecnologia SSO (Single Sign-On).

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
6. Nell'elenco a discesa **Tecnologia di criptaggio** selezionare **Crittografia unità BitLocker**.
7. Nell'elenco a discesa **Modalità di criptaggio**, selezionare la voce **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.

8. Configurare le opzioni avanzate di Crittografia unità BitLocker (vedere la tabella seguente).
9. Salvare le modifiche.

Come eseguire Crittografia unità BitLocker tramite Web Console e Cloud Console

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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. Accedere a **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
5. Nel blocco **Gestire il criptaggio**, selezionare **Crittografia unità BitLocker**.
6. Fare clic sul collegamento **Crittografia unità BitLocker**.
Viene aperta la finestra delle impostazioni di Crittografia unità BitLocker.
7. 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.

8. Configurare le opzioni avanzate di Crittografia unità BitLocker (vedere la tabella seguente).
9. 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](#).

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
<p>Consenti l'utilizzo dell'autenticazione BitLocker che richiede l'input da tastiera prima dell'avvio nei tablet</p>	<p>Questa casella di controllo consente di abilitare o disabilitare l'utilizzo dell'autenticazione tramite 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).</p> <div data-bbox="440 369 1493 526" style="border: 1px solid black; padding: 5px;"> <p>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.</p> </div> <p>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.</p> <p>Se la casella di controllo è deselezionata, Crittografia unità BitLocker non è disponibile nei tablet.</p>
<p>Usa criptaggio hardware (sistema operativo Windows 8 e versioni successive)</p>	<p>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.</p>
<p>Cripta solo lo spazio su disco utilizzato (Windows 8 e versioni successive)</p>	<p>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.</p> <div data-bbox="440 1200 1493 1429" style="border: 1px solid black; padding: 5px;"> <p>L'abilitazione o la disabilitazione della funzionalità Cripta solo lo spazio su disco utilizzato (Windows 8 e versioni successive) dopo l'avvio del criptaggio non comporta la modifica di questa impostazione finché i dischi rigidi non vengono decrittati. È necessario selezionare o deselezionare la casella di controllo prima di avviare il criptaggio.</p> </div> <p>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.</p> <p>Se la casella di controllo è deselezionata, viene criptato l'intero disco rigido, inclusi i frammenti residui dei file precedentemente eliminati e modificati.</p> <div data-bbox="440 1693 1493 1888" style="border: 1px solid black; padding: 5px;"> <p>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.</p> </div> <p>Questa casella di controllo è deselezionata per impostazione predefinita.</p>
<p>Impostazioni di autenticazione</p>	<p>Usa password (sistema operativo Windows 8 e versioni successive)</p> <p>Se questa opzione è selezionata, Kaspersky Endpoint Security richiede una password quando si tenta di accedere a un'unità crittografata.</p>

Questa opzione può essere selezionata quando non viene utilizzato un Trusted Platform Module (TPM).

Usa 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 decryptate 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.
È possibile consentire all'utente di utilizzare il PIN avanzato. *PIN avanzato* consente di utilizzare altri caratteri oltre a quelli numerici: lettere latine maiuscole e minuscole, caratteri speciali e spazi.
- **Usa Trusted Platform Module (TPM). Se non è disponibile, usa la password.** Se la casella di controllo 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.

Decriptaggio di un disco rigido protetto da BitLocker

Gli utenti possono decryptare 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
6. Nell'elenco a discesa **Tecnologia di criptaggio** selezionare **Crittografia unità BitLocker**.
7. Nell'elenco a discesa **Modalità di criptaggio**, selezionare la voce **Decripta tutti i dischi rigidi**.
8. Salvare le modifiche.

[Come decriptare un disco rigido criptato con BitLocker tramite Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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. Accedere a **Criptaggio dei dati** → **Criptaggio dell'intero disco**.
5. Selezionare la tecnologia **Crittografia unità BitLocker** e seguire il collegamento per configurare le impostazioni.
Vengono aperte le impostazioni di criptaggio.
6. Nell'elenco a discesa **Modalità di criptaggio** selezionare **Decripta tutti i dischi rigidi**.
7. Fare clic su **OK**.

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](#).

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:

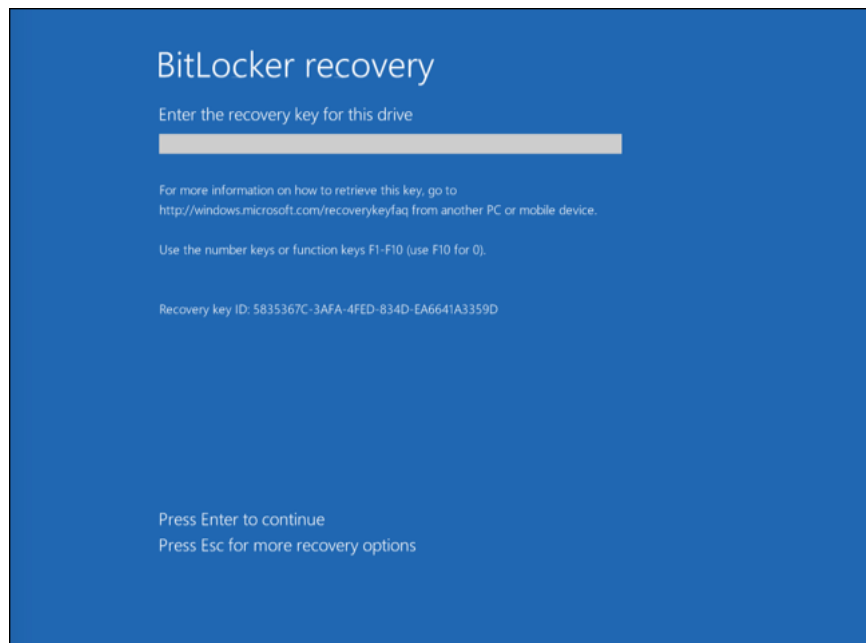
1. L'utente comunica all'amministratore l'ID della chiave di ripristino (vedere la figura seguente).
2. L'amministratore verifica l'ID della chiave di ripristino nelle proprietà del computer in Kaspersky Security Center. L'ID fornito dall'utente deve corrispondere all'ID visualizzato nelle proprietà 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.

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 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. 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.
5. Nel menu di scelta rapida selezionare **Concedi l'accesso in modalità offline**.
6. Nella finestra visualizzata selezionare la scheda **Accesso all'unità di sistema protetta da BitLocker**.
7. 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.

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, selezionare **Dispositivi** → **Dispositivi gestiti**.
2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso all'unità.
3. Fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.
4. Nella finestra visualizzata, selezionare la scheda **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 sul pulsante **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 master 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 \(MMC\)](#) ²

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 for Windows**.
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**.

[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, selezionare **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 sul pulsante **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 sul pulsante **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 \(MMC\)](#),²

1. In Administration Console accedere alla cartella **Administration Server** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)** → **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

Chiusura della 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, selezionare **Dispositivi** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

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 **Selezionare i 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

Chiusura della 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 nelle proprietà del computer in Kaspersky Security Center Console.

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 l'autenticazione ogni volta prima dell'avvio**.

Criptaggio a livello di file nelle unità locali del computer

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio a livello di file**.
6. Nell'elenco a discesa **Modalità di criptaggio**, selezionare **In base alle regole**.

7. 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.
- **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.

8. 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 creare le regole di accesso ai file criptati per le applicazioni:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio a livello di file**.
6. 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.

7. Nella parte destra della finestra selezionare la scheda **Regole per le applicazioni**.
8. 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 sul pulsante **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**.

9. 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**.

10. 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio a livello di file**.
6. 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.

7. Nella parte destra della finestra selezionare la scheda **Regole per le applicazioni**.
8. 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 sul pulsante **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**.

9. 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**.

10. Salvare le modifiche.

Generazione di una regola di decriptaggio

Per generare una regola di decriptaggio:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio a livello di file**.
6. Nell'elenco a discesa **Modalità di criptaggio**, selezionare **In base alle regole**.
7. 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.
8. 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Criptaggio a livello di file**.
6. Nella parte destra della finestra selezionare la scheda **Criptaggio**.
7. 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 **Rimuovi**.

I file e le cartelle rimossi dall'elenco di criptaggio vengono automaticamente aggiunti all'elenco di decriptaggio.

8. [Creare un elenco di decriptaggio dei file.](#)

9. 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio, selezionare **Criptaggio dei dati** → **Impostazioni di criptaggio generali**.
6. Nella sezione **Impostazioni password** fare clic sul pulsante **Impostazioni**.
7. Nella finestra visualizzata, selezionare la scheda **Pacchetti criptati**.
8. 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, selezionare **Dispositivi** → **Criteri e profili**.
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. Accedere a **Criptaggio dei dati** → **Criptaggio a livello di file**.
5. Nella sezione **Impostazioni password del pacchetto criptato** configurare i criteri di complessità della password richiesti durante la creazione di pacchetti criptati.

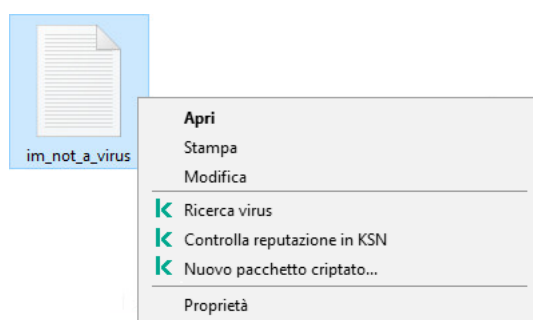
È possibile creare pacchetti criptati su computer in cui è installato Kaspersky Endpoint Security con Criptaggio a livello di file disponibile.

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. Dal menu di scelta rapida, selezionare **Nuovo pacchetto criptato** (vedere la figura di seguito).
3. Nella finestra visualizzata, selezionare una posizione su un'unità rimovibile in cui salvare il pacchetto criptato, quindi specificare il nome del pacchetto e fare clic sul pulsante **Salva**.
4. Nella finestra visualizzata, specificare la password e confermarla.
La password deve soddisfare i criteri di complessità specificati nel criterio.
5. Fare clic sul pulsante **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 - ).



Creazione di un pacchetto criptato

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.

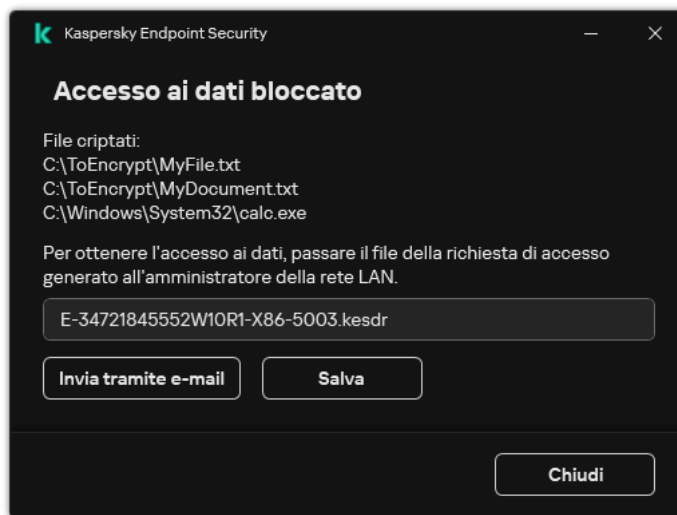
L'utente può utilizzare i file criptati nelle seguenti circostanze:

- 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 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. 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.
5. Nel menu di scelta rapida selezionare **Concedi l'accesso in modalità offline**.
6. Nella finestra visualizzata selezionare la scheda **Criptaggio dei dati**.
7. Nella scheda **Criptaggio dei dati** fare clic sul pulsante **Sfoglia**.
8. 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.

[Come ottenere un file della chiave di accesso ai dati criptati in Web Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Dispositivi gestiti**.
 2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso ai dati.
 3. Fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.
 4. Selezionare la sezione **Criptaggio dei dati**.
 5. Fare clic sul pulsante **Selezionare un 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra del criterio selezionare **Criptaggio dei dati** → **Impostazioni di criptaggio generali**.
6. Nel blocco **Modelli**, fare clic sul pulsante **Modelli**.
7. 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 finestra **Accesso ai dati bloccato**. Facendo clic sul pulsante **Invia tramite e-mail** nella finestra **Accesso ai dati bloccato**, viene creato automaticamente un messaggio per l'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**. Questo messaggio viene creato automaticamente quando si fa clic sul pulsante **Invia tramite e-mail** nella finestra **Richiesta di accesso a file criptati** e viene inviato all'utente quando si concede all'utente l'accesso ai file criptati.
8. Modificare i modelli dei messaggi.
9. Salvare le modifiche.

Criptaggio unità rimovibili

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:

- Criptaggio dell'intero disco (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").

- Criptaggio a livello di file (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. Decrypta 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 nei file system FAT32 e NTFS. Se un'unità rimovibile con un file system non supportato è connessa al computer, il criptaggio dell'unità rimovibile termina con un errore e Kaspersky Endpoint Security assegna l'accesso di sola lettura all'unità rimovibile.

Per criptare le unità rimovibili:

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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
6. 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.

7. 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.

8. 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.

9. Se si desidera configurare il criptaggio per le unità rimovibili individuali, [definire le regole di criptaggio](#).
10. 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.

11. Salvare le modifiche.

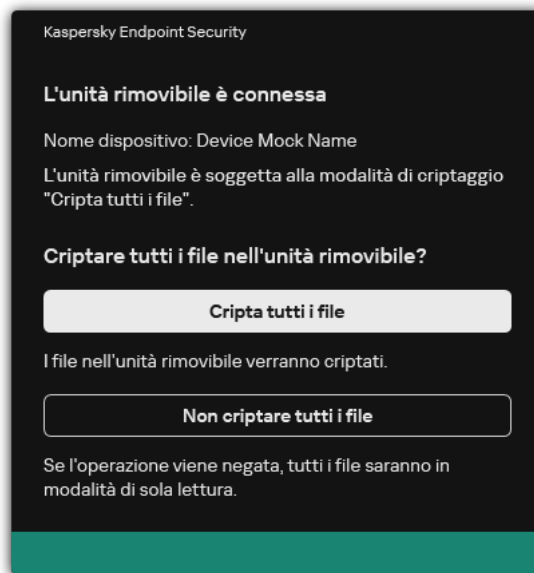
Dopo l'applicazione del criterio, quando l'utente si connette a un'unità rimovibile o se l'unità rimovibile è già connessa, Kaspersky Endpoint Security chiede conferma all'utente per eseguire l'operazione di criptaggio (vedere la figura di seguito).

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
6. 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**.
7. 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.
8. 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](#).

9. 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.

10. 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**.

11. 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
6. 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.
7. 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.
8. Salvare le modifiche.

[Come esportare e importare un elenco di regole di criptaggio delle unità rimovibili in Web Console !\[\]\(c8d96c8885d3000a912c2582004aed63_img.jpg\)](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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. Accedere a **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
5. Nella sezione **Regole di criptaggio per i dispositivi selezionati** fare clic sul collegamento **Regole di criptaggio**.
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.

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:

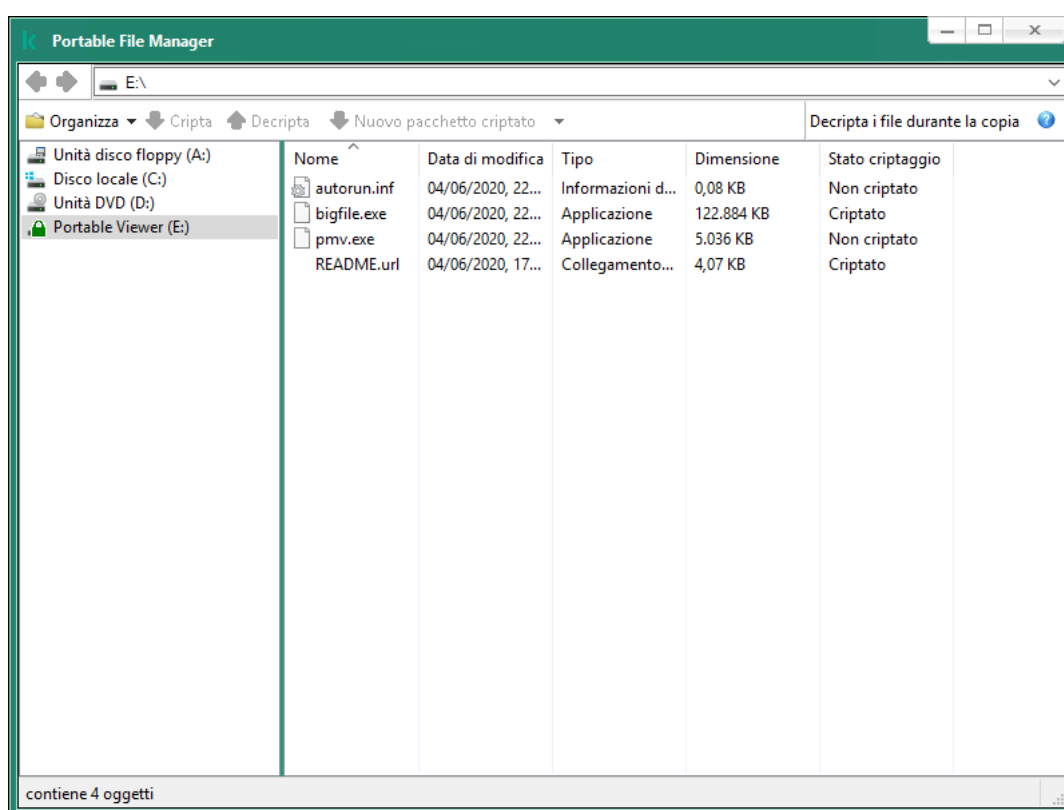
- Non è disponibile la connessione tra il computer e Kaspersky Security Center Administration Server.
- L'infrastruttura è cambiata con la modifica di Kaspersky Security Center Administration Server.
- Kaspersky Endpoint Security non è installato nel computer.

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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
6. 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).

7. Selezionare la casella di controllo **Modalità portatile**.
8. Se necessario, [aggiungere regole di criptaggio per singole unità rimovibili](#).
9. Salvare le modifiche.
10. Dopo aver applicato il criterio, collegare l'unità rimovibile al computer.
11. Confermare l'operazione di criptaggio dell'unità rimovibile.
Verrà visualizzata una finestra in cui è possibile creare una password per Portable File Manager.
12. Specificare una password che soddisfi i requisiti di complessità e confermarla.
13. 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.

[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, selezionare **Dispositivi** → **Criteri e profili**.
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. Accedere a **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
5. In **Gestire il criptaggio**, 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.
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.
- 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.

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.
- Viene selezionata la modalità **Cripta tutti i file** o **Cripta solo i nuovi file**.

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 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. 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.
5. Nel menu di scelta rapida selezionare **Concedi l'accesso in modalità offline**.
6. Nella finestra visualizzata selezionare la scheda **Criptaggio dei dati**.
7. Nella scheda **Criptaggio dei dati** fare clic sul pulsante **Sfoglia**.
8. 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.

[Come ottenere un file di accesso ai dati criptati in Web Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Dispositivi gestiti**.
2. Selezionare la casella di controllo accanto al nome del computer per il quale si desidera ripristinare l'accesso ai dati.
3. Fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.
4. Selezionare la sezione **Criptaggio dei dati**.
5. Fare clic sul pulsante **Selezionare un 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. 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri selezionare **Criptaggio dei dati** → **Criptaggio unità rimovibili**.
6. Per decriptare tutti i file criptati archiviati nelle unità rimovibili, dall'elenco a discesa **Modalità di criptaggio** selezionare **Decripta intera unità rimovibile**.
7. 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**, fare clic su **Decripta intera unità rimovibile**.
8. 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.

Sono possibili i seguenti valori per lo stato di criptaggio:

- *Criterio di criptaggio non definito.* Non è stato definito un criterio di criptaggio Kaspersky Security Center per il computer.
- *Applicazione del criterio in corso.* È in corso il criptaggio e/o decriptaggio dei dati nel computer.

- *Errore.* Si è verificato un errore durante il criptaggio e/o decriptaggio dei dati nel computer.
- *È necessario il riavvio.* È necessario riavviare il sistema operativo per avviare o completare il criptaggio o il decriptaggio dei dati nel computer.
- *Conforme al criterio.* Il criptaggio dei dati nel computer è stato completato utilizzando le impostazioni di criptaggio specificate nel criterio di Kaspersky Security Center applicato al computer.
- *Annullato dall'utente.* L'utente ha rifiutato di confermare l'operazione di criptaggio dei file nell'unità rimovibile.

Visualizzazione dello stato di criptaggio

Per visualizzare lo stato di criptaggio dei dati del computer:

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. Nella scheda **Dispositivi** nell'area di lavoro trascinare la barra di scorrimento completamente a destra.
5. Se non viene visualizzata la colonna **Stato criptaggio**:
 - a. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida relativo all'intestazione della tabella.
 - b. Nel menu di scelta rapida, nell'elenco a discesa **Visualizza**, selezionare **Aggiungi/Rimuovi colonne**.
 - c. Nella finestra visualizzata, selezionare la casella **Stato criptaggio**.
 - d. Fare clic su **OK**.

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.

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 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. Selezionare il nome del computer nell'elenco, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
5. Dal menu di scelta rapida del computer selezionare **Proprietà**. Nella finestra visualizzata, selezionare la scheda **Protezione**.
6. 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

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 seguenti elementi:
 - **Rapporto sullo stato di criptaggio dei dispositivi gestiti.**
 - **Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa.**
 - **Rapporto sugli errori di criptaggio dei file.**
 - **Rapporto sul blocco dell'accesso ai file criptati.**

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.

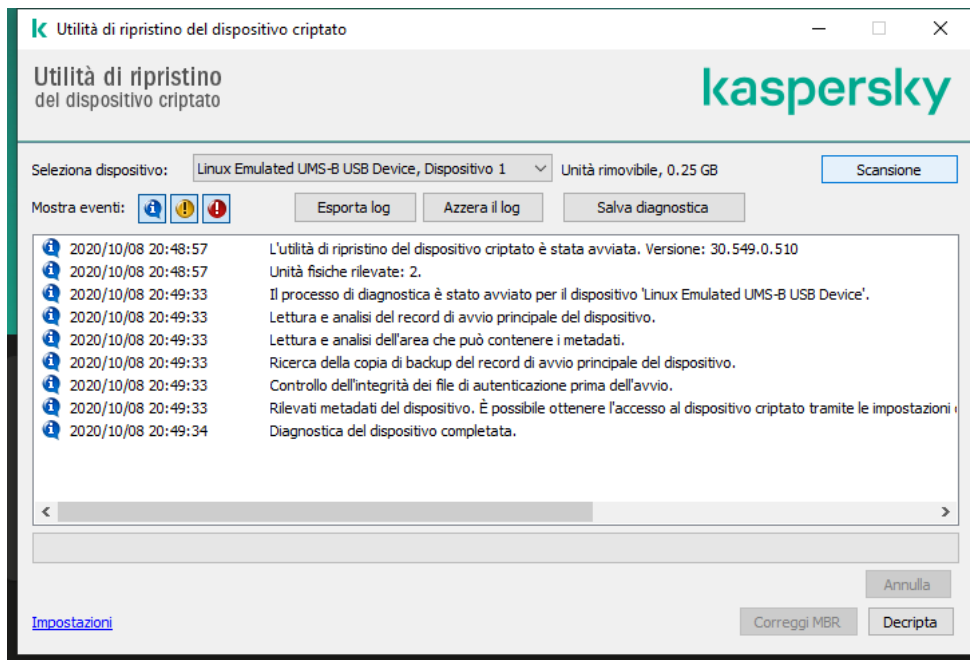
Ripristino dei dati utilizzando l'utilità di ripristino FDERT

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 **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 **Sfoggia** 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 for Windows**.

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 for Windows**.

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: *Criptaggio avanzato (AES256)* o *Criptaggio superficiale (AES56)*. La libreria di criptaggio AES viene installata insieme all'applicazione.
5. Fare clic su **Sfoggia** 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 sul pulsante **Apri**.

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, selezionare **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 sul pulsante **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: *Criptaggio avanzato (AES256)* o *Criptaggio superficiale (AES56)*. La libreria di criptaggio AES viene installata insieme all'applicazione.

c. Fare clic sul pulsante **Selezionare un file** e selezionare il file della richiesta di accesso ricevuto dall'utente (un file con estensione FDERTC).

d. Fare clic sul pulsante **Salva chiave** e selezionare una cartella in cui salvare il file chiave per accedere 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

Kaspersky Endpoint Security supporta le soluzioni Detection and Response tramite un agente integrato. Per utilizzare Detection and Response, è necessario abilitare l'integrazione con queste soluzioni durante l'installazione dell'applicazione. 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 Sandbox 2.0.

È possibile utilizzare Kaspersky Endpoint Security con la soluzione Detection and Response in diverse configurazioni, ad esempio [MDR+EDR Optimal 2.0+Kaspersky Sandbox 2.0].

Kaspersky Endpoint Agent supporta le soluzioni Detection and Response non supportate in Kaspersky Endpoint Security integrato (ad esempio, Kaspersky Sandbox 1.0).

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.

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 for Windows 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*

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.

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

Migrazione di criteri e attività per Kaspersky Endpoint Agent

Kaspersky Endpoint Security 11.7.0 offre ora 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 Managed Detection and Response (MDR).

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, selezionare **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 su un criterio di Kaspersky Endpoint Agent per selezionare il criterio di Kaspersky Endpoint Security di 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

Chiusura della procedura guidata. Di conseguenza, la procedura guidata:

- 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 per Kaspersky Endpoint Detection and Response e Kaspersky Sandbox. Allo stesso tempo, la procedura guidata lascia le attività Kaspersky Endpoint Agent immutate.

Migrazione della configurazione [KES+KEA] alla configurazione [KES+agente integrato]

Kaspersky Endpoint Security 11.7.0 ora è dotato di agenti integrati per le soluzioni Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum) e Kaspersky Sandbox 2.0. Non è più necessaria un'applicazione Kaspersky Endpoint Agent separata per utilizzare tali soluzioni. Quando si esegue l'upgrade di Kaspersky Endpoint Security alla versione 11.7.0, le soluzioni EDR Optimum e Kaspersky Sandbox continuano a funzionare con Kaspersky Endpoint Security. Inoltre, Kaspersky Endpoint Agent viene rimosso dal computer.

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.

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, incluso Administration 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. Per gestire i componenti di EDR Optimum e Kaspersky Sandbox, è necessario utilizzare Web Console.

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 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, 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.

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 Endpoint Detection and Response Optimum o Kaspersky Sandbox nelle impostazioni del pacchetto di installazione.
- Escludere il componente Kaspersky Endpoint Agent nelle impostazioni del pacchetto di installazione.

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.

In questo caso, è necessario controllare la configurazione di Kaspersky Endpoint Agent installata nel computer. Se l'applicazione Kaspersky Endpoint Agent installata include il componente Endpoint Detection and Response Expert (KATA EDR), rimuovere il componente prima di eseguire l'upgrade dell'applicazione. Se non è possibile rimuovere il componente Endpoint Detection and Response Expert (KATA EDR), Kaspersky Endpoint Security ignorerà i componenti EDR Optimum e Kaspersky Sandbox durante l'upgrade dell'applicazione. È possibile installare i componenti tramite l'attività [Modifica componenti dell'applicazione](#) dopo aver eseguito l'upgrade dell'applicazione.

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 attive 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 attive delle soluzioni Kaspersky. In questo caso, Kaspersky Endpoint Security seleziona automaticamente i componenti in base alla configurazione di Kaspersky Endpoint Agent come segue:

- Se è installato il componente Endpoint Detection and Response Expert (KATA EDR), Kaspersky Endpoint Security seleziona il componente Endpoint Agent. Kaspersky Endpoint Security seleziona solo il componente Endpoint Agent, anche se Kaspersky Endpoint Agent dispone di altri componenti installati, ad esempio la configurazione [KATA EDR+KSB].
- Se è installato il componente Kaspersky Sandbox, EDR Optimal o la configurazione [Kaspersky Sandbox+EDR Optimal], Kaspersky Endpoint Security seleziona i componenti pertinenti. In questo modo, 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 Administration Agent 13.2.
- Verificare lo stato operativo dei componenti EDR Optimum e Kaspersky Sandbox visualizzando il *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non installato*, installare i componenti tramite l'attività [Modifica componenti dell'applicazione](#).
- Accertarsi di accettare l'Informativa di Kaspersky Security Network nel nuovo criterio di Kaspersky Endpoint Security for Windows.

Accertarsi che la funzionalità EDR Optimum sia attivata nel *Rapporto sullo stato dei componenti dell'applicazione*. Se un componente presenta lo stato *Non coperto dalla licenza*, accertarsi che [la funzionalità di distribuzione della chiave di licenza automatica di EDR Optimum sia attivata](#).

Upgrade dell'applicazione come parte di KATA EDR

Se Kaspersky Endpoint Agent è installato per l'integrazione con Kaspersky Anti Targeted Attack Platform (il componente Endpoint Detection and Response Expert (KATA EDR)), è possibile eseguire l'upgrade di Kaspersky Endpoint Security for Windows in uno dei seguenti modi:

- Utilizzo di un'attività di installazione remota.

A tale scopo, è necessario modificare le seguenti impostazioni:

- Escludere i componenti Endpoint Detection and Response Optimum e Kaspersky Sandbox nelle impostazioni del pacchetto di installazione.

- Selezionare il componente Kaspersky Endpoint Agent nelle impostazioni del pacchetto di installazione. Se nel computer è già installato Kaspersky Endpoint Agent, viene eseguito l'upgrade dell'applicazione alla versione 3.11.
- Utilizzando il servizio di aggiornamento di Kaspersky (SMU).
A tale scopo, è necessario confermare l'upgrade dell'applicazione. Kaspersky Endpoint Security esclude l'installazione di Endpoint Detection and Response Optimum e Kaspersky Sandbox. L'upgrade di Kaspersky Endpoint Agent non è supportato. È possibile effettuare l'upgrade di Kaspersky Endpoint Agent manualmente.
- In locale, utilizzando l'installazione guidata.
Kaspersky Endpoint Security esclude l'installazione di Endpoint Detection and Response Optimum e Kaspersky Sandbox. Se nel computer è già installato Kaspersky Endpoint Agent, viene eseguito l'upgrade dell'applicazione alla versione 3.11.

Managed Detection and Response



Kaspersky Endpoint Security 11.6.0 introduce l'agente integrato per 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](#).

Integrazione 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.

Per consentire il funzionamento di Managed Detection and Response, è necessario abilitare i seguenti componenti.

- [Kaspersky Security Network \(modalità estesa\)](#).
- [Rilevamento del Comportamento](#).

L'abilitazione di questi componenti non è facoltativa. Se non abilitati, Kaspersky Managed Detection and Response potrebbe non funzionare, poiché non riceve i dati di telemetria necessari.

Inoltre, Kaspersky Managed Detection and Response utilizza i dati ricevuti da altri componenti applicativi. L'abilitazione di tali componenti è facoltativa. I componenti che forniscono ulteriori dati includono:

- [Protezione minacce web](#).
- [Protezione minacce di posta](#).
- [Firewall](#).

Affinché Kaspersky Managed Detection and Response funzioni con Administration Server tramite Kaspersky Security Center Web Console, è inoltre 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. Per ulteriori dettagli sull'integrazione di Kaspersky Security Center con altre soluzioni Kaspersky, consultare la [Guida di Kaspersky Security Center](#).

L'integrazione con Kaspersky Managed Detection and Response prevede i seguenti passaggi:

1 Configurazione dell'istanza privata di Kaspersky Security Network

Ignorare questo passaggio se si utilizza Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console configura automaticamente Kaspersky Security Network locale quando si installa il plug-in MDR.

L'istanza privata di KSN supporta lo scambio dei dati tra computer e i server dedicati di Kaspersky Security Network, ma non l'istanza globale di KSN.

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 Security Network privato, 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 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 <nome file>
```

dove <nome file> è il nome del file di configurazione contenente le impostazioni dell'istanza privata di KSN (formato file PKCS7 o PEM).

Esempio:

```
avp.com KSN /private C:\kpsn_config.pkcs7
```

Di conseguenza, Kaspersky Endpoint Security utilizzerà KSN Privato per determinare la reputazione di file, applicazioni e siti Web. Le impostazioni dei criteri nella sezione **Kaspersky Security Network** mostreranno il seguente stato operativo: *Rete KSN: KSN Privato*.

Per consentire il funzionamento di Managed Detection and Response è necessario [abilitare la modalità KSN estesa](#).

2 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](#).

[Come abilitare Managed Detection and Response 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. Selezionare il criterio necessario e fare doppio clic per aprire le proprietà del criterio.
5. Nella finestra dei criteri, selezionare **Detection and Response** → **Managed Detection and Response**.
6. Selezionare la casella di controllo **Managed Detection and Response**.
7. Nella sezione **Impostazioni** fare clic su **Importa** e selezionare il file BLOB ricevuto in Kaspersky Managed Detection and Response Console. Il file ha l'estensione P7.
8. Salvare le modifiche.

[Come abilitare il componente Managed Detection and Response in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 **Detection and Response** → **Managed Detection and Response**.
5. Attivare l'interruttore **Managed Detection and Response**.
6. Fare clic su **Importa** e selezionare il file BLOB ottenuto in Kaspersky Managed Detection and Response Console. Il file ha l'estensione P7.
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 <nome file> /login=<nome utente> /password=<password>
```

Per eseguire questo comando, [Protezione tramite password deve essere abilitato](#). L'utente deve disporre dell'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 caricherà il file e lo invierà al computer durante la successiva sincronizzazione con Kaspersky Security Center. Verificare 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.

Migrazione da Kaspersky Endpoint Agent

Kaspersky Endpoint Security versione 11 e successive supporta la soluzione MDR. Kaspersky Endpoint Security versioni 11-11.5.0 invia solo i dati di telemetria a Kaspersky Managed Detection and Response per abilitare il rilevamento delle minacce. Kaspersky Endpoint Security versione 11.6.0 è dotato di tutte le funzionalità dell'agente integrato (Kaspersky Endpoint Agent).

Se si utilizza Kaspersky Endpoint Security 11-11.5.0, è necessario aggiornare i database alla versione più recente per l'integrazione con la soluzione MDR. È inoltre necessario installare Kaspersky Endpoint Agent.

Se si utilizza Kaspersky Endpoint Security 11.6.0 o versioni successive, non è necessario installare Kaspersky Endpoint Agent per utilizzare la soluzione MDR.

Per eseguire la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows:

1. Configurare l'integrazione con Kaspersky Managed Detection and Response nei criteri di Kaspersky Endpoint Security.
2. Disabilitare il componente Managed Detection and Response nei criteri di Kaspersky Endpoint Agent.

Se i criteri di Kaspersky Endpoint Security si applicano anche ai computer senza Kaspersky Endpoint Security 11-11.5.0 installato, è innanzitutto necessario creare un criterio di Kaspersky Endpoint Agent separato per tali computer. Nel nuovo criterio, configurare l'integrazione con Kaspersky Managed Detection and Response.

Endpoint Detection and Response



Kaspersky Endpoint Security 11.7.0 dispone ora di un agente integrato per la soluzione Kaspersky Endpoint Detection and Response Optimum (di seguito denominato anche "EDR Optimum").

Kaspersky Endpoint Security 11.8.0 dispone ora di 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. *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](#).

Kaspersky Endpoint Detection and Response utilizza i seguenti strumenti di Threat Intelligence:

- 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. EDR Expert utilizza la soluzione Kaspersky Private Security Network (KPSN), che invia i dati ai server regionali senza inviare i dati dai dispositivi a KSN.
- Integrazione con il sistema informativo [Kaspersky Threat Intelligence Portal](#), che contiene e mostra informazioni sulla reputazione di file e indirizzi Web.
- Database delle [minacce di Kaspersky](#).

Integrazione con Kaspersky Endpoint Detection and Response

Per l'integrazione con Kaspersky Endpoint Detection and Response, è necessario aggiungere il componente Endpoint Detection and Response Optimal (EDR Optimal) o il componente Endpoint Detection and Response Expert (EDR Expert) e configurare Kaspersky Endpoint Security.

I componenti EDR Optimum ed EDR Expert non sono compatibili.

Per il corretto funzionamento di Endpoint Detection and Response, è necessario soddisfare le seguenti condizioni:

- Kaspersky Security Center 13.2. Nelle versioni precedenti di Kaspersky Security Center, non è possibile attivare la funzionalità Endpoint Detection and Response.
- 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 Web 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 e 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 EDR Optimum o EDR Expert durante l'[installazione](#) o l'[upgrade](#), oltre a utilizzare l'attività [Modifica 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 sarà 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 sarà disponibile dopo aver aggiunto una chiave separata per Kaspersky Endpoint Detection and Response. Di conseguenza, nel computer vengono installate 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](#).

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 e Cloud Console](#) 

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 **Detection and Response** → **Endpoint Detection and Response**.
5. Attivare l'interruttore **Endpoint Detection and Response**.
6. Salvare le modifiche.

Il componente Kaspersky Endpoint Detection and Response è abilitato. Verificare 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** 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 e Cloud Console. Ad esempio, è possibile scaricare un file dalla quarantena per l'analisi in Web Console e Cloud Console.

- Dati della catena di sviluppo delle minacce.

I dati sono necessari per ottenere informazioni sulle minacce rilevate in un computer in Web Console e Cloud Console. È possibile visualizzare i dettagli degli avvisi ed eseguire azioni di risposta in Web Console e Cloud Console.

[Come abilitare il trasferimento dei dati ad Administration Server in Web Console e Cloud Console](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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. Selezionare le seguenti caselle nel blocco **Trasferimento dei dati ad Administration Server**:
 - **Informazioni sui file in quarantena**
 - **Informazioni sulla catena di sviluppo delle minacce**
6. Salvare le modifiche.

Migrazione da Kaspersky Endpoint Agent

Se si utilizza Kaspersky Endpoint Security 11.7.0 o versione successiva con il componente EDR Optimal (agente integrato) installato, il supporto dell'integrazione con la soluzione Kaspersky Endpoint Detection and Response Optimal è immediatamente disponibile dopo l'installazione. Il componente EDR Optimum non è compatibile con Kaspersky Endpoint Agent. Se Kaspersky Endpoint Agent è installato nel computer, quando Kaspersky Endpoint Security viene aggiornato alla versione 11.7.0, Kaspersky Endpoint Detection and Response Optimum continua a funzionare con Kaspersky Endpoint Security ([migrazione della configurazione \[KES+KEA\] a \[KES1+agente integrato\]](#)). Inoltre, Kaspersky Endpoint Agent verrà rimosso dal computer. Per completare la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows, è necessario trasferire le impostazioni dei criteri e delle attività tramite la [migrazione guidata](#).

Se si utilizza Kaspersky Endpoint Security 11.4.0-11.6.0 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. È necessario scaricare il pacchetto di distribuzione di Kaspersky Endpoint Agent separatamente.

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).

Il componente EDR 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.

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. Le attività di *scansione IOC* consentono 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 di 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.

 [DOWNLOAD DEL 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 di un'attività di scansione IOC

È possibile creare attività *Scansione IOC* manualmente:

- Nei dettagli degli avvisi (solo per EDR Optimum).

Dettagli dell'avviso è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli dell'avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Per informazioni dettagliate sulla gestione dei dettagli dell'avviso, 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 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 di scansione IOC:

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

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

b. Nell'elenco a discesa **Tipo di attività**, selezionare **Scansione IOC**.

c. Nel campo **Nome attività**, immettere una breve descrizione.

d. Nel blocco **Selezionare i 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. Chiusura della 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 **Impostazioni scansione IOC**.

10. Caricare i file IOC per cercare gli indicatori di compromissione.

Dopo aver caricato i file IOC, è possibile visualizzare l'elenco degli indicatori dai file IOC.

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. Configurare le azioni se viene rilevato un indicatore di compromissione:

- **Isola il computer 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](#).
- **Sposta la copia in Quarantena, elimina l'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.

12. Accedere alla sezione **Avanzate**.

13. 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:

- **Files - 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 di 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 tipo di dati **Registro di sistema di Windows - RegistryItem**, Kaspersky Endpoint Security esamina [una serie di chiavi del Registro di sistema](#).

14. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

15. Configurare la pianificazione dell'attività.

La funzionalità di riattivazione LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

16. Salvare le modifiche.

17. Selezionare la casella di controllo accanto all'attività.

18. Fare clic sul pulsante **Esegui**.

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 nella 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.

Sposta il file in Quarantena

Quando reagisce alle minacce, Kaspersky Endpoint Detection and Response Optimum può creare attività *Spostare un 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 associato alle soluzioni Kaspersky Sandbox e Kaspersky Endpoint 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](#) e la [Guida di Kaspersky Endpoint Detection and Response Expert](#).

È possibile creare attività *Spostare un 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.

L'attività *Sposta file in Quarantena* ha le seguenti limitazioni:

1. La dimensione del file non deve superare i 100 MB.
2. Gli oggetti critici di sistema (SCO) non possono essere messi in quarantena. Gli SCO sono file necessari per l'esecuzione del sistema operativo e dell'applicazione Kaspersky Endpoint Security for Windows.
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.

Per creare un'attività Spostare un file in Quarantena:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Attività**.
Viene aperto l'elenco delle attività.
2. Fare clic sul pulsante **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 (11.9.0)**.
 - 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 **Selezionare i 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 sul pulsante **Avanti**.
5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic sul pulsante **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\cartella_condivisa\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.

La funzionalità di riattivazione LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

13. Fare clic sul pulsante **Salva**.

14. Selezionare la casella di controllo accanto all'attività.

15. Fare clic sul pulsante **Esegui**.

A questo punto, Kaspersky Endpoint Security sposta il file in Quarantena. 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 *Spostare un 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 *Spostare un file in Quarantena* può non riuscire con l'errore *Spazio insufficiente nell'archivio Quarantena* se si sta tentando di mettere in quarantena un file troppo grande. 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 terze parti. Per ottenere il file, è necessario creare un'attività dedicata. Come risultato dell'esecuzione dell'attività, il file viene salvato nella Quarantena. È possibile scaricare questo file dalla Quarantena sul computer tramite Web Console. Sul computer dell'utente, il file rimane nella cartella originale.

La dimensione del file non deve superare i 100 MB.

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 **Dispositivi** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

b. Nell'elenco a discesa **Tipo di attività**, selezionare **Ottieni file**.

c. Nel campo **Nome attività**, immettere una breve descrizione.

d. Nel blocco **Selezionare i 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 sul pulsante **Avanti**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic sul pulsante **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\cartella_condivisa\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.

La funzionalità di riattivazione LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

13. Fare clic sul pulsante **Salva**.

14. Selezionare la casella di controllo accanto all'attività.

15. Fare clic sul pulsante **Esegui**.

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 file*. Ad esempio, è possibile eliminare da remoto un file quando si risponde alle minacce.

L'attività *Elimina il file* ha le seguenti limitazioni:

- Gli oggetti critici di sistema (SCO) non possono essere eliminati. Gli SCO sono file necessari per l'esecuzione del sistema operativo e dell'applicazione Kaspersky Endpoint Security for Windows.
- 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 file*:

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

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

b. Nell'elenco a discesa **Tipo di attività**, selezionare **Elimina file**.

c. Nel campo **Nome attività**, immettere una breve descrizione.

d. Nel blocco **Selezionare i 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 sul pulsante **Avanti**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic sul pulsante **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\cartella_condivisa\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.

La funzionalità di riattivazione LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

13. Fare clic sul pulsante **Salva**.

14. Selezionare la casella di controllo accanto all'attività.

15. Fare clic sul pulsante **Esegui**.

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 *Completata*, 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 file* può terminare con l'errore *Accesso negato* 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 di avvio del processo:

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

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.
- b. Nell'elenco a discesa **Tipo di attività**, selezionare **Avvio del processo**.
- c. Nel campo **Nome attività**, immettere una breve descrizione.
- d. Nel blocco **Selezionare i 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 sul pulsante **Avanti**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic sul pulsante **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.

Ad esempio, se si desidera eseguire un'utilità (`utility.exe`) che salva le informazioni sulla configurazione del computer in un file denominato `conf.txt`, è necessario immettere i seguenti valori:

- **Comando eseguibile** - `utility.exe`
- **Argomenti della riga di comando** - `/R conf.txt`
- **Percorso della cartella di lavoro** - `C:\Utenti\admin\Diagnostic\`

In alternativa, nel campo **Comando eseguibile**, è possibile immettere `C:\Users\admin\Diagnostic\utility.exe /R conf.txt`. In questo caso, non è necessario immettere le altre impostazioni.

11. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

12. Configurare la pianificazione dell'attività.

La funzionalità di riattivazione LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

13. Fare clic sul pulsante **Salva**.

14. Selezionare la casella di controllo accanto all'attività.

15. Fare clic sul pulsante **Esegui**.

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 nella sezione **Risultati**.

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 [Avvio del 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:

- Gli oggetti critici di sistema (SCO) non possono essere terminati. Gli SCO sono file necessari per l'esecuzione del sistema operativo e dell'applicazione Kaspersky Endpoint Security for Windows.
- 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 **Dispositivi** → **Attività**.

Viene aperto l'elenco delle attività.

2. Fare clic sul pulsante **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 (11.9.0)**.

b. Nell'elenco a discesa **Tipo di attività**, selezionare **Terminazione processo**.

c. Nel campo **Nome attività**, immettere una breve descrizione.

d. Nel blocco **Selezionare i 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 sul pulsante **Avanti**.

5. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic sul pulsante **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 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\cartella_condivisa\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. Nella finestra delle proprietà dell'attività, selezionare la scheda **Pianificazione**.

11. Configurare la pianificazione dell'attività.

La funzionalità di riattivazione LAN non è disponibile per questa attività. Assicurarsi che il computer sia acceso per eseguire l'operazione.

12. Fare clic sul pulsante **Salva**.

13. Selezionare la casella di controllo accanto all'attività.

14. Fare clic sul pulsante **Esegui**.

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 nella 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 dell'avviso è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli dell'avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Per informazioni dettagliate sulla gestione dei dettagli dell'avviso, 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 del file o l'hash (SHA256 o MD5) oppure sia il percorso del file che l'hash del file.

È inoltre possibile gestire Prevenzione dell'esecuzione in locale tramite la [riga di comando](#).

Si sconsiglia di creare più di 5000 regole di prevenzione delle esecuzioni, per evitare di causare instabilità di sistema.

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.

Modalità delle regole di prevenzione dell'esecuzione

Il componente Prevenzione dell'esecuzione può funzionare in due modalità:

- **Solo statistiche.**

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.

- **Attivo.**

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, selezionare **Dispositivi** → **Criteri e profili**.
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 **Detection and Response** → **Endpoint Detection and Response**.

5. Utilizzare l'interruttore **Prevenzione dell'esecuzione** per abilitare o disabilitare il componente.
6. Nel blocco **Azione in caso di esecuzione o apertura di un oggetto vietato**, selezionare la modalità operativa del componente:
 - **Blocca e scrivi nel rapporto.** 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.
 - **Registra solo gli 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.
7. Creare un elenco di regole di prevenzione dell'esecuzione:
 - a. Fare clic sul pulsante **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**.

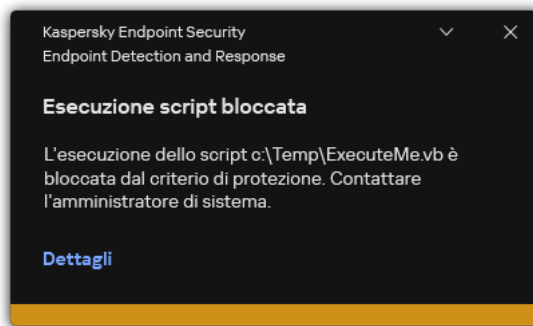
Se si seleziona un tipo di oggetto errato, Kaspersky Endpoint Security non blocca il file o lo script.
 - d. Per aggiungere il file, è necessario inserire l'hash del file (SHA256 o MD5), il percorso completo del file oppure sia l'hash che il percorso.

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\cartella_condivisa\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](#).

- e. Fare clic su **OK**.
8. 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 l'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.

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, selezionare **Dispositivi** → **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. Nel blocco **Azione se viene rilevato un oggetto IOC**, selezionare le caselle di controllo **Intraprendi azioni di risposta in seguito al rilevamento di un oggetto IOC** e **Isola il computer dalla rete**.

5. 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 Isolamento di rete in modo che venga disattivato automaticamente 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 **Dispositivi** → **Criteri e profili**.

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 **Detection and Response** → **Endpoint Detection and Response**.

5. Nel blocco **Isolamento di rete**, fare clic su **Configura le impostazioni di sblocco del computer**.

6. Si apre una finestra; in questa finestra, selezionare la casella di controllo **Sblocca automaticamente il computer isolato tra N ore** e immettere il ritardo per la disattivazione automatica di Isolamento di rete.

7. Salvare le modifiche.

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.

Come attivare manualmente l'isolamento di rete di un computer

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Dispositivi gestiti**.
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**.
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 Isolamento di rete in modo che venga disattivato automaticamente 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, selezionare **Dispositivi** → **Dispositivi gestiti**.
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, selezionare **Dispositivi** → **Dispositivi gestiti**.
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**.
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 **Sblocca il computer isolato dalla rete**.

È inoltre possibile disabilitare Isolamento di rete in locale tramite la [riga di comando](#).

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, selezionare **Dispositivi** → **Criteri e profili**.
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 **Detection and Response** → **Endpoint Detection and Response**.
5. Nel blocco **Esclusioni dall'isolamento di rete**, fare clic su **Esclusioni**.
6. 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.
7. 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.
8. Salvare le modifiche.

[Come aggiungere un'esclusione di Isolamento di rete in modalità manuale](#)

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Dispositivi gestiti**.
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.

Appendice 1. 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	acrord32.exe	pdf
Foxit PDF Reader	FoxitReader.exe	
STDU Viewer	STDUViewerApp.exe	
Microsoft Edge	MicrosoftEdge.exe	
Google Chrome	chrome.exe	
Mozilla Firefox	firefox.exe	
Yandex Browser	browser.exe	
Tor Browser	tor.exe	

Appendice 2. Interpreti di script supportati

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
- msixexec.exe
- perl.exe
- powershell.exe

- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacyelevated.exe
- wscript.exe
- wvhost.exe

Prevenzione dell'esecuzione supporta l'esecuzione delle applicazioni Java nell'ambiente di runtime Java (processi java.exe e javaw.exe).

Appendice 3. Ambito della scansione IOC nel Registro di sistema (RegistryItem)

Quando si aggiunge il tipo di dati RegistryItem all'ambito della scansione IOC, 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 4. 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.
- 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.

 [DOWNLOAD DEL 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	<p>OpenIOC 1.0:</p> <p><code>is</code> <code>isnot</code> (come eccezione dal set) <code>contains</code> <code>containsnot</code> (come eccezione dal set)</p> <p>OpenIOC 1.1:</p> <p><code>is</code> <code>contains</code> <code>starts-with</code> <code>ends-with</code> <code>matches</code> <code>greater-than</code> <code>less-than</code></p>
Attributi di condizioni supportate	<p>OpenIOC 1.1:</p> <p><code>preserve-case</code> <code>negate</code></p>
Operatori supportati	<p>AND OR</p>
Tipi di dati supportati	<p>"date": data (condizioni applicabili: <code>is</code>, <code>greater-than</code>, <code>less-than</code>)</p> <p>"int": numero intero (condizioni applicabili: <code>is</code>, <code>greater-than</code>, <code>less-than</code>)</p> <p>"string": stringa (condizioni applicabili: <code>is</code>, <code>contains</code>, <code>matches</code>, <code>starts-with</code>, <code>ends-with</code>)</p> <p>"duration": durata in secondi (condizioni applicabili: <code>is</code>, <code>greater-than</code>, <code>less-than</code>)</p>
Funzionalità dell'interpretazione dei tipi di dati	<p>I tipi di dati "boolean string", "restricted string", "md5", "IP", "sha256" e "base64Binary" sono interpretati come stringa.</p> <p>L'applicazione supporta l'interpretazione dell'impostazione Content per i tipi di dati int e date quando è impostata in formato di intervalli:</p>

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.

Kaspersky Sandbox



Kaspersky Endpoint Security 11.7.0 dispone ora di un agente integrato per l'integrazione con la soluzione Kaspersky Sandbox. *La soluzione Kaspersky Sandbox* rileva e blocca automaticamente le minacce avanzate sui computer. Kaspersky Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Kaspersky Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Kaspersky Sandbox). Per ulteriori dettagli sulla soluzione, consultare la Guida di [Kaspersky Sandbox](#).

Per la soluzione Kaspersky Sandbox sono disponibili le seguenti configurazioni:

Kaspersky Sandbox 2.0

Kaspersky Sandbox 2.0 supporta la configurazione [KES+agente integrato].

Requisiti minimi:

- Kaspersky Endpoint Security 11.7.0 for Windows o versioni successive.
- Kaspersky Endpoint Agent non è necessario.
- Kaspersky Security Center 13.2.

Kaspersky Sandbox 1.0

Kaspersky Sandbox 1.0 supporta la configurazione [KES+KEA].

Requisiti minimi:

- Kaspersky Endpoint Security 11.2.0 - 11.6.0 for Windows.
- Kaspersky Endpoint Agent 3.8.

È possibile installare Kaspersky Endpoint Agent dal kit di distribuzione Kaspersky Endpoint Security for Windows.

- Kaspersky Security Center 11.

Integrazione con Kaspersky Sandbox

L'aggiunta del componente Kaspersky Sandbox è necessaria per l'integrazione con il componente Kaspersky Sandbox. È possibile selezionare il componente Kaspersky Sandbox durante l'[installazione](#) o l'[upgrade](#), oltre a utilizzare l'attività [Modifica 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, selezionare **Dispositivi** → **Criteri e profili**.
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 **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, selezionare **Impostazioni della console** → **Integrazione**.
2. Passare alla sezione **Integrazione tra servizi**.
3. Utilizzare l'interruttore **Stabilisci una connessione in background per l'integrazione tra servizi**.
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.

- Il componente Kaspersky Sandbox è abilitato.

È possibile abilitare o disabilitare l'integrazione con Kaspersky Sandbox in Web Console o in locale con la [riga di comando](#).

Per abilitare e disabilitare l'integrazione con Kaspersky Sandbox:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 **Detection and Response** → **Kaspersky Sandbox**.
5. Utilizzare l'interruttore **Integrazione con Kaspersky Sandbox** per abilitare o disabilitare il componente.
6. Salvare le modifiche.

A questo punto, il componente Kaspersky Sandbox è abilitato. Verificare 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 **Kaspersky Sandbox** verrà aggiunto all'elenco dei componenti di Kaspersky Endpoint Security.

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 Codice di errore: formato XXX (ad esempio, 0xa67b01f4), contattare l'[Assistenza tecnica](#).

Migrazione da Kaspersky Endpoint Agent

Se si utilizza Kaspersky Endpoint Security 11.7.0 o versione successiva con il componente Kaspersky Sandbox installato, l'interoperabilità con la soluzione Kaspersky Sandbox (agente integrato) è disponibile subito dopo l'installazione. Il componente Kaspersky Sandbox non è compatibile con Kaspersky Endpoint Agent. Se Kaspersky Endpoint Agent è installato nel computer, quando Kaspersky Endpoint Security viene aggiornato alla versione 11.7.0, Kaspersky Sandbox continua a funzionare con Kaspersky Endpoint Security ([migrazione della configurazione \[KES+KEA\] a \[KES+agente integrato\]](#)). Inoltre, Kaspersky Endpoint Agent verrà rimosso dal computer. Per completare la migrazione da Kaspersky Endpoint Agent a Kaspersky Endpoint Security for Windows, è necessario trasferire le impostazioni dei criteri e delle attività tramite la [migrazione guidata](#).

Se si utilizza Kaspersky Endpoint Security 11.4.0-11.6.0 per l'interoperabilità con Kaspersky Sandbox, 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. È necessario scaricare il pacchetto di distribuzione di Kaspersky Endpoint Agent separatamente.

Il componente Kaspersky Sandbox che fa parte di Kaspersky Endpoint Security supporta l'interoperabilità con la soluzione Kaspersky Sandbox 2.0. La soluzione Kaspersky Sandbox 1.0 non è supportata.

Aggiunta di un certificato TLS

Per configurare una connessione attendibile con i server di Kaspersky Sandbox, è necessario preparare un certificato TLS. Successivamente, è necessario aggiungere il certificato ai server di Kaspersky Sandbox e al criterio di Kaspersky Endpoint Security. Per ulteriori dettagli sulla preparazione del certificato e sull'aggiunta del certificato ai server, consultare la [Guida di Kaspersky Sandbox](#).

È possibile aggiungere un certificato TLS in Web Console o in locale tramite la [riga di comando](#).

Per aggiungere un certificato TLS in Web Console:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 **Detection and Response** → **Kaspersky Sandbox**.
5. Fare clic sul collegamento **Impostazioni della connessione al server**.
Si apre la finestra Impostazioni della connessione al server di Kaspersky Sandbox.
6. Nel blocco **Certificato TLS del server**, fare clic su **Aggiungi** e selezionare il file del certificato TLS.
Kaspersky Endpoint Security può disporre di un solo certificato TLS per un server di Kaspersky Sandbox. Se in precedenza è stato aggiunto un certificato TLS, tale certificato viene revocato. Viene utilizzato solo l'ultimo certificato aggiunto.
7. Configurare le impostazioni di connessione avanzate per i server di Kaspersky Sandbox:

- **Timeout.** Timeout della connessione per il server Kaspersky Sandbox. Allo scadere del timeout configurato, Kaspersky Endpoint Security invia una richiesta al server successivo. È possibile aumentare il timeout della connessione per Kaspersky Sandbox 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 delle richieste Kaspersky Sandbox.** Dimensione della cartella della coda di richieste. Quando si accede a un oggetto sul computer (file eseguibile avviato o documento aperto, ad esempio in formato DOCX o PDF), Kaspersky Endpoint Security può anche inviare l'oggetto da sottoporre a scansione da parte di Kaspersky Sandbox. Se sono presenti più richieste, 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, Kaspersky 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.

8. 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.

Aggiunta dei server di Kaspersky Sandbox

Per connettere i computer ai server di Kaspersky Sandbox con immagini virtuali dei sistemi operativi, è necessario immettere un indirizzo server e una porta. Per ulteriori dettagli sulla distribuzione di immagini virtuali e sulla configurazione dei server di Kaspersky Sandbox, consultare la [Guida di Kaspersky Sandbox](#).

Per aggiungere server Kaspersky Sandbox a Web Console:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 **Detection and Response** → **Kaspersky Sandbox**.
5. Nel blocco **Server Kaspersky Sandbox**, fare clic su **Aggiungi**.
6. Si apre una finestra; nella finestra, immettere l'indirizzo e la porta del server di Kaspersky Sandbox (IPv4, IPv6, DNS).
7. Salvare le modifiche.

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. Le attività di *scansione IOC* consentono 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 di 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 dell'attività 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 di scansione IOC:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **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 scansione IOC**.
5. Configurare le azioni se viene rilevato un indicatore di compromissione:
 - **Sposta la copia in Quarantena, elimina l'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.
6. Configurare la modalità di esecuzione dell'attività Scansione IOC utilizzando la casella di controllo **Esegui solo quando il computer è inattivo**. Questa casella di controllo consente di abilitare o disabilitare la funzione che sospende l'attività *Scansione IOC* quando le risorse del computer sono limitate. Kaspersky Endpoint Security sospende l'attività *Scansione IOC* se lo screensaver è disattivato e il computer non è bloccato.
Questa opzione di pianificazione consente di conservare le risorse del computer durante l'utilizzo del computer.

7. Salvare le modifiche.

È possibile visualizzare i risultati dell'attività nelle proprietà dell'attività nella 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.

Kaspersky Anti Targeted Attack Platform (KATA EDR)



Kaspersky Endpoint Security 11.9.0 aggiunge il supporto per l'integrazione con il componente Kaspersky Endpoint Detection and Response che fa 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 due blocchi funzionali: Kaspersky Anti Targeted Attack (in seguito definito anche "KATA") e Kaspersky Endpoint Detection and Response (di seguito definito anche "KEDR"). È possibile acquistare KEDR separatamente. Per informazioni dettagliate sulla soluzione, consultare la [Guida di Kaspersky Anti Targeted Attack Platform](#).

Kaspersky Endpoint Detection and Response utilizza i seguenti strumenti di Threat Intelligence:

- 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.
- Integrazione con il sistema informativo [Kaspersky Threat Intelligence Portal](#), che contiene e mostra informazioni sulla reputazione di file e indirizzi Web.
- Database delle [minacce di Kaspersky](#).

Principio di funzionamento della soluzione

L'applicazione Kaspersky Endpoint Agent 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 vengono inviate al server di Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Agent può integrarsi con Kaspersky Endpoint Security for Windows. In questo caso, l'applicazione Kaspersky Endpoint Agent invia anche informazioni al server di Kaspersky Anti Targeted Attack Platform sulle minacce rilevate da Kaspersky Endpoint Security for Windows, nonché informazioni sull'elaborazione dei risultati di tali minacce.

Integrazione con KATA EDR

L'integrazione con KATA EDR richiede l'aggiunta del componente Kaspersky Anti Targeted Attack Platform (KATA EDR) e l'installazione di Kaspersky Endpoint Agent. È possibile selezionare il componente KATA EDR durante l'[installazione](#) o l'[upgrade](#), oltre a utilizzare l'attività [Modifica componenti dell'applicazione](#).

Il componente KATA EDR non è compatibile con i componenti EDR Optimum ed EDR Expert.

In Kaspersky Endpoint Security 11.9.0, il kit di distribuzione non include più il pacchetto di distribuzione di Kaspersky Endpoint Agent. È possibile scaricare il pacchetto di distribuzione di Kaspersky Endpoint Agent dal kit di distribuzione di Kaspersky Anti Targeted Attack Platform.

KATA EDR utilizza le informazioni ricevute dai componenti dell'applicazione. I seguenti componenti assicurano il funzionamento di KATA EDR:

- [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.](#)

Assicurarsi che tali componenti siano abilitati e in esecuzione.

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 associato alle soluzioni Kaspersky Sandbox e Kaspersky Endpoint 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](#) e la [Guida di Kaspersky Endpoint Detection and Response Expert](#).

Kaspersky Endpoint Security utilizza l'account di sistema (SYSTEM) per mettere in quarantena i file.

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.) 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 200 MB. Al raggiungimento della dimensione massima, Kaspersky Endpoint Security elimina automaticamente i file meno recenti da Quarantena.

Per configurare la dimensione massima della quarantena:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.

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 a N MB.** Dimensione massima della quarantena in MB. Ad esempio, è possibile impostare la dimensione massima della quarantena su 200 MB. Quando la Quarantena raggiunge la dimensione massima, Kaspersky Endpoint Security invia l'evento corrispondente 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 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.
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](#).

Per abilitare il trasferimento dei dati dei file in quarantena a Kaspersky Security Center:

1. Nella finestra principale di Web Console, selezionare **Dispositivi** → **Criteri e profili**.
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 **Trasferimento dei dati ad Administration Server**, selezionare la casella di controllo **Informazioni sui file in Quarantena**.
6. Salvare le modifiche.

Di conseguenza, in Web Console è possibile visualizzare l'elenco dei file in quarantena su un computer (**Operazioni** → **Archivi** → **Quarantena**). È possibile utilizzare Web Console per gestire gli oggetti in quarantena (ripristino, eliminazione, aggiunta ecc.)

Kaspersky Security for Windows Server



Kaspersky Endpoint Security 11.8.0 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 KSWS a Kaspersky Endpoint Security for Windows e utilizzare la stessa soluzione per la protezione di workstation e server.

Installazione di KES su KSWS

Kaspersky Endpoint Security (KES) supporta le funzionalità di base dell'applicazione Kaspersky Security for Windows Server (KSWS). A partire da Kaspersky Endpoint Security versione 11.8.0, è possibile utilizzare KES anziché KSWS.

Prima di installare KES, è necessario disinstallare KSWS. È possibile disinstallare l'applicazione in remoto tramite l'attività [Disinstalla l'applicazione in remoto](#) o [in locale sul server](#). Dopo aver disinstallato KSWS, potrebbe essere necessario riavviare il server. Se si desidera installare Kaspersky Endpoint Security senza riavviare il computer, si consiglia di verificare che Kaspersky Security for Windows Server sia completamente disinstallato. Vedere l'elenco di file e servizi da verificare di seguito. Se l'applicazione non viene disinstallata completamente, potrebbero verificarsi errori del server dopo l'installazione di Kaspersky Endpoint Security. Si consiglia inoltre di verificare che l'applicazione sia completamente disinstallata se è stata utilizzata l'utilità [Kavremover](#) non supporta KSWS.

Dopo aver disinstallato KSWS, [installare Kaspersky Endpoint Security for Windows](#) utilizzando qualsiasi metodo disponibile.

Verifica della rimozione di Kaspersky Security for Windows Server

Verificare che Kaspersky Security for Windows Server sia completamente disinstallato:

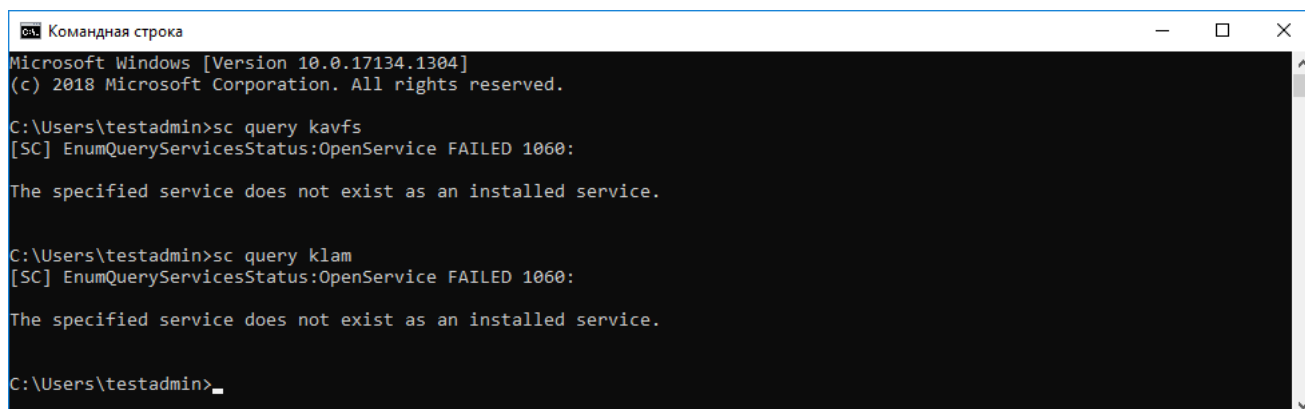
- La cartella %ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\ non esiste.
- I seguenti servizi non sono in esecuzione:
 - Kaspersky Security Service (KAVFS)
 - Kaspersky Security Management Service (KAVFSGT)
 - Kaspersky Security Exploit Prevention Service (KAVFSSLP)
 - Kaspersky Security Script Checker Service (KAVFSSCS)

È possibile verificare i servizi in esecuzione in Gestione attività oppure utilizzando il comando `sc query` (vedere la figura riportata di seguito).

- I seguenti driver non sono installati:
 - klam.sys

- klflt.sys
- klramdisk.sys
- klelaml.sys
- klfltdev.sys
- klips.sys
- klids.sys
- klwtpee

È possibile verificare i driver installati nella cartella `C:\Windows\System32\drivers` oppure utilizzando il comando `sc query`. Se il servizio o il driver è assente, si riceverà la seguente risposta:



```

Microsoft Windows [Version 10.0.17134.1304]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\testadmin>sc query kavfs
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.

C:\Users\testadmin>sc query klam
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

The specified service does not exist as an installed service.

C:\Users\testadmin>
  
```

Verifica della rimozione dei servizi e dei driver di Kaspersky Security for Windows Server

Se i file dell'applicazione o i driver rimangono ancora nel server, eliminarli manualmente. Se alcuni servizi di Kaspersky Security for Windows Server sono ancora in esecuzione, arrestare (`sc stop`) ed eliminarli manualmente (`sc delete`). 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).

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	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

aggiunta da un'attività.	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 .

Gestione dell'applicazione su un server in modalità Core

Un server in modalità 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 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 sul server in modalità Core non è diversa dalla gestione di un computer. È possibile utilizzare criteri e attività per configurare l'applicazione.

La gestione dell'applicazione sui server in modalità Core comporta le seguenti considerazioni speciali:

- Il server in modalità 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 virus*. Quindi, è necessario avviare l'attività *Scansione virus*.
- 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 Core, eseguire il comando seguente:

```
setup_ks.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Per attivare l'applicazione, eseguire il comando seguente:

```
avp.com license /add <codice di attivazione o file della chiave>
```

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
```

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 `HELP`. Per leggere la sintassi di un comando specifico, immettere `HELP <comando>`.

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 `%%`.

Installazione dell'applicazione

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. 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 terze parti) 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.

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] [/pALLOWREBOOT=1]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<nome utente> /pKLPASSWD=
<password> /pKLPASSWDAREA=<ambito della password>] [/pENABLETRACES=1|0 /pTRACESLEVEL=
<livello di traccia>] [/s]
```

oppure

```
msiexec /i <nome kit di distribuzione> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<nome utente> KLPASSWD=<password>
KLPASSWDAREA=<ambito della password>] [ENABLETRACES=1|0 TRACESLEVEL=<livello di
traccia>] [/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](#).

EULA=1	<p>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.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>L'accettazione delle condizioni del Contratto di licenza con l'utente finale è necessaria per installare l'applicazione o eseguire l'aggiornamento della versione.</p> </div>
PRIVACYPOLICY=1	<p>Accettazione dell'Informativa sulla privacy. Il testo dell'Informativa sulla privacy è incluso nel kit di distribuzione di Kaspersky Endpoint Security.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Per installare l'applicazione o eseguire l'upgrade della versione dell'applicazione, è necessario accettare la Informativa sulla privacy.</p> </div>
KSN	<p>Accettazione o rifiuto della partecipazione a Kaspersky Security Network. 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:</p> <ul style="list-style-type: none"> • 1 – accettazione della partecipazione a KSN. • 0 – rifiuto della partecipazione a KSN (valore predefinito). <p>Il pacchetto di distribuzione di Kaspersky Endpoint Security è ottimizzato per l'utilizzo con Kaspersky Security Network. Se si è scelto di non partecipare a Kaspersky Security Network, è necessario aggiornare Kaspersky Endpoint Security subito dopo il completamento dell'installazione.</p>
ALLOWREBOOT=1	<p>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.</p> <p>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.</p>
SKIPPRODUCTCHECK=1	<p>Disabilitazione della verifica della presenza di software incompatibile. L'elenco del software incompatibile è disponibile nel file incompatible.txt incluso nel kit di distribuzione. Se non viene impostato alcun valore per questo parametro e viene rilevato software incompatibile, l'installazione di Kaspersky Endpoint Security verrà terminata.</p>
SKIPPRODUCTUNINSTALL=1	<p>Disabilitazione della rimozione automatica del software incompatibile rilevato. Se non viene impostato alcun valore per questo parametro, Kaspersky Endpoint Security tenta di rimuovere il software incompatibile.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Non è possibile abilitare la rimozione automatica del software incompatibile quando si installa Kaspersky Endpoint Security utilizzando il programma di installazione msiexec. Utilizzare setup_ks.exe per abilitare la rimozione automatica del software incompatibile.</p> </div>

KLLOGIN	<p>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 ai parametri KLPASSWD e KLPASSWDAREA. Per impostazione predefinita, viene utilizzato il nome utente KLAdmin.</p>
KLPASSWD	<p>Specificare una password per accedere a funzionalità e impostazioni di Kaspersky Endpoint Security (la password è specificata insieme ai parametri KLLOGIN e KLPASSWDAREA).</p> <p>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.</p>
KLPASSWDAREA	<p>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:</p> <ul style="list-style-type: none"> • 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.
ENABLETRACES	<p>Abilitazione o disabilitazione del tracciamento dell'applicazione. Dopo l'avvio, Kaspersky Endpoint Security salva i file di traccia nella cartella %ProgramData%\Kaspersky Lab\KES\Traces. Valori disponibili:</p> <ul style="list-style-type: none"> • 1 - il tracciamento è abilitato. • 0 - il tracciamento è disabilitato (valore predefinito).
TRACESLEVEL	<p>Livello di dettaglio delle tracce. Valori disponibili:</p> <ul style="list-style-type: none"> • 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).

	<ul style="list-style-type: none"> • 600 (basso). Tutti i messaggi.
AMPPL	<p>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.</p> <p>La tecnologia AM-PPL è disponibile per i sistemi operativi Windows 10 versione 1703 (RS2) o successiva e Windows Server 2019.</p> <p>Valori disponibili:</p> <ul style="list-style-type: none"> • 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.
RESTAPI	<p>Gestione dell'applicazione tramite REST API. Per gestire l'applicazione tramite REST API, è necessario specificare il nome utente (parametro RESTAPI_User).</p> <p>Valori disponibili:</p> <ul style="list-style-type: none"> • 1 - la gestione tramite REST API è consentita. • 0 – la gestione tramite l'API REST è bloccata (valore predefinito). <p>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.</p>
RESTAPI_User	<p>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 <DOMINIO>\<Nome utente> (ad esempio RESTAPI_User=COMPANY\Administrator). È possibile selezionare un solo utente per l'utilizzo dell'API REST.</p> <p>L'aggiunta di un nome utente è un prerequisito per la gestione dell'applicazione tramite REST API.</p>
RESTAPI_Port	<p>Porta utilizzata per la gestione dell'applicazione tramite REST API. La porta 6782 è utilizzata per impostazione predefinita.</p>
RESTAPI_Certificate	<p>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.</p>
ADMINKITCONNECTOR	<p>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 terze parti. A tale scopo, Kaspersky Endpoint Security fornisce un'API.</p> <p>Valori disponibili:</p> <ul style="list-style-type: none"> • 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.

Esempio:

```
setup_ks.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_ks.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 per l'installazione dell'applicazione
- [install.cfg](#) – impostazioni dell'esecuzione di Kaspersky Endpoint Security
- setup.reg – chiavi del Registro di sistema

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 dei file setup.ini, install.cfg e setup.reg, inserire i 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=<percorso del file setup.reg>.

Attivazione dell'applicazione

Per attivare l'applicazione dalla riga di comando:

digitare la seguente stringa nella riga di comando:

```
avp.com license /add <codice di attivazione o file chiave> [/login=<nome utente>  
/password=<password>]
```

È necessario immettere le credenziali dell'account utente (`/login=<nome utente> /password=<password>`) se [Protezione tramite password è abilitata](#).

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. 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. Il GUID dell'applicazione è disponibile 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 /pKLLLOGIN=<nome utente> /pKLPASSWD=<password> /s /x
```

oppure

```
msiexec.exe /x <GUID> KLLLOGIN=<nome utente> KLPASSWD=<password> /qn
```

Esempio:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLLOGIN=KLAdmin  
KLPASSWD=!Password1 /qn
```

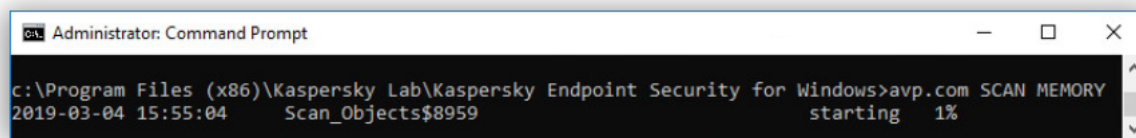
Comandi AVP

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.
3. Per eseguire un comando immettere:

```
avp.com <comando> [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 virus

Eseguire l'attività di scansione virus.

Sintassi del comando

```
SCAN [<ambito della scansione>] [<azione al rilevamento della minaccia>] [<tipi di file>] [<esclusioni della scansione>] [/R[A]:<file del rapporto>] [<tecnologie di scansione>] [/C:<file con impostazioni di scansione virus>]
```

Ambito della scansione	
<file da esaminare>	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: <ul style="list-style-type: none">"C:\Program Files (x86)\Cartella di esempio" – percorso lungo.C:\PROGRA~2\EXAMPL~1 – percorso breve.
/ALL	Eseguire l'attività <i>Scansione completa</i> . Kaspersky Endpoint Security esamina i seguenti oggetti: <ul style="list-style-type: none">Memoria del kernelOggetti caricati all'avvio del sistema operativoSettori di avvioBackup del sistema operativoTutti i dischi rigidi e le unità rimovibili
/MEMORY	Esaminare la memoria del kernel
/STARTUP	Esaminare gli oggetti caricati all'avvio del sistema operativo
/MAIL	Esaminare la cassetta postale di Outlook
/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>	<p>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:</p> <ul style="list-style-type: none"> • "C:\Program Files (x86)\Cartella di esempio" – percorso lungo. • C:\PROGRA~2\EXAMPL~1 – percorso breve.

Azione se viene rilevata una minaccia	
/i0	Avvisa. 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 non è possibile, blocca). Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non è possibile, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive.
/i2	<p>Disinfetta (se non è possibile, elimina). Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.</p> <p>Questa azione è selezionata per impostazione predefinita.</p>
/i3	Disinfetta i file infetti rilevati. Se la disinfezione non riesce, elimina i file infetti. Elimina anche i file composti (ad esempio gli archivi) se il file infetto non può essere disinfettato o eliminato.
/i4	Elimina i file infetti. 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, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security 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	<p>Tutti i file. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina tutti i file senza eccezioni (tutti i formati e le estensioni).</p> <p>Rappresenta l'impostazione predefinita.</p>

Esclusioni dalla scansione	
-e:a	Gli archivi RAR, ARJ, ZIP, CAB, LHA, JAR e ICE sono esclusi dall'ambito della scansione.

-e:b	I database di posta, i messaggi e-mail in entrata e in uscita sono esclusi dall'ambito della scansione.
-e:<maschera file>	I file che corrispondono alla maschera file sono esclusi dall'ambito della scansione. Ad esempio: <ul style="list-style-type: none"> • La maschera *.exe includerà tutti i percorsi dei file con estensione exe. • La maschera example* includerà tutti i percorsi dei file denominati EXAMPLE.
-e:<secondi>	I file la cui scansione richiede più tempo rispetto al limite specificato (in secondi) sono esclusi dall'ambito della scansione.
-es:<megabyte>	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:<file di rapporto>	Salva solo gli eventi critici nel file di rapporto.
/RA:<file di rapporto>	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 dalla scansione 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 con impostazioni di scansione virus>	File con impostazioni dell'attività di scansione virus. Il file deve essere creato manualmente e salvato in formato TXT. Il file può avere i seguenti contenuti: [<ambito della scansione>] [<azione al rilevamento della minaccia>] [<tipi di file>] [<esclusioni della scansione>] [/R[A]:<file del rapporto>] [<tecnologie di scansione>].

Esempio:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Aggiornamento di database e moduli software dell'applicazione

Eseguire l'attività *Aggiornamento*.

Sintassi del comando

```
UPDATE [local] ["<sorgente aggiornamenti>"] [/R[A]:<file di rapporto>] [/C:<file con impostazioni di aggiornamento >]
```

Impostazioni attività di aggiornamento	
local	<p>Avvio dell'attività <i>Aggiornamento</i> creata automaticamente dopo l'installazione dell'applicazione. È possibile modificare le impostazioni dell'attività <i>Aggiornamento</i> nell'interfaccia locale dell'applicazione o nella console di Kaspersky Security Center. Se questa impostazione non è configurata, Kaspersky Endpoint Security avvia l'attività <i>Aggiornamento</i> con le impostazioni predefinite o con le impostazioni specificate nel comando. È possibile configurare le impostazioni dell'attività <i>Aggiornamento</i> come segue:</p> <ul style="list-style-type: none">• UPDATE avvia l'attività <i>Aggiornamento</i> 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 <i>Aggiornamento</i> creata automaticamente dopo l'installazione (attività predefinita).• UPDATE <impostazioni di aggiornamento> avvia l'attività <i>Aggiornamento</i> con impostazioni definite manualmente (vedere di seguito).

Sorgente degli aggiornamenti	
"<sorgente aggiornamenti>"	<p>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: i server degli aggiornamenti di Kaspersky.</p>

Salvataggio degli eventi in una modalità file di rapporto (solo per i profili di Scansione, Updater e Rollback)	
/R:<file di rapporto>	Salva solo gli eventi critici nel file di rapporto.
/RA:<file di rapporto>	Salva tutti gli eventi in un file di rapporto.

Impostazioni avanzate	
/C:<file con impostazioni di aggiornamento>	File con le impostazioni dell'attività <i>Aggiornamento</i> . Il file deve essere creato manualmente e salvato in formato TXT. Il file può avere i seguenti contenuti: ["<sorgente aggiornamenti>"] [/R[A]:<file di rapporto>].

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.

Sintassi del comando

```
ROLLBACK [/R[A]:<file del rapporto>]
```

Salvataggio degli eventi in una modalità file di rapporto (solo per i profili di Scansione, Updater e Rollback)

```
/R:<file di rapporto>
```

Salva solo gli eventi critici nel file di rapporto.

```
/RA:<file di rapporto>
```

Salva tutti gli eventi in un file di rapporto.

Esempio:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Tracciamento

Abilitare o disabilitare il 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\Traces. Per impostazione predefinita il tracciamento è disabilitato.

Sintassi del comando

```
TRACES on|off [<livello di traccia>] [<impostazioni avanzate>]
```

Livello di traccia

<livello di traccia>

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 <code>dbg</code> , <code>file</code> e <code>mem</code> .
dbg	Utilizzare la funzione <code>OutputDebugString</code> e salvare il file di traccia. La funzione <code>OutputDebugString</code> invia una stringa di caratteri al debugger dell'applicazione da mostrare sullo schermo. Per i dettagli, visitare il sito Web MSDN .
file	Salva un file di traccia (nessun limite di dimensioni).
rot	Salva le tracce in un numero limitato 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.

Esempi:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Avvio del profilo

Avvia il profilo (ad esempio per aggiornare i database o abilitare un componente di protezione).

Sintassi del comando

```
START <profilo> [/R[A]:<file del rapporto>]
```

Profilo	
<profilo>	Nome del profilo. Un <i>Profilo</i> è un componente, un'attività o una funzionalità di Kaspersky Endpoint Security. È possibile visualizzare l'elenco dei profili disponibili eseguendo il comando <code>HELP START</code> .

Salvataggio degli eventi in una modalità file di rapporto (solo per i profili di Scansione, Updater e Rollback)

/R:<file di rapporto>	Salva solo gli eventi critici nel file di rapporto.
/RA:<file di rapporto>	Salva tutti gli eventi in un file di rapporto.

Esempio:
avp.com START Scan_Objects

STOP. Arresto di un profilo

Interrompi il profilo in esecuzione (ad esempio interrompi la scansione, interrompi la scansione delle unità rimovibili o disabilita un componente di 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**.

Sintassi del comando

```
STOP <profilo> /login=<nome utente> /password=<password>
```

Profilo	
<profilo>	Nome del profilo. Un <i>Profilo</i> 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=<nome utente> /password=<password>	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

STATUS. Stato del profilo

Mostra informazioni sullo stato per i [profili delle applicazioni](#) (ad esempio `in esecuzione` o `completato`). 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.

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

Visualizza informazioni statistiche su 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`.

Sintassi del comando

```
STATISTICS <profilo>
```

RESTORE. Ripristino di file da Backup

È possibile ripristinare 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\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.

Sintassi del comando

```
RESTORE [/REPLACE] <nome del file> /login=<nome utente> /password=<password>
```

Impostazioni avanzate	
/REPLACE	Sovrascrivi un file esistente.
<nome del file>	Il nome del file da ripristinare.

Autenticazione	
/login=<nome utente> /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=!Password1
```

EXPORT. Esportazione delle impostazioni dell'applicazione

Esportare le impostazioni di Kaspersky Endpoint Security in un file. Il file sarà posizionato nella cartella C:\Windows\SysWOW64.

Sintassi del comando

```
EXPORT <profilo> <nome file>
```

Profilo	
<profilo>	Nome del profilo. Un <i>Profilo</i> è un componente, un'attività o una funzionalità di Kaspersky Endpoint Security. È possibile visualizzare l'elenco dei profili disponibili eseguendo il comando <code>HELP EXPORT</code> .

File da esportare	
<nome del file>	Il nome del file nel quale verranno esportate le impostazioni dell'applicazione. 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.

Esempi:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Importazione delle impostazioni dell'applicazione

Importa le impostazioni per Kaspersky Endpoint Security da un file creato con il comando `EXPORT`.

Per eseguire questo comando, [Protezione tramite password deve essere abilitato](#). L'utente deve disporre dell'autorizzazione **Configura le impostazioni dell'applicazione**.

Sintassi del comando

```
IMPORT <nome del file> /login=<nome utente> /password=<password>
```

File da importare	
<nome del file>	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=<nome utente> /password=<password>	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Applicazione di un file chiave

Applica il file chiave per attivare Kaspersky Endpoint Security. Se l'applicazione è già attivata, la chiave verrà aggiunta come chiave di riserva.

Sintassi del comando

```
ADDKEY <nome del file> /login=<nome utente> /password=<password>
```

File chiave	
<nome del file>	Nome file chiave.

Autenticazione	
/login=<nome utente> /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

Eseguire le operazioni con le chiavi di licenza di Kaspersky Endpoint Security o con le chiavi di 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**.

Sintassi del comando

```
avp.com LICENSE <operazione> [/login=<nome utente> /password=<password>]
```

Operazione	
/ADD <nome del file>	Applica il file chiave per attivare Kaspersky Endpoint Security. Se l'applicazione è già attivata, la chiave verrà aggiunta come chiave di riserva.

<code>/ADD <codice di attivazione></code>	Attiva Kaspersky Endpoint Security tramite un codice di attivazione. Se l'applicazione è già attivata, la chiave verrà aggiunta come chiave di riserva.
<code>/REFRESH</code>	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.
<code>/REFRESH EDR</code>	Aggiorna lo stato della licenza del componente aggiuntivo Kaspersky Endpoint Detection and Response. Di conseguenza, l'applicazione riceve informazioni aggiornate sullo stato della licenza dai server di attivazione di Kaspersky.
<code>/DEL /login=<nome utente> /password=<password></code>	Rimuove la chiave di licenza dell'applicazione. Verrà rimossa anche la chiave di riserva.
<code>/DEL EDR /login=<nome utente> /password=<password></code>	Rimuove la chiave di licenza del componente aggiuntivo Kaspersky Endpoint Detection and Response. Verrà rimossa anche la chiave di riserva.

Autenticazione	
<code>/login=<nome utente> /password=<password></code>	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio:

- `avp.com LICENSE /ADD file.key`
- `avp.com LICENSE /ADD AAAAAA-BBBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL EDR /login=KLAdmin /password=!Password1`

RENEW. Acquisto di una licenza

Aprire il sito Web Kaspersky per acquistare o rinnovare la licenza.

PBATESTRESET. Ripristinare i risultati del controllo del disco prima di criptare il disco

Ripristinare i 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.

EXIT. Chiudi l'applicazione

Chiude Kaspersky Endpoint Security. L'applicazione verrà scaricata dalla RAM del computer.

Per eseguire questo comando, [Protezione tramite password deve essere abilitato](#). L'utente deve disporre dell'autorizzazione **Chiudi l'applicazione**.

Sintassi del comando

```
EXIT /login=<nome utente> /password=<password>
```

EXITPOLICY. Disabilitazione del criterio

Disabilita 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 disporre dell'autorizzazione **Disabilita il criterio di Kaspersky Security Center**.

Sintassi del comando

```
EXITPOLICY /login=<nome utente> /password=<password>
```

STARTPOLICY. Abilitazione del criterio

Abilita un criterio di Kaspersky Security Center nel computer. Le impostazioni dell'applicazione verranno configurate in base al criterio.

DISABLE. Disabilitazione della protezione

Disabilita 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.

SPYWARE. Rilevamento spyware

Abilita/disabilita il rilevamento spyware. Rilevamento spyware è abilitato per impostazione predefinita.

Sintassi del comando

```
SPYWARE on|off
```

KSN. Transizione KSN Globale/Privato

Selezione di una soluzione Kaspersky Security Network per determinare la reputazione di file o siti Web. Kaspersky Endpoint Security supporta le seguenti soluzioni infrastrutturali KSN:

- *KSN Globale* è la soluzione utilizzata dalla maggior parte delle applicazioni Kaspersky. I partecipanti KSN ricevono le informazioni da Kaspersky Security Network 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 di Kaspersky Security Network.
- *KSN Privato* 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 Security Network e ad altri dati statistici senza inviare dati a KSN dai propri computer. KSN Privato 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.

Sintassi del comando

```
KSN /global | /private <nome file>
```

File di configurazione KSN Privato	
<nome del file>	Nome del file di configurazione contenente le impostazioni del server proxy KSN. Questo file ha l'estensione PKCS7 o PEM.

Esempio:

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

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 scansioni virus e aggiornamenti del database.

È possibile visualizzare l'elenco dei comandi KESCLI utilizzando il comando `--help` o il comando abbreviato `-h`.

Per gestire Kaspersky Endpoint Security dalla riga di comando:

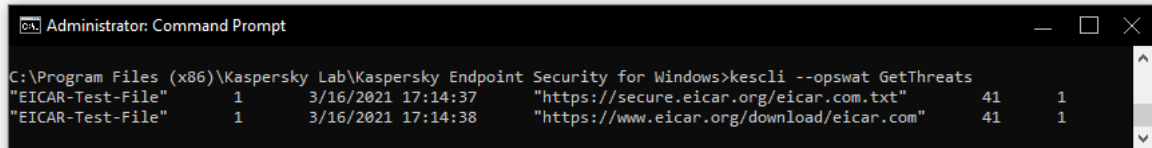
1. Eseguire l'interprete della riga di comando (cmd.exe) come amministratore.

2. Passare alla cartella in cui si trova il file eseguibile di Kaspersky Endpoint Security.

3. Per eseguire un comando immettere:

```
kescli <comando> [opzioni]
```

In seguito a questa operazione, Kaspersky Endpoint Security eseguirà il comando (vedere la figura seguente).



```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Gestione dell'applicazione dalla riga di comando

Scan. Scansione virus

Eseguire l'attività di scansione virus.

Per eseguire l'attività, per l'amministratore deve essere selezionato [Consenti utilizzo delle attività locali](#).

Sintassi del comando

```
kescli --opswat Scan "<ambito della scansione>" <azione se viene rilevata una minaccia>
```

È possibile controllare lo stato di completamento dell'attività *Scansione completa* utilizzando il comando [GetScanState](#) e visualizzare la data e l'ora dell'ultimo completamento della scansione tramite il comando [GetLastScanTime](#).

Ambito della scansione	
<file da esaminare>	Elenco di file e cartelle separato da ;. Ad esempio, "C:\Programmi (x86)\Cartella di esempio".

Azione se viene rilevata una minaccia	
0	Avvisa. 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, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati. 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

Ricevere informazioni sullo stato del completamento dell'attività *Scansione completa*:

- 1 – la scansione è in corso.
- 0 – la scansione non è in esecuzione.

Sintassi del comando

```
--opswat GetScanState
```

Esempio:

```
kescli --opswat GetScanState
```

GetLastScanTime. Definizione del tempo di completamento della scansione

Ricevere informazioni su data e ora dell'ultimo completamento dell'attività *Scansione completa*.

Sintassi del comando

```
kescli --opswat GetLastScanTime
```

GetThreats. Ottenimento dei dati sulle minacce rilevate

Ricevere 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.

Sintassi del comando

```
--opswat GetThreats
```

Quando questo comando viene eseguito, Kaspersky Endpoint Security invierà una risposta nel seguente formato:

```
<nome dell'oggetto rilevato> <tipo di oggetto> <data e ora del rilevamento> <percorso del file> <azione se viene rilevata una minaccia> <livello di pericolosità della minaccia>
```

```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Gestione dell'applicazione dalla riga di comando

Tipo di oggetto	
0	Non noto (Sconosciuto).
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 (Compressi).
20	Oggetti sconosciuti (Xfiles).
21	Applicazioni note (Software).
22	File nascosti (Nascosti).
23	Applicazioni che richiedono attenzione (Pupware).
24	Comportamento anomalo (Anomalia).
30	Non determinato (Non rilevato).
40	Banner pubblicitari (Banner).
50	Attacco di rete (Attacco).
51	Accesso al Registro di sistema (Registro di sistema).
52	Attività sospette (Sospetto).
60	Vulnerabilità (Vulnerabilità).
70	Phishing.
80	Allegato di posta elettronica indesiderato (Allegato).
90	Malware rilevato da Kaspersky Security Network (Urgente).
100	Collegamento sconosciuto (URL sospetta).
110	Altro malware (Comportamentale).

Azione se viene rilevata una minaccia	
0	Non noto (sconosciuto).

1	La minaccia è stata risolta (ok).
2	L'oggetto è stato infettato e non è stato disinfettato (infetto).
5	L'oggetto si trova in un archivio e non è stato disinfettato (archivio).
9	L'oggetto è stato disinfettato (disinfettato).
10	L'oggetto non è stato disinfettato (non disinfettato).
11	L'oggetto è stato eliminato (eliminato).
13	È stata creata una copia di backup dell'oggetto (sottoposto a backup).
15	L'oggetto è stato spostato in Backup (in quarantena).
23	L'oggetto è stato eliminato al riavvio del computer (elimina al riavvio).
25	L'oggetto è stato disinfettato al riavvio del computer (disinfetta al riavvio).
29	L'oggetto è stato spostato in Backup da un utente (aggiunto dall'utente).
30	L'oggetto è stato aggiunto alle esclusioni (aggiunto alle esclusioni).
31	L'oggetto è stato spostato in Backup al riavvio del computer (metti in quarantena al riavvio).
36	Falso positivo (falso allarme).
38	Il processo è stato terminato (terminato).
40	L'oggetto non è stato rilevato (non trovato).
41	Impossibile risolvere la minaccia (non trattabile).
42	L'oggetto è stato ripristinato (sottoposto a rollback).
43	L'oggetto è stato creato a seguito dell'attività di una minaccia (prodotto dalla minaccia).
44	L'oggetto è stato ripristinato al riavvio del computer (rollback al riavvio).
0xffffffff	L'oggetto non è stato elaborato (ignorato).

Livello di pericolosità della minaccia	
0	Sconosciuto
1	Alto
2	Media
4	Basso
8	Info (inferiore a <i>Basso</i>)

UpdateDefinitions. Aggiornamento di database e moduli software dell'applicazione

Eseguire l'attività *Aggiornamento*. Kaspersky Endpoint Security utilizza l'origine predefinita: i server degli aggiornamenti di Kaspersky.

Per eseguire l'attività, per l'amministratore deve essere selezionato [Consenti utilizzo delle attività locali](#).

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. Definizione del tempo di completamento dell'aggiornamento


Ricevi informazioni sulla data e l'ora di rilascio dei database antivirus in uso.

Sintassi del comando

```
kescli --opswat GetDefinitionState
```

EnableRTP. Abilitazione della protezione

Abilitare i componenti della protezione 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).

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

Ricevere informazioni sullo stato operativo del componente Protezione minacce file:

- 1 – il componente è abilitato.

- 0 – il componente è disabilitato.

Sintassi del comando

```
kescli --opswat GetRealTimeProtectionState
```

Versione. Identificazione della versione dell'applicazione

Identificare la versione di Kaspersky Endpoint Security for Windows.

Sintassi del comando

```
--Version
```

È inoltre possibile utilizzare il comando abbreviato `-v`.

Esempio:
`kescli -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 <comando>`.

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. Per eseguire un comando immettere:

```
avp.com <comando> [options]
```

In seguito a questa operazione, Kaspersky Endpoint Security eseguirà il comando (vedere la figura seguente).

SANDBOX. Gestione di Kaspersky Sandbox

Comandi per la gestione del componente Kaspersky Sandbox:

- Abilitare o disabilitare il componente Kaspersky Sandbox.

Il componente Kaspersky Sandbox consente l'interoperabilità con la soluzione Kaspersky Sandbox.

- Configurare il componente Kaspersky Sandbox:

- Connettere il computer ai server di Kaspersky 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 ulteriori dettagli sulla distribuzione di immagini virtuali e sulla configurazione dei server di Kaspersky Sandbox, consultare la [Guida di Kaspersky Sandbox](#).

- Configurare il timeout della connessione per il server Kaspersky Sandbox.

Timeout per la ricezione di una risposta a una richiesta di scansione di oggetti dal server di Kaspersky Sandbox. Allo scadere del timeout, Kaspersky Sandbox reindirizza la richiesta al server successivo. Il valore di timeout dipende dalla velocità e dalla stabilità della connessione. Il valore predefinito è 5 secondi.

- Configurare una connessione attendibile tra il computer e i server di Kaspersky Sandbox.

Per configurare una connessione attendibile con i server di Kaspersky Sandbox, è necessario preparare un certificato TLS. Successivamente, è necessario aggiungere il certificato ai server di Kaspersky Sandbox e al criterio di Kaspersky Endpoint Security. Per ulteriori dettagli sulla preparazione del certificato e sull'aggiunta del certificato ai server, consultare la [Guida di Kaspersky Sandbox](#).

- Mostra le impostazioni correnti del componente.

Sintassi del comando

```
stop sandbox [/login=<nome utente> /password=<password>]
start sandbox
sandbox /set [--tls=yes|no] [--servers=<indirizzo del server>:<port>] [--timeout=
<Timeout della connessione al server di Kaspersky Sandbox (ms)>] [--pinned-
certificate=<percorso del certificato TLS>][/login=<nome utente> /password=<password>]
sandbox /show
```

Operazione	
stop	Disabilitare il componente Kaspersky Sandbox.
start	Abilitare il componente Kaspersky Sandbox.
set	Configurare il componente Kaspersky Sandbox. Non è possibile modificare le seguenti impostazioni: <ul style="list-style-type: none">• Utilizzare una connessione attendibile (--tls).• Aggiungere un certificato TLS (--pinned-certificate).• Impostare il timeout della connessione al server di Kaspersky Sandbox (--timeout).• Aggiungere i server di Kaspersky Sandbox (--server).
show	Mostra le impostazioni correnti del componente. Si riceve la seguente risposta: sandbox.timeout=<Timeout della connessione al server di Kaspersky Sandbox (ms)> sandbox.tls=<stato connessione attendibile> sandbox.servers=<elenco dei server di Kaspersky Sandbox>

Autenticazione	
/login=<nome utente> /password=<password>	Credenziali dell'account utente con le autorizzazioni di Protezione tramite password richieste.

Esempio:

```
avp.com start sandbox
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"
avp.com sandbox /set --servers=10.10.111.0:147
```

PREVENZIONE. Gestione della prevenzione dell'esecuzione

Disabilitare Prevenzione dell'esecuzione o mostrare le impostazioni del componente corrente, incluso l'elenco delle regole di prevenzione dell'esecuzione.

Sintassi del comando

```
prevention disable
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: <ID regola>
```

```
target: script|process|document
```

```
md5: <hash MD5 del file>
```

```
sha256: <hash SHA256 del file>
```

```
pattern: <percorso dell'oggetto>
```

```
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).

ISOLAMENTO. Gestione dell'isolamento di rete

Disattivare l'isolamento di rete del computer o visualizzare le impostazioni correnti del componente. Le impostazioni dei componenti includono anche un elenco di connessioni di rete aggiunte alle esclusioni.

Sintassi del comando:

```
isolation /OFF /login=<nome utente> /password=<password>  
isolation /STAT
```

Come risultato dell'esecuzione del comando `stat`, si riceverà la seguente risposta: `Network isolation on|off`.

RESTORE. Ripristino dei file dalla quarantena

È possibile ripristinare un file dalla Quarantena nella cartella originale. Se la cartella di destinazione è stata eliminata, l'applicazione inserisce il file in una cartella speciale nel computer. Quindi, è necessario spostare manualmente il file nella cartella di destinazione. *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 associato alle soluzioni Kaspersky Sandbox e Kaspersky Endpoint 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](#) e la [Guida di Kaspersky Endpoint Detection and Response Expert](#).

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).

Sintassi del comando

```
avp.com RESTORE [/REPLACE] <nome del file> /login=<nome utente> /password=<password>
```

Impostazioni avanzate	
/REPLACE	Sovrascrivi un file esistente.
<nome del file>	Il nome del file da ripristinare.

Autenticazione	
/login=<nome utente> /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=!Password1
```

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)

Eseguire l'attività Scansione indicatori di compromissione (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. Le attività di *scansione IOC* consentono di trovare indicatori di compromissione sul computer e di adottare misure di risposta alle minacce.

Sintassi del comando

```
IOCSCAN <percorso completo del file IOC> [/path=<percorso della cartella dei file IOC>
[/process=on|off] [/hint=<percorso completo del file eseguibile di un processo|percorso
completo del file>] [/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=<data di pubblicazione dell'evento>] [/channels=<elenco
dei canali>] [/files=on|off] [/drives=<all|system|critical|custom>] [/excludes=<elenco
delle esclusioni>] [/scope=<elenco delle cartelle da sottoporre a scansione>]
```

File IOC	
<percorso completo del file IOC>	<p>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.</p> <p>Ad esempio, C:\Utenti\Admin\Desktop\IOC\file1.ioc</p>
/path=<percorso della cartella con i file IOC>	<p>Percorso della cartella con i file IOC che si desidera utilizzare per la scansione. I <i>file IOC</i> 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.</p> <p>Ad esempio, C:\Utenti\Admin\Desktop\IOC</p>

Tipo di dati per la scansione IOC	
/process=on off	<p>Analizza i dati dei processi durante l'esecuzione della scansione IOC (termine ProcessItem).</p> <p>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).</p> <p>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.</p>
/hint=<percorso completo del file eseguibile del	<p>Analizza i dati dei file durante l'esecuzione della scansione IOC (termini ProcessItem e FileItem).</p>

<p>processo percorso completo del file></p>	<p>È possibile selezionare un file in uno dei seguenti modi:</p> <ul style="list-style-type: none"> • <percorso completo del file eseguibile del processo> - ProcessItem; • <percorso completo del file> - FileItem.
<p>/registry=on off</p>	<p>Analizza i dati del registro di sistema di Windows durante l'esecuzione di una scansione IOC (termine RegistryItem).</p> <p>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).</p> <p>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.</p> <p>Per il tipo di dati RegistryItem, Kaspersky Endpoint Security esamina una serie di chiavi del Registro di sistema.</p>
<p>/dnsentry=on off</p>	<p>Analizza i dati sui record nella cache DNS locale durante l'esecuzione della scansione IOC (termine DnsEntryItem).</p> <p>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).</p> <p>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.</p>
<p>/arpentry=on off</p>	<p>Analizza i dati sui record nella tabella ARP durante l'esecuzione della scansione IOC (termine ArpEntryItem).</p> <p>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).</p> <p>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.</p>
<p>/ports=on off</p>	<p>Analizza i dati sulle porte aperte per l'ascolto durante l'esecuzione della scansione IOC (termine PortItem).</p> <p>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).</p> <p>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.</p>
<p>/services=on off</p>	<p>Analizza i dati sui servizi installati nel dispositivo durante l'esecuzione della scansione IOC (termine ServiceItem).</p>

	<p>Se il valore dell'argomento è <code>off</code>, Kaspersky Endpoint Security non esegue la scansione dei dati sui servizi installati nel dispositivo. Se il file IOC contiene i termini del documento IOC Serviceltem, vengono ignorati (rilevati come nessuna corrispondenza).</p> <p>Se l'argomento non è specificato, Kaspersky Endpoint Security analizza i dati del servizio solo se il documento Serviceltem IOC è descritto nel file IOC specificato per la scansione.</p>
<code>/system=on off</code>	<p>Analizza i dati dell'ambiente durante l'esecuzione della scansione IOC (termine SystemInfoltem).</p> <p>Se il valore dell'argomento è <code>off</code>, Kaspersky Endpoint Security non analizza i dati dell'ambiente. Se il file IOC contiene i termini del documento IOC SystemInfoltem, vengono ignorati (rilevati come nessuna corrispondenza).</p> <p>Se l'argomento non è specificato, Kaspersky Endpoint Security analizza i dati dell'ambiente solo se il documento IOC SystemInfoltem è descritto nel file IOC specificato per la scansione.</p>
<code>/users=on off</code>	<p>Analizza i dati sugli utenti durante l'esecuzione della scansione IOC (termine UserItem).</p> <p>Se il valore dell'argomento è <code>off</code>, 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).</p> <p>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.</p>
<code>/volumes=on off</code>	<p>Analizza i dati sui volumi durante l'esecuzione della scansione IOC (termine Volumeltem).</p> <p>Se il valore dell'argomento è <code>off</code>, Kaspersky Endpoint Security non esegue la scansione dei dati sui volumi nel dispositivo. Se il file IOC contiene i termini del documento IOC Volumeltem, vengono ignorati (rilevati come nessuna corrispondenza).</p> <p>Se l'argomento non è specificato, Kaspersky Endpoint Security analizza i dati del volume solo se il documento IOC Volumeltem è descritto nel file IOC specificato per la scansione.</p>
<code>/eventlog=on off</code>	<p>Analizza i dati sui record nel registro eventi di Windows durante l'esecuzione della scansione IOC (termine EventLogItem).</p> <p>Se il valore dell'argomento è <code>off</code>, 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).</p> <p>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.</p>
<code>/datetime=<data di pubblicazione dell'evento></code>	<p>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.</p>

	<p>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.</p> <p>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.</p> <p>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.</p> <p>L'impostazione viene utilizzata solo se il documento IOC EventLogItem è descritto nel file IOC specificato per la scansione.</p>
<p>/Channel=<elenco dei canali></p>	<p>Elenco dei nomi dei canali (registro) per i quali si desidera eseguire una scansione IOC.</p> <p>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.</p> <p>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.</p> <p>Se l'argomento non è specificato, Kaspersky Endpoint Security esegue la scansione dei record per i canali Applicazione, Sistema, Sicurezza.</p>
<p>/files=on off</p>	<p>Analizza i dati del file durante l'esecuzione della scansione IOC (termine FileItem).</p> <p>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).</p> <p>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.</p>
<p>/drives= <all system critical custom></p>	<p>Imposta l'ambito della scansione IOC durante l'analisi dei dati per il documento IOC FileItem.</p> <p>È possibile impostare i seguenti valori per l'ambito della scansione:</p> <ul style="list-style-type: none"> • <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=<elenco delle cartelle da sottoporre a scansione>). <p>Se l'argomento non è specificato, la scansione viene eseguita per le aree critiche.</p>

<code>/excludes=<elenco delle esclusioni></code>	Imposta l'ambito di esclusione durante l'analisi dei dati per il documento IOC FileItem. È possibile specificare più percorsi separati da spazi.
<code>/scope=<elenco delle cartelle da sottoporre a scansione></code>	Ambito della scansione IOC definito dall'utente durante l'analisi dei dati per il documento IOC FileItem (<code>/drives=custom</code>). È possibile specificare più percorsi separati da spazi.

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 <code><ioc id=""></code>)
Nome	Descrizione del file IOC dall'intestazione della struttura del file IOC (il tag <code><description></description></code>)
Elementi degli indicatori abbinati	Elenco degli ID di tutti gli indicatori abbinati.
Oggetti abbinati	Dati per ogni documento IOC per cui è stata rilevata una corrispondenza.

MDRLICENSE. Attivazione MDR

Eseguire operazioni con il 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 .

Sintassi del comando

```
MDRLICENSE <operazione> [/login=<nome utente> /password=<password>]
```

Operazione	
<code>/ADD</code>	Applicare il file di configurazione BLOB per l'integrazione con Kaspersky Managed Detection

<nome del file>	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=<nome utente> /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=!Password1

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 **Errore: impossibile avviare l'attività 'EntAppControl'**. Kaspersky Endpoint Security può inoltre mostrare informazioni aggiuntive sotto forma di un codice, ad esempio **error=8947906D** (vedere la tabella seguente).

Codici di errore

Codice di errore	Descrizione
09479001	La chiave di licenza per Kaspersky Endpoint Security è già in uso in questo computer.
0947901D	La licenza è scaduta. L'aggiornamento dei database non è disponibile.
89479002	Chiave non trovata.
89479003	Firma digitale mancante o danneggiata.
89479004	Dati danneggiati.
89479005	File chiave danneggiato.
89479006	Licenza scaduta o chiave di licenza scaduta.
89479007	File chiave non specificato.
89479008	Impossibile applicare il file chiave.
89479009	Salvataggio dei dati non riuscito.
8947900A	Lettura dei 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 digitale del file non corrisponde alla firma digitale di Kaspersky.
89479015	Impossibile utilizzare una chiave per una licenza non commerciale come chiave per una licenza commerciale.
89479016	È necessaria la licenza beta per utilizzare la versione beta dell'applicazione.
89479017	File chiave non compatibile con questa applicazione.
89479018	Chiave bloccata da Kaspersky.
89479019	L'applicazione è già stata utilizzata con una licenza di prova. Impossibile aggiungere nuovamente la chiave di prova.
8947901A	File chiave 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	Errore nei dati del servizio chiavi di licenza.
89479023	Impossibile utilizzare un file chiave non valido per aggiungere una chiave di riserva.
89479025	Errore durante l'invio della richiesta al server di attivazione. Possibili motivi: errore di connessione a Internet o problemi temporanei sul server di attivazione. Provare ad attivare l'applicazione con il codice di attivazione in un secondo momento. Se l'errore persiste, contattare il proprio provider Internet.
89479026	Errore nella risposta dal server di attivazione.
89479027	Impossibile ottenere lo stato della risposta.
89479028	Errore di salvataggio del file temporaneo.
89479029	Il codice di attivazione è stato inserito in modo errato o la data di sistema è errata. Controllare la data di sistema nel computer.
8947902A	File chiave non compatibile con questa applicazione o la licenza è scaduta. Non è possibile attivare Kaspersky Endpoint Security utilizzando un file chiave per un'altra applicazione.
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	Il server di attivazione ha restituito l'errore 404.
89479030	Il server di attivazione ha restituito l'errore 405.
89479031	Il server di attivazione ha restituito l'errore 406.
89479032	Necessaria autenticazione sul server proxy. Controllare le opzioni di rete.

89479033	Timeout richiesta scaduto.
89479034	Il server di attivazione ha restituito l'errore 409.
89479035	Il server di attivazione ha restituito l'errore 410.
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 opzioni di rete.
8947903F	Servizio non disponibile (errore HTTP 503).
89479040	Il timeout per la risposta del gateway è scaduto. Controllare le opzioni 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 di conversione dei parametri in una stringa ANSI (URL, cartella, agente).
8947904A	Errore di 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.
89479053	La chiave di licenza è scaduta.
89479054	Data di sistema errata impostata nel computer.
89479055	La licenza di prova è scaduta.
89479056	La licenza è scaduta.
89479057	È stato superato il limite di attivazioni dell'applicazione per il codice specificato.
89479058	La procedura di attivazione si è conclusa con un errore di sistema.
89479059	Impossibile utilizzare una chiave per una licenza non commerciale 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. Controllare le impostazioni della connessione Internet e ritentare l'attivazione.
89479065	La data di rilascio dei database dell'applicazione supera la data di scadenza della licenza.
89479066	Impossibile sostituire la chiave attiva con una chiave scaduta.
89479067	Impossibile aggiungere una chiave di riserva se scade prima della licenza corrente.
89479068	Chiave di abbonamento aggiornata mancante.
8947906A	Codice di attivazione errato (checksum non corrispondente).
8947906B	La chiave è già attiva.
8947906C	I tipi di licenza relativi alle chiavi attiva e di riserva non corrispondono.
8947906D	Componente non supportato dalla licenza.
8947906E	Impossibile aggiungere una chiave di abbonamento come chiave di riserva.
89479213	Errore generico del livello di trasporto.
89479214	Impossibile connettersi al server di attivazione.
89479215	Formato dell'URL non valido.
89479216	Impossibile convertire l'indirizzo del server proxy.
89479217	Impossibile convertire l'indirizzo del server. Controllare le impostazioni della connessione Internet.
89479218	Impossibile connettersi al server di attivazione o al server proxy.
89479219	Accesso remoto negato.
8947921A	Il timeout per la risposta è scaduto.
8947921B	Errore durante l'invio della richiesta HTTP.
8947921C	Errore di connessione SSL.
8947921D	Operazione interrotta da callback.
8947921E	Troppi tentativi di inoltro.
8947921F	Controllo del destinatario non riuscito.
89479220	Risposta vuota dal server di attivazione.
89479221	Errore durante l'invio dei dati.
89479222	Errore durante la ricezione dei dati.
89479223	Errore del certificato SSL locale.
89479224	Errore di criptaggio SSL.
89479225	Errore del certificato SSL del server.
89479226	Contenuto non valido del pacchetto di rete.
89479227	Accesso utente negato.
89479228	File di certificato SSL non valido.
89479229	Impossibile stabilire la connessione SSL.

8947922A	Impossibile inviare o ricevere il pacchetto di rete. Riprovare più tardi.
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	Non è disponibile alcuna chiave di licenza per il codice di attivazione immesso.
89479404	Chiave attiva bloccata.
89479405	Parametri obbligatori della richiesta di attivazione dell'applicazione mancanti.
89479406	Nome utente o password non validi.
89479407	Codice di attivazione errato inviato al server.
89479408	Il codice di attivazione non è valido per Kaspersky Endpoint Security. Non è possibile attivare Kaspersky Endpoint Security utilizzando un file chiave per un'applicazione sconosciuta.
89479409	Nella richiesta manca un codice di attivazione.
8947940B	Licenza scaduta (secondo i dati del server di attivazione).
8947940C	È stato superato il numero massimo di attivazioni consentite per il codice specificato.
8947940D	ID richiesta in formato non valido.
8947940E	Il codice di attivazione non è valido per Kaspersky Endpoint Security. Il codice di attivazione è destinato a un'altra applicazione Kaspersky.
8947940F	Impossibile aggiornare la chiave di licenza.
89479410	Codice di attivazione non valido per questa regione.
89479411	Il codice di attivazione non è valido per la versione della lingua di Kaspersky Endpoint Security.
89479412	È richiesto un ulteriore accesso al server di attivazione.
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	Formato del codice di attivazione non supportato dal server di attivazione.
89479418	Codice di attivazione in formato non valido.
89479419	Ora di sistema errata impostata nel computer.
8947941A	Il codice di attivazione non è valido per la versione di Kaspersky Endpoint Security.
8947941B	Abbonamento scaduto.
8947941C	Numero di attivazioni superato per questa chiave di licenza.
8947941D	Firma digitale della chiave di licenza non valida.
8947941E	Sono necessari ulteriori dati.
8947941F	Verifica dei dati dell'utente non riuscita.
89479420	Abbonamento inattivo.

89479421	Il server di attivazione è in fase di manutenzione.
89479501	Errore sconosciuto di Kaspersky Endpoint Security.
89479502	È stato trasferito un parametro non valido (ad esempio un elenco vuoto di indirizzi di server di attivazione).
89479503	Codice di attivazione errato.
89479504	Nome utente non valido.
89479505	Password utente non valida.
89479506	Risposta non valida dal server di attivazione.
89479507	Richiesta di attivazione 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`, `EXPORT` e `IMPORT`. 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.
- `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.
- `Mail_Monitoring` o `EM` – Protezione minacce di posta.
- `Rollback` – Rollback dell'aggiornamento.
- `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 – Aggiornamento.
- 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 terze parti. 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 terze parti 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=<Nome utente>

Nome utente per la gestione dell'applicazione mediante REST API. Immettere il nome utente nel formato <DOMINIO>\<Nome utente> (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=<Porta>

Porta utilizzata per lo scambio dei dati. Parametro opzionale. La porta 6782 è selezionata per impostazione predefinita.

- RESTAPI_Certificate=<Percorso del certificato>

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 del Registro di sistema che contiene le impostazioni della REST API:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\Rest

3. Immettere il percorso del certificato, ad esempio Certificato = C:\Cartella\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

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 nella community degli utenti

Se la domanda non richiede una risposta urgente, è possibile sottoporla agli esperti di Kaspersky e ad altri utenti nella [community](#).

Nella Community 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\Traces.

I file di traccia vengono denominati come segue: KES<numero versione servizio_dateXX.XX_timeXX.XX_pidXXX.><tipo di file di traccia>.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.

Kaspersky Endpoint Security salva le password degli utenti in un file di traccia solo in formato criptato.

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 vengono denominati come segue: KES<numero versione_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 `shelllex.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 `Programmi\Kaspersky Lab\Kaspersky Security Center Web Console\log`.

I file di traccia del plug-in Web dell'applicazione vengono denominati come segue: `logs-kes_windows-<tipo di file di traccia>.DESKTOP-<data dell'aggiornamento file>.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 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 sono verificati durante l'esecuzione dell'applicazione.

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 tracce 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 rotazione**. 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 il numero massimo di file per la rotazione e la dimensione massima per ogni file.
 - **Scrivi in un singolo file**. Salva un file di traccia (nessun limite di dimensioni).
5. Nell'elenco a discesa **Livello** selezionare il livello di traccia:

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 (500)**.
6. Riavviare Kaspersky Endpoint Security.
7. 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\Traces viene creato un file di traccia delle prestazioni. Dopo la creazione del file di traccia, inviare il 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 tracce 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 rotazione**. 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.
 - **Scrivi in un singolo file**. Salva un file di traccia (nessun limite di dimensioni).
5. Nell'elenco a discesa **Livello** selezionare il livello di traccia:
 - **Light**. 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 assistenza** e disabilitare il tracciamento.

Di conseguenza, nella cartella %ProgramData%\Kaspersky Lab\KES\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\Traces.

Per abilitare o disabilitare la scrittura di dump:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
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.

Per abilitare e disabilitare la protezione dei file di dump e di traccia:

1. Nella finestra principale dell'applicazione, fare clic sul pulsante .
2. Nella finestra delle impostazioni dell'applicazione, selezionare **Impostazioni generali** → **Impostazioni applicazione**.
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.

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 tenta di installare una qualsiasi versione del modulo di criptaggio AES in un computer in cui è installato Kaspersky Endpoint Security for Windows 11.9.0 ma non sono installati componenti di criptaggio, l'installazione del modulo di criptaggio terminerà con un messaggio di errore che indica che è installata una versione più recente dell'applicazione. A partire da Kaspersky Endpoint Security 10 for Windows Service Pack 2 (versione 10.3.0.6294), non è disponibile un file di installazione separato per il modulo di criptaggio. Le librerie di criptaggio sono incluse nel pacchetto di distribuzione dell'applicazione. Kaspersky Endpoint Security 11.9.0 non è compatibile con i moduli di criptaggio AES. Le librerie necessarie per il criptaggio vengono installate automaticamente quando viene selezionato il componente Criptaggio dell'intero disco o Criptaggio a livello di file.
- 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 dell'applicazione, avviare il ripristino dopo il riavvio del computer.
- 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](#) ².
- 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.
- 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.

[Upgrade dell'applicazione](#) ²

- Quando si esegue l'upgrade da Kaspersky Endpoint Security 10 Service Pack 2 for Windows (build 10.3.0.6294), il [componente Prevenzione Intrusioni Host viene attivato](#).
- Durante l'aggiornamento di Kaspersky Endpoint Security 10 for Windows Service Pack 2 (build 10.3.0.6294), i file che sono stati collocati in Backup o Quarantena nella versione precedente dell'applicazione verranno trasferiti in Backup nella nuova versione dell'applicazione. Questi file non vengono trasferiti per le versioni precedenti a Kaspersky Endpoint Security 10 for Windows Service Pack 2 (build 10.3.0.6294). Per salvarli, è necessario ripristinare i file da Quarantena e Backup prima di eseguire l'upgrade dell'applicazione. Al termine dell'upgrade, eseguire nuovamente la scansione dei file ripristinati.
- 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*, *Scansione delle Aree Critiche*, *Scansione Personalizzata* e *Controllo integrità* 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](#) .
- Se si esegue l'upgrade di una versione precedente dell'applicazione alla versione 11.9.0, per installare Kaspersky Endpoint Agent riavviare il computer e accedere al sistema utilizzando un account con diritti di amministratore locale. In caso contrario, Kaspersky Endpoint Agent non verrà installato durante la procedura di upgrade.
- Se si esegue l'upgrade di Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 4 con il componente Criptaggio a livello di file (FLE) installato nei computer che eseguono Windows 10 versione 1809, 1903 e 1909, i driver FDE non verranno installati nell'immagine WinRE.
- 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 *I server KSN non sono 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 dell'applicazione dalle versioni precedenti a Kaspersky Endpoint Security 11 for Windows, il computer deve essere riavviato.

- 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 virus funziona correttamente.
 - Dopo l'avvio del controllo anti-virus del server, 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.
- La modalità 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 preavviso. 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.
- Le sessioni multiple di Windows 10 Enterprise sono supportate con limitazioni:
 - Kaspersky Endpoint Security disinfecta 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\**\*"
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.

Compatibilità con Kaspersky Security Center

- È possibile gestire il componente Controllo adattivo delle anomalie solo in Kaspersky Security Center 11 o versione successiva.
- Il rapporto sulle minacce di Kaspersky Security Center 11 potrebbe non visualizzare le informazioni sull'azione eseguita sulle minacce rilevate da Protezione AMSI.
- Lo stato operativo dei componenti Protezione AMSI e Controllo adattivo delle anomalie è disponibile solo in Kaspersky Security Center 11 o versione successiva. È possibile visualizzare lo stato operativo in Kaspersky Security Center Console all'interno delle proprietà del computer, nella sezione **Attività**. I rapporti per questi componenti sono disponibili solo in Kaspersky Security Center 11 o versione successiva.

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.
- Non è possibile attivare l'applicazione tramite abbonamento utilizzando Kaspersky Security Center se la licenza è scaduta o se nel computer è attiva una licenza di prova. Per sostituire una licenza di prova o una licenza in scadenza con una licenza in abbonamento, [utilizzare l'attività di distribuzione delle licenze](#).
- 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. Questo avviene perché l'applicazione prima installa e tenta di attivare la licenza di prova integrata, che richiede l'accesso a Internet per l'attivazione durante la procedura di installazione.
- 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. Questo avviene perché l'applicazione installa nuovamente e tenta di attivare la licenza di prova integrata, che richiede l'accesso a Internet per l'attivazione durante l'installazione di un upgrade.
- 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 11.9.0, 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.

Motore di Remediation

- L'applicazione ripristina i file solo nei dispositivi con file system NTFS o FAT32.
- L'applicazione può ripristinare i file con le seguenti estensioni: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls,xlsx, xlsx, xslm, xlsx, xlsx, xlsx, xlsx, xlsx, 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, srf, 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.
- L'applicazione non monitora le modifiche apportate ai file tramite un'interfaccia di rete (se ad esempio un file è archiviato in una cartella condivisa e un processo viene avviato in remoto da un altro computer).

Firewall

- Il filtro di pacchetti o connessioni per indirizzo locale, interfaccia fisica e TTL (Time-To-Live) del pacchetto è supportato nei seguenti casi:
 - In 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.
- Nelle versioni dell'applicazione 11.0.0 e 11.0.1 gli indirizzi MAC definiti vengono applicati in modo errato. Le impostazioni dell'indirizzo MAC per le versioni 11.0.0, 11.0.1 e 11.1.0 o successive non sono compatibili. Dopo l'upgrade dell'applicazione o del plug-in da queste versioni alla versione 11.1.0 o successiva, è necessario verificare e riconfigurare gli indirizzi MAC definiti nelle regole Firewall.
- Quando si esegue l'upgrade dell'applicazione dalle versioni 11.1.1 e 11.2.0 alla versione 11.9.0, non viene eseguita la migrazione degli stati delle autorizzazioni per le seguenti regole Firewall:
 - Richieste al server DNS su TCP.
 - Richieste al server DNS su UDP.
 - Qualsiasi attività di rete.
 - Risposte destinazione irraggiungibile ICMP in entrata.
 - Flusso ICMP in entrata.
- 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.

[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](#).

[Controllo applicazioni](#)

- Solo gli archivi ZIP inferiori a 104 MB sono supportati durante la gestione delle 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 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.
- 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 Blocco note Metro, ubicato nella cartella C:\Programmi\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.

Controllo dispositivi

- 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.

Controllo Web

- I formati OGV e WEBM non sono supportati.
- Il protocollo RTMP non è supportato.

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.
- [Non è possibile generare un rapporto di Controllo adattivo delle anomalie](#) 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](#).

Crittografia unità (FDE)

- 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.
- Per informazioni dettagliate sul ripristino di un sistema operativo da una copia di backup a un dispositivo GPT criptato, visitare la [Knowledge Base dell'Assistenza tecnica](#).
- In un computer criptato non possono coesistere più agenti di download.
- 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 <dominio>/<nome account windows>, 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 Andrea nel computer Andrea e che sia stato creato un account dell'Agente di Autenticazione con il nome Andrea/Andrea per questo utente. Se il nome del computer Andrea è stato modificato in Andrea-PC, è necessario modificare il nome dell'account dell'Agente di Autenticazione per l'utente Andrea da Andrea/Andrea a Andrea-PC/Andrea. 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 Andrea/Andrea).
- 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](#) ².

[Criptaggio a livello di file \(FLE\)](#) ²

- Il criptaggio di file e cartelle non è supportato nei sistemi operativi della famiglia Microsoft Windows Embedded.
- Dopo aver installato l'applicazione, è necessario riavviare il sistema operativo affinché il criptaggio di file e cartelle funzioni correttamente.
- 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.
- 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 Cache sul lato client non è supportata. 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. Per i dettagli relativi al supporto per Cache sul lato client quando si utilizza il criptaggio, fare riferimento alla [Knowledge Base dell'Assistenza tecnica](#).
- [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](#).
- Dopo aver aggiornato Kaspersky Endpoint Security for Windows versione 11.0.1 o precedente, per accedere ai file criptati dopo aver riavviato il computer, assicurarsi che Network Agent sia in esecuzione. Network Agent ha un avvio ritardato, quindi non è possibile accedere ai file criptati subito dopo il caricamento del sistema operativo. Non è necessario attendere l'avvio di Network Agent dopo il successivo avvio del computer.

[Altre limitazioni](#)

- 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.
- Controllo sistema. Le informazioni complete sui processi non vengono visualizzate.
- 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 la scansione della posta con l'[estensione Protezione minacce di posta per Microsoft Outlook](#), è consigliabile utilizzare la Modalità cache (l'opzione Usa modalità cache).
- [L'attività Scansione virus](#) non supporta la versione a 64 bit di Microsoft Outlook. Di conseguenza, Kaspersky Endpoint Security non esegue la scansione dei file MS Outlook (file PST e OST) se nel computer è installata una versione a 64 bit di MS Outlook, anche se la [posta è inclusa nell'ambito della scansione](#).
- In Kaspersky Security Center, quando si passa dall'utilizzo di Kaspersky Security Network globale all'utilizzo di Kaspersky Security Network 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.

- 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 componente [Sensore Endpoint](#) non può essere installato in Microsoft Windows Server 2008.
- 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 un 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 modalità provvisoria.
- Per garantire il corretto funzionamento di Kaspersky Endpoint Security for Windows versioni 11.5.0 e 11.6.0 con il software Cisco AnyConnect, è necessario installare il modulo di conformità versione 4.3.183.2048 o successive. Ulteriori informazioni sulla compatibilità con Cisco Identity Services Engine sono disponibili nella [documentazione di Cisco](#).
- 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.
- L'attività di controllo della disponibilità di KSN non è più supportata.
- 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:\cartella1\cartella2, la scansione verrà eseguita per il percorso C:\cartella1\.
- Quando si esegue l'upgrade dell'applicazione dalla versione 11.1.0 alla 11.9.0, vengono ripristinati i valori predefiniti delle impostazioni di Protezione AMSI.
- Se si utilizzano criteri restrizione software (SRP, Software Restriction Policies), il computer potrebbe avere difficoltà di caricamento (schermo nero). È consigliabile modificare le impostazioni SRP come segue: impostare il valore **Tutti i file nel software tranne le librerie (ad esempio, le DLL)** per il parametro **Applica criteri restrizione software ai seguenti oggetti** e aggiungere regole con il livello di sicurezza **Senza restrizioni** per i percorsi dei file dell'applicazione (C:\Programmi\Common Files\Kaspersky Lab e C:\Programmi\Kaspersky Lab). Per informazioni dettagliate sull'utilizzo di SRP, fare riferimento alla [documentazione di Microsoft](#).
- Se il computer appartiene a un dominio nell'oggetto Criteri di gruppo (GPO) di Windows con il parametro DriverLoadPolicy impostato su 8 (solo Buono), il riavvio del computer con Kaspersky Endpoint Security installato causa un BSOD. Per evitare un errore, il parametro Antimalware ad avvio anticipato (ELAM) in Criteri di gruppo deve essere impostato su 1 (Buono e sconosciuto). Le impostazioni ELAM si trovano nel criterio in: **Configurazione computer** → **Modelli amministrativi** → **Sistema** → **Antimalware ad avvio anticipato**.
- 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.
- Non è possibile eseguire la scansione di un oggetto inserito in Quarantena a causa dell'attività [Spostare un file in Quarantena](#).
- 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`.
- 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 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.
- Non è possibile spostare in Quarantena un flusso di dati alternativo (ADS, Alternate Data Stream) di dimensioni superiori ai 4 MB. Kaspersky Endpoint Security ignora qualsiasi ADS di queste dimensioni senza avvisare l'utente.
- 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.
- 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).
- 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.
 - 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.
- 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.

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, Aggiornamento database.

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 aggiuntiva

Chiave che certifica il diritto di utilizzare l'applicazione, ma che non è attualmente in uso.

Chiave attiva

Chiave attualmente utilizzata dall'applicazione.

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.

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 l'estensione TXT situati nella cartella denominata `Cartella` e nelle relative sottocartelle. 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 `Cartella` 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.

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 nella RAM del computer. Il componente esegue la scansione dei file in tutte le unità del computer, nonché nelle unità connesse. 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 disinfecta 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 sono archiviati nel cloud OneDrive, Kaspersky Endpoint Security scarica ed esamina i contenuti dei file.

Impostazioni del componente Protezione minacce file

Parametro	Descrizione
Livello di sicurezza <i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i>	<p>Per Protezione minacce file, Kaspersky Endpoint Security può applicare diversi gruppi di impostazioni. I gruppi di impostazioni archiviate nell'applicazione sono denominati <i>livelli di protezione</i>:</p> <ul style="list-style-type: none">• 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 composti.
Tipi di file	Tutti i file. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina tutti i file senza eccezioni (tutti i formati e le estensioni).

<p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>File esaminati per formato. Se questa impostazione è abilitata, Kaspersky Endpoint Security 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.</p> <p>File esaminati per estensione. Se questa impostazione è abilitata, Kaspersky Endpoint Security esamina solo i file infettabili . Il formato del file viene quindi determinato in base all'estensione.</p>
<p>Ambito della protezione</p>	<p>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.</p> <p>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 inoltre possibile escludere un oggetto (ad esempio unità rimovibili) dalle scansioni.</p>
<p>Machine Learning e analisi delle firme</p> <p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>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.</p> <p>In base ai suggerimenti degli esperti Kaspersky, il metodo Machine Learning e analisi delle firme è sempre abilitato.</p>
<p>Analisi euristica</p> <p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>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.</p> <p>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.</p>
<p>Azione se viene rilevata una minaccia</p>	<p>Disinfetta (se non è possibile, elimina). Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non riesce, i file vengono eliminati.</p> <p>Disinfetta (se non è possibile, blocca). Se questa opzione è selezionata, Kaspersky Endpoint Security tenta automaticamente di disinfettare tutti i file infetti rilevati. Se la disinfezione non è possibile, Kaspersky Endpoint Security aggiunge le informazioni sui file infetti rilevati all'elenco delle minacce attive.</p> <p>Blocca. Se questa opzione è selezionata, il componente Protezione minacce file blocca automaticamente tutti i file infetti senza tentare di disinfettarli.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Prima di tentare di disinfettare o eliminare un file infetto, Kaspersky Endpoint Security crea una copia di backup del file nel caso in cui sia necessario ripristinare il file o se può essere disinfettato in futuro.</p> </div>

Esamina solo i file nuovi e modificati	<p>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.</p>
Esamina gli archivi	<p>Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. Kaspersky Endpoint Security 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).</p>
Esamina i pacchetti di distribuzione	<p>Questa casella di controllo consente di abilitare o disabilitare la scansione dei pacchetti di distribuzione di terze parti.</p>
Esamina i file nei formati Microsoft Office	<p>Esamina i file di Microsoft Office (DOC, DOCX, XLS, PPT e altre estensioni Microsoft). I file in formato Office includono anche gli oggetti OLE.</p>
Non decomprimere i file compositi di grandi dimensioni	<p>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.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esamina i file compositi di qualsiasi dimensione.</p> <div data-bbox="384 936 1493 1059" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.</p> </div>
Decomprimi file compositi in background	<p>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.</p> <p>Kaspersky Endpoint Security consente di accedere ai file compositi di dimensioni inferiori a questo valore solo dopo la decompressione e la scansione dei file.</p> <p>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.</p>
Modalità di scansione <i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i>	<div data-bbox="384 1541 1493 1664" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>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.</p> </div> <p>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.</p> <p>In fase di accesso e modifica. In questa modalità Protezione minacce file esamina gli oggetti in caso di tentativo di apertura o modifica.</p> <p>Al momento dell'accesso. In questa modalità Protezione minacce file esamina gli oggetti solo in caso di tentativo di apertura.</p> <p>In fase di esecuzione. In questa modalità Protezione minacce file esamina gli oggetti solo in caso di tentativo di esecuzione.</p>

<p>Tecnologia iSwift</p> <p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>Questa tecnologia consente una maggiore velocità, grazie all'esclusione di alcuni file dalla scansione. I file vengono esclusi dalla scansione 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.</p>
<p>Tecnologia iChecker</p> <p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>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).</p>
<p>Sospendi Protezione minacce file</p> <p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>Il funzionamento di Protezione minacce file viene temporaneamente e automaticamente sospeso all'ora specificata o quando si utilizzano le applicazioni specificate.</p>

Protezione minacce Web

Il componente Protezione minacce Web impedisce il download di file dannosi da Internet e blocca inoltre i 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. È possibile [specificare le porte che verranno monitorate da Kaspersky Endpoint Security](#), oppure selezionare tutte le porte.

Per il monitoraggio del traffico HTTPS è necessario [abilitare la scansione delle connessioni criptate](#).

Quando un utente tenta di aprire un sito Web dannoso o di phishing, Kaspersky Endpoint Security bloccherà l'accesso e mostrerà un avviso (vedere la figura seguente).



Accesso negato

Impossibile fornire l'indirizzo Web richiesto.

http://kl-test-page.avp.ru/new_ksn_samples/AVS_RISKWARE-KSN_BAD.exe


Motivo:

oggetto infettato da [UDS:DangerousObject.Multi.Generic](#)

Data generazione messaggio: 10/8/2020 1:42:11 PM

Messaggio di accesso negato al sito Web

Impostazioni del componente Protezione minacce Web

Parametro	Descrizione
Livello di sicurezza <i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i>	<p>Per Protezione minacce Web, Kaspersky Endpoint Security può applicare diversi gruppi di impostazioni. I gruppi di impostazioni archiviate nell'applicazione sono denominati <i>livelli di protezione</i>:</p> <ul style="list-style-type: none">• Alto. Il livello di sicurezza in cui il componente Protezione minacce Web esegue la massima scansione del traffico Web ricevuto dal computer tramite i protocolli 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 di Kaspersky Endpoint Security 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 Media.
Azione se viene rilevata una minaccia	<p>Blocca il download. 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.</p> <p>Notifica. 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.</p>
Verifica l'indirizzo Web a fronte del database degli indirizzi Web dannosi <i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i>	<p>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 e incluso nel pacchetto di installazione dell'applicazione e viene aggiornato durante gli aggiornamenti del database di Kaspersky Endpoint Security.</p>

<p>Usa l'Analisi euristica</p> <p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>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.</p> <p>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.</p>
<p>Verifica l'indirizzo Web a fronte del database degli indirizzi Web di phishing</p> <p><i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>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.</p>
<p>Non esaminare il traffico Web per gli indirizzi Web attendibili</p>	<p>Se la casella 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.</p>

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
- Microsoft Outlook Express
- Windows Mail

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 operazioni con Outlook 2010, 2013, 2016 e 2019.

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 rinomina l'oggetto del messaggio come segue: [Il messaggio richiede la partecipazione dell'utente all'elaborazione] <oggetto del messaggio> o [Il messaggio è stato elaborato] <oggetto del messaggio>.

Impostazioni del componente Protezione minacce di posta

Parametro	Descrizione
<p>Livello di sicurezza (disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</p>	<p>Per Protezione minacce di posta, Kaspersky Endpoint Security applica diversi gruppi di impostazioni. I gruppi di impostazioni archiviate nell'applicazione sono denominati <i>livelli di protezione</i>.</p> <ul style="list-style-type: none"> • 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 di Kaspersky Endpoint Security 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.
<p>Azione se viene rilevata una minaccia</p>	<p>Disinfetta (se non è possibile, elimina). Quando un oggetto infetto viene rilevato in un messaggio in entrata o in uscita, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security elimina l'oggetto infetto. Kaspersky Endpoint Security aggiunge informazioni sull'azione eseguita nell'oggetto del messaggio: [Il messaggio è stato elaborato] <oggetto del messaggio>.</p>

	<p>Disinfetta (se non è possibile, blocca). Quando un oggetto infetto viene rilevato in un messaggio in entrata, Kaspersky Endpoint Security 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, Kaspersky Endpoint Security aggiunge un avviso all'oggetto del messaggio: [Il messaggio richiede la partecipazione dell'utente all'elaborazione] <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, Kaspersky Endpoint Security tenta di disinfettare l'oggetto rilevato. Se l'oggetto non può essere disinfettato, Kaspersky Endpoint Security blocca la trasmissione del messaggio e il client di posta mostra un errore.</p> <p>Blocca. Se un oggetto infetto viene rilevato in un messaggio in entrata, Kaspersky Endpoint Security aggiunge un avviso all'oggetto del messaggio: [Il messaggio richiede la partecipazione dell'utente all'elaborazione] <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, Kaspersky Endpoint Security blocca la trasmissione del messaggio e il client di posta mostra un errore.</p>
<p>Ambito della protezione <i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>L'<i>ambito della protezione</i> include gli oggetti che il componente controlla durante l'esecuzione: Messaggi in entrata e in uscita o Solo messaggi in entrata.</p> <p>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.</p>
<p>Esegui scansione traffico POP3, SMTP, NNTP e IMAP</p>	<p>Questa casella di controllo consente di abilitare o disabilitare la scansione da parte del componente Protezione minacce di posta del traffico trasferito tramite i protocolli POP3, SMTP, NNTP e IMAP.</p>
<p>Connetti estensione Microsoft Outlook</p>	<p>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.</p> <p>Se viene eseguita la scansione dei messaggi tramite l'estensione per Microsoft Outlook, è consigliabile utilizzare la modalità cache. Per informazioni più dettagliate sulla Modalità cache e per raccomandazioni sul relativo utilizzo, fare riferimento alla Microsoft Knowledge Base.</p>
<p>Analisi euristica <i>(disponibile solo in Administration Console (MMC) e nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>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.</p> <p>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.</p>
<p>Esamina gli archivi allegati</p>	<p>Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. Kaspersky Endpoint Security esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato.</p>

	<p>Se durante la scansione Kaspersky Endpoint Security 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.</p>
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.
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	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Il filtro allegati non viene applicato ai messaggi e-mail in uscita.</p> </div> <p>Disabilita il filtro. Se questa opzione è selezionata, il componente Protezione minacce di posta non filtra i file allegati ai messaggi e-mail.</p> <p>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.</p> <p>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.</p> <p>Nell'elenco delle maschere di file è possibile specificare i tipi di file allegati da rinominare o eliminare dai messaggi e-mail.</p>

Protezione minacce di rete

Il componente Protezione minacce di Rete esamina il traffico di rete in entrata alla ricerca di attività tipiche degli attacchi di rete. Quando Kaspersky Endpoint Security 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 di Kaspersky Endpoint Security 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
<p>Considera la scansione delle porte e il flooding di rete come attacchi</p>	<p>Il <i>flooding di rete</i> 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.</p> <p>Un attacco di <i>scansione delle porte</i> 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.</p> <p>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.</p> <p>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.</p>
<p>Aggiungi il computer che ha originato l'attacco all'elenco dei computer bloccati per N min</p>	<p>Se la casella di controllo è selezionata, 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 32.768 minuti.</p> <p>È possibile visualizzare l'elenco dei blocchi nella finestra dello strumento Monitor di rete.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security cancella l'elenco dei blocchi al riavvio dell'applicazione e quando le impostazioni di Protezione minacce di rete vengono modificate.</p> </div>
<p>Esclusioni</p>	<p>L'elenco contiene gli indirizzi IP da cui Protezione minacce di rete non blocca gli attacchi di rete.</p> <p>L'applicazione non registra le informazioni sugli attacchi di rete dagli indirizzi IP che fanno parte dell'elenco delle esclusioni.</p>
<p>Protezione dallo spoofing MAC</p>	<p>Un <i>attacco di spoofing MAC</i> 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.</p>

Firewall

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. Inserisce l'applicazione in uno dei *gruppi di attendibilità*: Attendibile, Restrizione bassa, Restrizione alta, Non attendibile.

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 come segue: una regola di rete per le applicazioni include regole di accesso basate sullo stato della rete: *pubblica*, *locale* o *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.

Stati delle connessioni di rete

Firewall consente di controllare l'attività di rete in base allo stato della connessione di rete. Kaspersky Endpoint Security riceve lo stato della connessione di rete dal sistema operativo del computer. Lo stato della connessione di rete nel sistema operativo viene impostato dall'utente durante la configurazione della connessione. È possibile [modificare lo stato della connessione di rete nelle impostazioni di Kaspersky Endpoint Security](#). Firewall monitorerà l'attività di rete in base allo stato della rete nelle impostazioni di Kaspersky Endpoint Security e non nel sistema operativo.

La connessione di rete può avere uno dei seguenti tipi di categoria:

- **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 la categoria *Rete pubblica*. Non è possibile modificare la categoria 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
-----------	-------------

<p>Regole per i pacchetti di rete</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Le regole per i pacchetti di rete hanno una priorità superiore rispetto alle regole di rete per le applicazioni.</p>
<p>Connessioni di rete</p>	<p>Questa tabella contiene informazioni sulle connessioni di rete rilevate da Firewall sul computer.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>La categoria <i>Rete pubblica</i> viene assegnata a Internet per impostazione predefinita. Non è possibile modificare la categoria di Internet.</p> </div>
<p>Regole di rete</p>	<p>Applicazioni</p> <p>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.</p> <p>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.</p> <p>Regole di rete</p> <p>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.</p> <p>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.</p>

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.

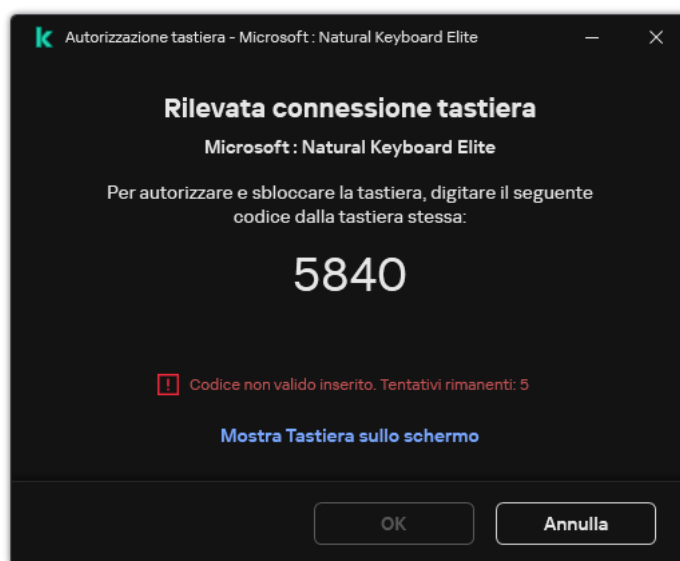
Se il codice è stato immesso correttamente, l'applicazione salva i parametri di identificazione (VID/PID della tastiera e numero della porta a cui è stata connessa) nell'elenco delle tastiere autorizzate. L'autorizzazione della tastiera non deve essere ripetuta quando la tastiera viene connessa di nuovo 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.

Il componente Prevenzione Attacchi BadUSB non è installato per impostazione predefinita. Se è necessario il componente Prevenzione Attacchi BadUSB, è possibile aggiungere il componente nelle proprietà del [pacchetto di installazione](#) prima di installare l'applicazione o [modificare i componenti dell'applicazione disponibili](#) dopo l'installazione dell'applicazione.



Autorizzazione tastiera

Impostazioni del componente Prevenzione Attacchi BadUSB

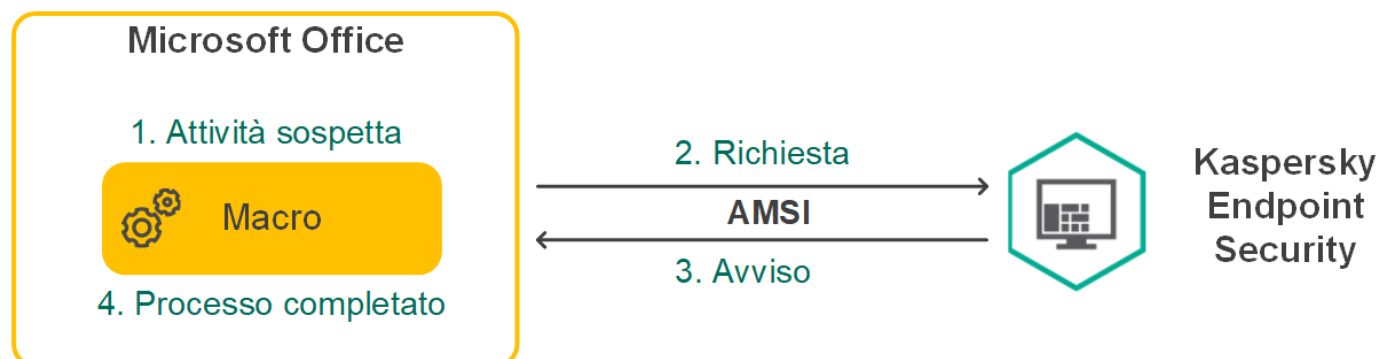
Parametro	Descrizione
Impedisci l'utilizzo di Tastiera sullo schermo per l'autorizzazione di dispositivi USB	Se la casella di controllo è selezionata, l'applicazione impedisce di utilizzare la Tastiera sullo schermo per l'autorizzazione di un dispositivo USB da cui non è possibile immettere un codice di autorizzazione.

Numero massimo di tentativi di autorizzazione del dispositivo	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 5 tentativi di immissione del codice di autorizzazione, il dispositivo USB viene bloccato dopo il quinto tentativo non riuscito. Kaspersky Endpoint Security mostra la durata del blocco per il dispositivo USB. Trascorso questo tempo, è possibile compiere 5 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).

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 terze parti 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 terze parti 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 terze parti della minaccia rilevata. Dopo la ricezione di una notifica di minaccia, l'applicazione di terze parti non consente di eseguire 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 terze parti, 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 terze parti ad Administration Server. Il componente Protezione AMSI non nega le richieste provenienti dalle applicazioni di terze parti 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;
- Windows 11;
- Windows Server 2016 Essentials/Standard/Datacenter;

- Windows Server 2019 Essentials/Standard/Datacenter;
- Windows Server 2022.

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. Kaspersky Endpoint Security 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 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.
Non decomprimere i file composti di grandi dimensioni	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security non esegue la scansione dei file composti se la loro dimensione supera il valore specificato.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security esamina i file composti di qualsiasi dimensione.</p> <p>Kaspersky Endpoint Security esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.</p>

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.

Impostazioni del componente Prevenzione Exploit

Parametro	Descrizione
Al rilevamento di exploit	<p>Blocca operazione. 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.</p> <p>Notifica. 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.</p>
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 (Behavior Stream Signature) 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 assicura una difesa proattiva del computer.

Impostazioni del componente Rilevamento del Comportamento

Parametro	Descrizione
Se viene rilevata un'attività malware	<ul style="list-style-type: none">• Elimina file. 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.• Termina l'applicazione. Se si seleziona questa opzione, Kaspersky Endpoint Security termina l'applicazione al momento del rilevamento dell'attività dannosa.• Notifica. 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.
Abilita la protezione delle cartelle condivise dal criptaggio esterno	<p>Se l'interruttore è attivato, Kaspersky Endpoint Security analizza l'attività nelle cartelle condivise. Se questa attività corrisponde a una firma BSS tipica del criptaggio esterno, Kaspersky Endpoint Security esegue l'azione selezionata.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>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.</p></div> <ul style="list-style-type: none">• Notifica. Se questa opzione è selezionata, quando viene rilevato un tentativo di modifica dei file nelle cartelle condivise, Kaspersky Endpoint Security aggiunge informazioni sul tentativo di modificare i file nelle cartelle condivise all'elenco delle minacce attive.• 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'attività di rete del computer che sta tentando di modificare i file e crea copie di backup dei file modificati. <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"><p>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.</p></div>
Esclusioni	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](#).

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 da [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. Inserisce l'applicazione in uno dei *gruppi di attendibilità*: Attendibile, Restrizione bassa, Restrizione alta, Non attendibile.

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.

Impostazioni del componente Prevenzione Intrusioni Host

Parametro	Descrizione
Diritti applicazione	<p>Applicazioni</p> <p>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.</p> <p>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.</p> <p>I diritti di accesso alle applicazioni sono riportati nelle seguenti tabelle:</p> <ul style="list-style-type: none"> • File e registro di sistema. Questa tabella contiene i diritti delle applicazioni all'interno di un gruppo di attendibilità per accedere alle risorse del sistema operativo e ai dati personali. • Diritti. Questa tabella contiene i diritti delle applicazioni in un gruppo di attendibilità per l'accesso ai processi e alle risorse del sistema operativo. • 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	<p>Nome</p> <p>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.</p> <p>Le risorse possono essere rappresentate da categorie di registro, file, cartelle o chiavi di registro.</p> <p>Applicazioni</p> <p>Tabella delle applicazioni monitorate dal componente Prevenzione Intrusioni Host per la risorsa selezionata. 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.</p>
Gruppo di attendibilità per le applicazioni avviate prima dell'esecuzione di Kaspersky Endpoint Security for Windows	<p>Un gruppo di attendibilità in cui Kaspersky Endpoint Security inserirà le applicazioni avviate prima di Kaspersky Endpoint Security.</p>

<p>Aggiorna i diritti per le applicazioni precedentemente sconosciute dal database KSN</p>	<p>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.</p>
<p>Considera attendibili le applicazioni con firma digitale</p>	<p>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.</p> <p><i>I produttori attendibili</i> sono i produttori di software considerati attendibili da Kaspersky. È inoltre possibile aggiungere manualmente il certificato del produttore all'archivio certificati attendibili.</p> <p>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.</p>
<p>Elimina le regole per le applicazioni non avviate per più di (giorni, da 1 a 90)</p>	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>Al successivo avvio dell'applicazione, Kaspersky Endpoint Security analizza l'applicazione come se si trattasse del primo avvio.</p>
<p>Gruppo di attendibilità per le applicazioni che non potevano essere aggiunte ai gruppi esistenti</p>	<p>Gli elementi in questo elenco a discesa determinano a quale gruppo di attendibilità Kaspersky Endpoint Security assegnerà un'applicazione sconosciuta.</p> <p>È possibile selezionare uno dei seguenti elementi:</p> <ul style="list-style-type: none"> • Restrizione bassa. • Restrizione alta. • Non attendibili.

Motore di Remediation

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 virus](#).

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.

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 l'utente sta partecipando a Kaspersky Security Network, i servizi KSN forniscono a Kaspersky Endpoint Security informazioni sulla categoria e sulla reputazione dei file esaminati, nonché informazioni sulla reputazione degli indirizzi Web esaminati.

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.

Per ridurre il carico sui server KSN, gli esperti di Kaspersky possono rilasciare aggiornamenti dell'applicazione che disabilitano temporaneamente o limitano parzialmente le richieste a Kaspersky Security Network. In tal caso, lo stato della connessione a KSN nell'interfaccia locale dell'applicazione è *Abilitato con restrizioni*.

Infrastruttura KSN

Kaspersky Endpoint Security supporta le seguenti soluzioni infrastrutturali KSN:

- *KSN Globale* è la soluzione utilizzata dalla maggior parte delle applicazioni Kaspersky. I partecipanti KSN ricevono le informazioni da Kaspersky Security Network 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 di Kaspersky Security Network.
- *KSN Privato* 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 Security Network e ad altri dati statistici senza inviare dati a KSN dai propri computer. KSN Privato 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 impostazione predefinita, Kaspersky Security Center utilizza KSN Globale. È possibile configurare l'uso di KSN Privato in Administration Console (MMC), in Kaspersky Security Center Web Console e nella [riga di comando](#). Non è possibile configurare l'utilizzo di KSN Privato in Kaspersky Security Center Cloud Console.

Per ulteriori dettagli su KSN Privato, consultare la documentazione relativa a Kaspersky Private Security Network.

Proxy KSN

I computer degli utenti gestiti tramite Kaspersky Security Center Administration Server possono interagire con KSN tramite il servizio Proxy KSN.

Il servizio Proxy KSN 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 proxy KSN 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 informazioni dettagliate sul servizio proxy KSN, consultare la [Guida di Kaspersky Security Center](#).

Parametro	Descrizione
Abilita modalità KSN estesa	<p><i>Modalità KSN estesa</i> 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.</p>
Abilita modalità cloud	<p>La <i>Modalità cloud</i> 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.</p> <p>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.</p> <div data-bbox="336 725 1493 848" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security scarica la versione leggera dei database anti-virus durante il successivo aggiornamento dopo la selezione della casella di controllo.</p> </div> <p>Se l'interruttore è disattivato, Kaspersky Endpoint Security utilizza la versione completa dei database anti-virus.</p> <div data-bbox="336 999 1493 1122" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security scarica la versione completa dei database anti-virus durante il successivo aggiornamento dopo la deselegazione della casella di controllo.</p> </div>
Stato del computer quando i server KSN non sono disponibili <i>(disponibile solo in Kaspersky Security Center Console)</i>	<p>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.</p>
Usa proxy KSN <i>(disponibile solo in Kaspersky Security Center Console)</i>	<p>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.</p>
Usa i server KSN quando il proxy KSN	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza i server KSN quando il servizio proxy KSN non è disponibile. I server KSN possono essere gestiti sia da Kaspersky (quando si utilizza KSN Globale) che da terze parti (quando si utilizza KSN Privato).</p>

non è disponibile

(disponibile solo in Kaspersky Security Center Console)

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).

Kaspersky Endpoint Security monitora solo il traffico HTTP e HTTPS.

Per il monitoraggio del traffico HTTPS è necessario [abilitare la scansione delle connessioni criptate](#).

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 grafiche. 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 "File di immagini".

- **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 "File di 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.



Impossibile fornire la pagina Web richiesta.


Indirizzo: <http://kaspersky.ru/>.

La pagina Web è stata bloccata dalla regola kasp.

Motivo: la risorsa Web appartiene alle categorie di contenuti Non determinato e alle categorie di tipo di dati Non determinato.

Questa risorsa Web non è consentita a livello di azienda. Se si ritiene che il blocco sia stato applicato per errore o è necessario accedere a questa risorsa Web, contattare l'amministratore della rete aziendale locale ([Richiedi accesso](#)).

Data generazione messaggio: 10/14/2020 1:31:27 AM



La pagina Web richiesta potrebbe essere non protetta o non consentita dal criterio aziendale.

Indirizzo: <http://kaspersky.ru/>.

La pagina Web è stata bloccata dalla regola kasp.

Motivo: la risorsa Web appartiene alle categorie di contenuti Non determinato e alle categorie di tipo di dati Non determinato.

Per aprire la pagina Web richiesta, fare clic sul collegamento <http://kaspersky.ru/>.
 Per ottenere l'accesso all'intero contenuto del sito Web a cui appartiene la pagina Web richiesta, fare clic sul collegamento http://kaspersky.ru/*.
 Per ottenere l'accesso a tutti i domini esistenti di livello pari o inferiore a quello contrassegnato da "*", fare clic sul collegamento *//*kaspersky.ru/*.

L'accesso alle risorse Web elencate in precedenza verrà concesso per la durata della sessione corrente dell'applicazione.
 Nel caso l'avviso sia stato visualizzato per errore, contattare l'amministratore della rete aziendale locale ([Richiedi accesso](#)).

Data generazione messaggio: 10/14/2020 1:31:50 AM

Messaggi di Controllo Web

Impostazioni dei componenti di Controllo Web

Parametro	Descrizione
-----------	-------------

Regola di accesso alle risorse Web	<p>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.</p>
Regola predefinita	<p>La <i>regola predefinita</i> è una regola di accesso alle risorse Web a cui non si applica nessun'altra regola. Sono disponibili le seguenti opzioni:</p> <ul style="list-style-type: none"> • Consenti tutto tranne l'elenco di regole, noto anche come modalità Lista vietati per i siti Web vietati. • Vieta tutto tranne l'elenco di regole, noto anche come modalità Lista consentiti per i siti Web consentiti.
Modelli di messaggi	<ul style="list-style-type: none"> • 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.
Registra l'apertura delle pagine consentite	<p>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.</p> <div data-bbox="336 1447 1495 1608" style="background-color: #f8d7da; padding: 10px; border: 1px solid #f5c6cb;"> <p>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.</p> </div> <div data-bbox="336 1648 1495 1771" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Il monitoraggio dell'attività Internet degli utenti può richiedere più risorse del computer quando si decripta il traffico HTTPS.</p> </div>

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.

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 – ❌.
- Dipende dal bus di connessione (eccetto per il 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). Di conseguenza è possibile limitare la connessione di tutti i dispositivi, ad esempio tramite 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.

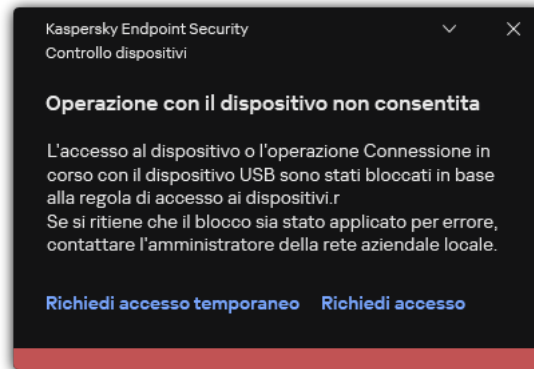
È possibile aggiungere dispositivi attendibili in base ai seguenti dati:

- **Dispositivi per ID** Ogni dispositivo ha un identificatore univoco (ID hardware o HWID). È possibile visualizzare l'ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. ID dispositivo di esempio: 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 ID fornitore (VID) e un ID prodotto (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.

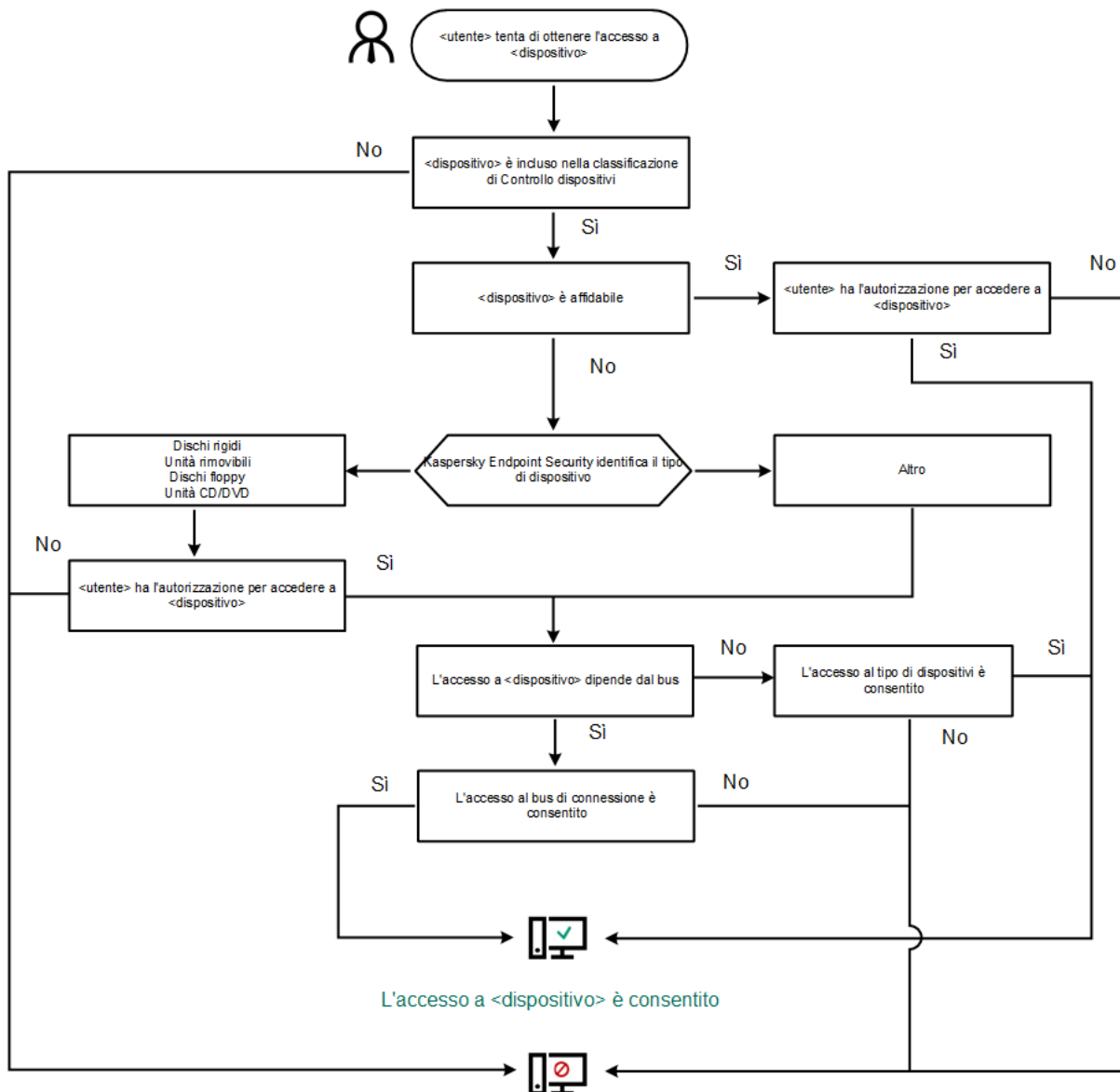
Quando un dispositivo bloccato da Controllo dispositivi viene connesso al computer, Kaspersky Endpoint Security bloccherà l'accesso e mostrerà una notifica (vedere la figura seguente).



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).



L'accesso a <dispositivo> è bloccato

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](#).

Impostazioni dei componenti di Controllo dispositivi

Parametro	Descrizione
Consenti richieste di accesso temporaneo	Se la casella di controllo è selezionata, il pulsante Richiedi accesso è disponibile nell'interfaccia locale di Kaspersky Endpoint Security. Questo pulsante apre la finestra Richiedi accesso al dispositivo . In questa finestra l'utente può richiedere l'accesso temporaneo a un dispositivo bloccato.

<i>(disponibile solo in Kaspersky Security Center Console)</i>	
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.
Dispositivi attendibili	Elenco di dispositivi attendibili e di utenti ai quali è stato concesso l'accesso a questi dispositivi.
Anti-Bridging	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Anti-Bridging supporta il funzionamento con i seguenti tipi di dispositivi: scheda di rete, Wi-Fi e modem.</p>
Modelli di messaggi	<p>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.</p> <p>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.</p>

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*), hash file, fornitore dell'applicazione e altri criteri.

2. Gestione 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.

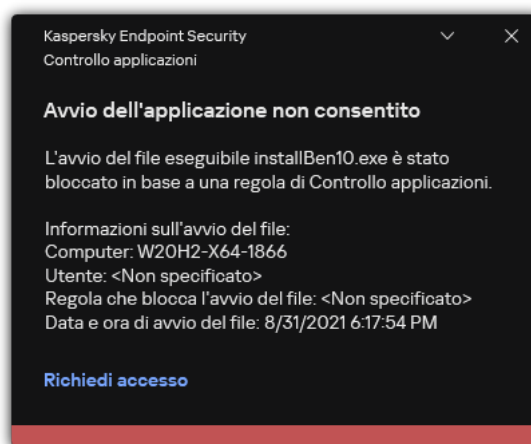
3. Selezione della modalità di Controllo applicazioni.

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](#).

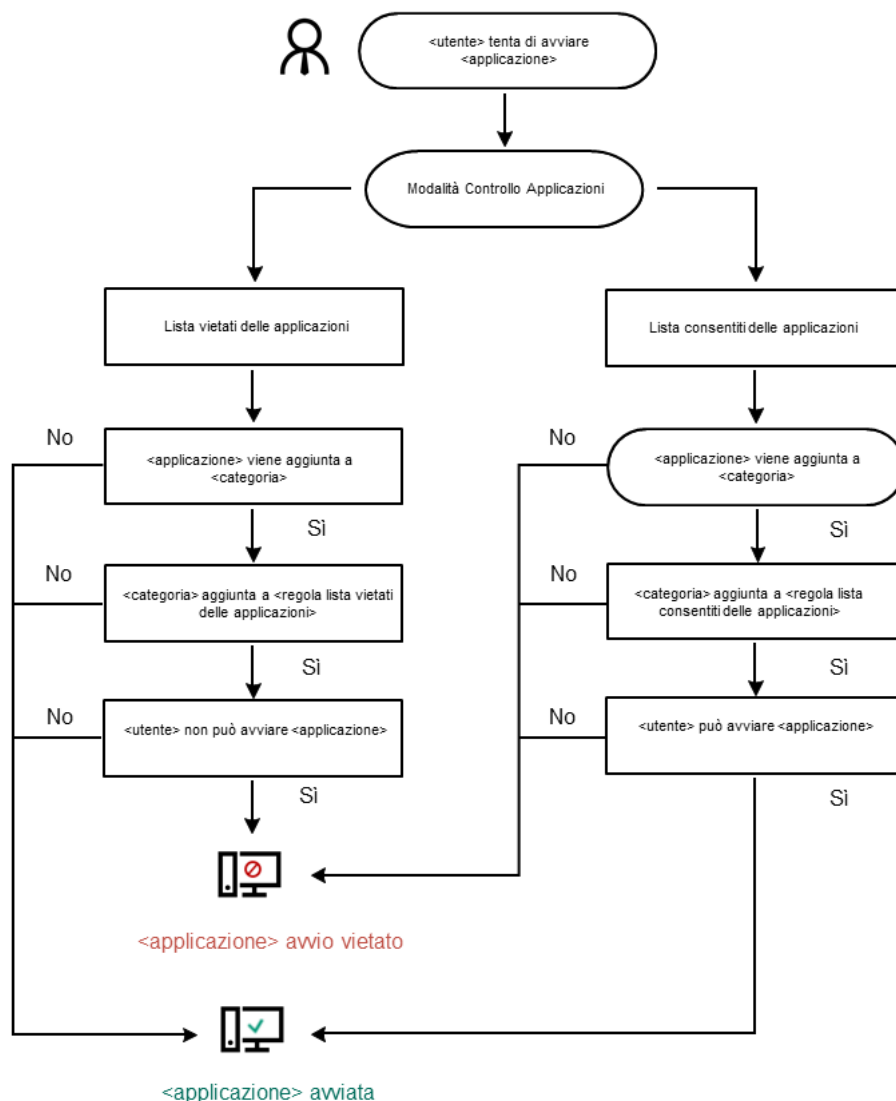
Le regole di Controllo applicazioni create in Kaspersky Security Center Administration Console si basano sulle categorie di applicazioni personalizzate e non sulle condizioni di inclusione ed esclusione, come nel caso dell'interfaccia locale di Kaspersky Endpoint Security.

- [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

Impostazioni dei componenti di Controllo applicazioni

Parametro	Descrizione
Modalità di test	Se l'interruttore è attivato, Kaspersky Endpoint Security consente l'avvio di un'applicazione bloccata nella modalità corrente di Controllo applicazioni, ma registra le informazioni sull'avvio nel rapporto.
Modalità Controllo applicazioni	<p>È possibile selezionare una delle seguenti opzioni:</p> <ul style="list-style-type: none"> • 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. <p>Quando la modalità Lista consentiti è selezionata, vengono automaticamente create due regole di Controllo applicazioni:</p> <ul style="list-style-type: none"> • Immagine gold

	<ul style="list-style-type: none"> • Programmi di aggiornamento attendibili <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Non è possibile modificare le impostazioni di o eliminare le regole create automaticamente. È possibile abilitare o disabilitare queste regole.</p> </div>
<p>Controlla caricamento moduli DLL (comporta un aumento significativo del carico sul sistema)</p>	<p>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.</p> <div style="border: 1px solid black; background-color: #ffe6e6; padding: 10px; margin-top: 10px;"> <p>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 "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.</p> </div> <p>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.</p>
<p>Modelli di messaggi</p>	<p>Messaggio relativo al blocco Modello del messaggio visualizzato quando viene attivata una regola di Controllo applicazioni che blocca l'avvio di un'applicazione.</p> <p>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.</p>

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 tenere traccia dei comportamenti inusuali (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 **Attivazione delle regole con stato Smart Training**.

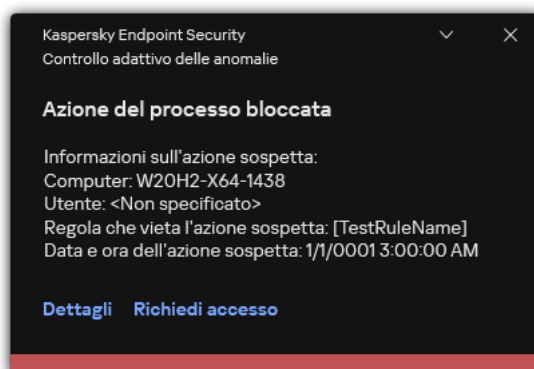
2. Analisi del rapporto sull'attivazione delle regole.

L'amministratore analizza il [rapporto sull'attivazione delle regole](#) o i contenuti dell'archivio **Attivazione delle regole con 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. Controllo adattivo delle anomalie viene configurato 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 **Attivazione delle regole con stato Smart Training**. È consigliabile consultare il rapporto sull'attivazione delle regole e i contenuti dell'archivio **Attivazione delle regole con stato Smart Training**.

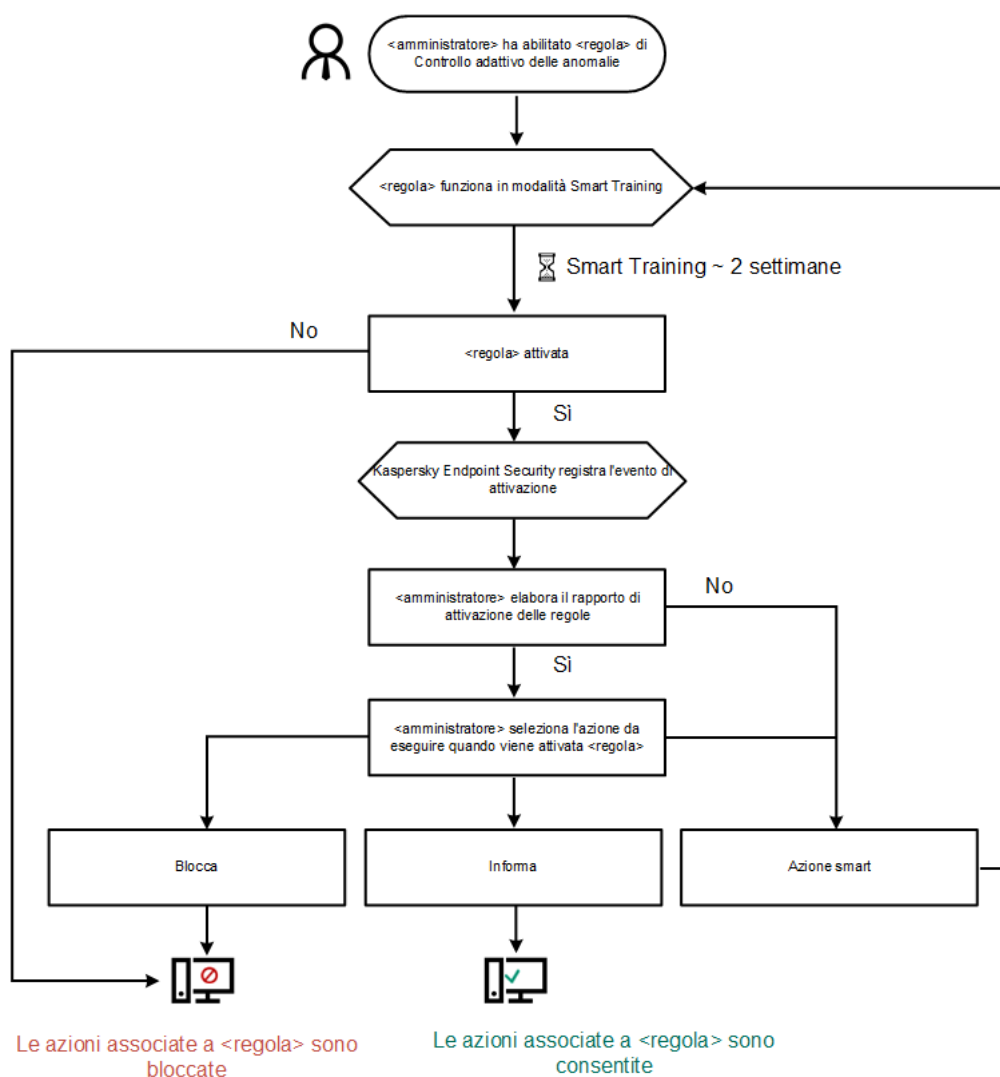
Quando un'applicazione dannosa tenta di eseguire un'azione, Kaspersky Endpoint Security blocca l'azione e visualizza una notifica (vedere la figura seguente).



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

Impostazioni del componente Controllo adattivo delle anomalie

Parametro	Descrizione
Rapporto sullo stato delle regole di Controllo adattivo delle anomalie <i>(disponibile solo in Kaspersky Security Center Console)</i>	Questo rapporto contiene informazioni sullo stato delle regole di rilevamento di Controllo adattivo delle anomalie (ad esempio <i>Disattivato</i> o <i>Blocca</i>). Il rapporto viene generato per tutti i gruppi di amministrazione.
Rapporto sulle regole attivate di	Questo rapporto contiene informazioni sulle azioni non tipiche rilevate da Controllo adattivo delle anomalie. Il rapporto viene generato per tutti i gruppi di amministrazione.

<p>Controllo adattivo delle anomalie</p> <p><i>(disponibile solo in Kaspersky Security Center Console)</i></p>	
<p>Regole</p>	<p>Tabella delle regole di Controllo adattivo delle anomalie. Le regole vengono create dagli esperti di Kaspersky in base agli scenari tipici delle attività potenzialmente dannose.</p>
<p>Modelli</p>	<p>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.</p> <p>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.</p>

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 Sensore Endpoint 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 due blocchi funzionali: Kaspersky Anti Targeted Attack (in seguito definito anche "KATA") e Kaspersky Endpoint Detection and Response (di seguito definito anche "KEDR"). È possibile acquistare KEDR 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 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](#).

Kaspersky Sandbox

Kaspersky Endpoint Security 11.7.0 dispone ora di un agente integrato per l'integrazione con la soluzione Kaspersky Sandbox. *La soluzione Kaspersky Sandbox* rileva e blocca automaticamente le minacce avanzate sui computer. Kaspersky Sandbox analizza il comportamento degli oggetti per rilevare attività dannose e le caratteristiche delle attività degli attacchi mirati sull'infrastruttura IT dell'organizzazione. Kaspersky Sandbox analizza ed esegue la scansione degli oggetti su server speciali con immagini virtuali distribuite dei sistemi operativi Microsoft Windows (server di Kaspersky Sandbox). Per ulteriori dettagli sulla soluzione, consultare la Guida di [Kaspersky Sandbox](#).

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 Kaspersky Sandbox

Parametro	Descrizione
Certificato TLS del server.	Per configurare una connessione attendibile con i server di Kaspersky Sandbox, è necessario preparare un certificato TLS. Successivamente, è necessario aggiungere il certificato ai server di Kaspersky Sandbox e al criterio di Kaspersky Endpoint Security. Per ulteriori dettagli sulla preparazione del certificato e sull'aggiunta del certificato ai server, consultare la Guida di Kaspersky Sandbox .
Timeout	Timeout della connessione per il server Kaspersky Sandbox. Allo scadere del timeout configurato, Kaspersky Endpoint Security invia una richiesta al server successivo. È possibile aumentare il timeout della connessione per Kaspersky Sandbox 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 delle richieste Kaspersky Sandbox	Dimensione della cartella della coda di richieste. Quando si accede a un oggetto sul computer (file eseguibile avviato o documento aperto, ad esempio in formato DOCX o PDF), Kaspersky Endpoint Security può anche inviare l'oggetto da sottoporre a scansione da parte di Kaspersky Sandbox. Se sono presenti più richieste, 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, Kaspersky 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.
Server Kaspersky Sandbox	Impostazioni di connessione al server Kaspersky 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.
Azione se viene rilevata una minaccia	<p>Sposta la copia in Quarantena, elimina l'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.</p> <p>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.</p> <p>Crea attività di scansione IOC. Se questa opzione è selezionata, Kaspersky Endpoint Security crea automaticamente l'attività Scansione IOC (<i>attività di scansione IOC autonoma</i>). Per questa attività, è possibile configurare la modalità di esecuzione, l'ambito della scansione e l'azione sul rilevamento IOC: eliminazione dell'oggetto, esecuzione dell'attività Scansione delle aree critiche. Per modificare altre impostazioni dell'attività di <i>scansione IOC</i>, passare alle impostazioni dell'attività.</p>
Ambito della scansione IOC	<p>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.</p> <p>Aree dei file nelle unità di sistema del computer. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue una scansione IOC sull'unità di sistema del computer.</p>
Attività Esegui scansione IOC.	<p>Manualmente. Modalità di esecuzione in cui è possibile avviare l'attività <i>Scansione IOC</i> manualmente in qualsiasi momento.</p> <p>In seguito al rilevamento della minaccia. Modalità di esecuzione in cui Kaspersky Endpoint Security esegue automaticamente l'attività di <i>scansione IOC</i> ogni volta che viene rilevata una minaccia.</p> <p>Esegui solo quando il computer è inattivo. Modalità di esecuzione in cui Kaspersky Endpoint Security esegue l'attività di <i>scansione IOC</i> 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.</p>

Endpoint Detection and Response

Kaspersky Endpoint Security 11.7.0 dispone ora di un agente integrato per la soluzione Kaspersky Endpoint Detection and Response Optimum (di seguito denominato anche "EDR Optimum"). Kaspersky Endpoint Security 11.8.0 dispone ora di 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 dell'avviso in una finestra separata. *Dettagli dell'avviso* è uno strumento che consente di visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Dettagli dell'avviso include, ad esempio, la cronologia dei file visualizzati nel computer. Per informazioni dettagliate sulla gestione dei dettagli dell'avviso, 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 EDR Optimal in Web Console e Cloud Console. Le impostazioni del componente per EDR Expert sono disponibili solo in Cloud Console.

Impostazioni di Endpoint Detection and Response

Parametro	Descrizione
Isolamento di rete	<p>Isolamento automatico del computer dalla rete in risposta alle minacce rilevate.</p> <p>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:</p> <ul style="list-style-type: none"> • Connessioni elencate in Esclusioni dall'isolamento di rete. • Connessioni avviate dai servizi di Kaspersky Endpoint Security. • Connessioni avviate dall'agente di Kaspersky Security Center Administration.
Sblocca automaticamente il computer isolato tra N ore	<p>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.</p>
Esclusioni dall'isolamento di rete	<p>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.</p> <p>Per configurare le esclusioni dall'isolamento di rete, è possibile utilizzare un elenco di <i>profili di rete standard</i>. 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.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>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.</p> </div>

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 .
Azione in caso di esecuzione o apertura di un oggetto vietato	<p>Blocca e scrivi nel rapporto. 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.</p> <p>Registra solo gli 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.</p>
Regole di prevenzione dell'esecuzione	Elenco delle regole di prevenzione dell'esecuzione degli oggetti. <i>Regola di prevenzione dell'esecuzione</i> 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.

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

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 [Gestire gli account per l'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 Kaspersky Security Center. 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](#).

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 di un'unità, BitLocker crea una chiave master. Kaspersky Endpoint Security invia la chiave master a Kaspersky Security Center in modo da poter [ripristinare l'accesso al disco](#), se ad esempio un utente ha dimenticato la password.

Se un utente cripta un disco utilizzando BitLocker, Kaspersky Endpoint Security invierà [informazioni sul criptaggio del disco a Kaspersky Security Center](#). Tuttavia, Kaspersky Endpoint Security non invierà la chiave master a Kaspersky Security Center, pertanto sarà impossibile ripristinare l'accesso al disco utilizzando Kaspersky Security Center. Per il corretto funzionamento di BitLocker con Kaspersky Security Center, [decriptare l'unità](#) e [criptarla nuovamente](#) utilizzando un criterio. È possibile decriptare un'unità in locale o utilizzando un criterio.

Dopo il criptaggio del disco rigido di sistema, l'utente deve eseguire l'autenticazione BitLocker per avviare il sistema operativo. Dopo la procedura di autenticazione, BitLocker consentirà agli utenti di accedere. BitLocker non supporta la tecnologia SSO (Single Sign-On).

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	<p>Cripta tutti i dischi rigidi. Se questo elemento è selezionato, l'applicazione cripta tutti i dischi rigidi quando viene applicato il criterio.</p> <p>Se nel computer sono installati diversi sistemi operativi, dopo il criptaggio sarà possibile caricare solo il sistema operativo in cui è installata l'applicazione.</p> <p>Decripta tutti i dischi rigidi. Se questo elemento è selezionato, l'applicazione decripta tutti i dischi rigidi criptati precedentemente quando viene applicato il criterio.</p> <p>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.</p>
Durante il	Se questa casella di controllo è selezionata, l'applicazione crea gli account dell'Agente

<p>criptaggio, crea automaticamente gli account dell'Agente di Autenticazione per gli utenti Windows</p>	<p>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.</p>
<p>Impostazioni di creazione dell'account per l'Agente di Autenticazione</p>	<p>Tutti gli account nel computer. Tutti gli account nel computer che sono stati attivi in qualsiasi momento.</p> <p>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.</p> <p>Tutti gli account locali nel computer. Tutti gli account locali nel computer che sono stati attivi in qualsiasi momento.</p> <p>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.</p> <p>Amministratore locale. Kaspersky Endpoint Security crea un account utente dell'Agente di Autenticazione per l'amministratore locale del computer.</p> <p>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.</p> <p>Account attivo. Kaspersky Endpoint Security crea automaticamente un account dell'Agente di Autenticazione per l'account attivo al momento del criptaggio del disco.</p>
<p>Crea automaticamente gli account dell'Agente di Autenticazione per tutti gli utenti di questo computer al momento dell'accesso</p>	<p>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 <i>Gestire gli account per l'Agente di Autenticazione</i> per i computer con unità già criptate.</p>
<p>Salva il nome utente immesso nell'Agente di Autenticazione</p>	<p>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.</p>
<p>Cripta solo lo spazio su disco utilizzato (riduce i tempi di criptaggio)</p>	<p>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.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>L'abilitazione o la disabilitazione della funzionalità Cripta solo lo spazio su disco utilizzato (Windows 8 e versioni successive) 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.</p> </div>

	<p>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.</p> <p>Se la casella di controllo è deselezionata, viene criptato l'intero disco rigido, inclusi i frammenti residui dei file precedentemente eliminati e modificati.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>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.</p> </div> <p>Questa casella di controllo è deselezionata per impostazione predefinita.</p>
<p>Usa Legacy USB Support (opzione non consigliata)</p>	<p>Questa casella di controllo consente di abilitare o disabilitare la funzione Legacy USB Support. <i>Legacy USB Support</i> 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.</p> <p>Se la casella di controllo è selezionata, il supporto dei dispositivi USB durante l'avvio iniziale del computer sarà abilitato.</p> <div style="border: 1px solid #ccc; background-color: #f8d7da; padding: 10px; margin: 10px 0;"> <p>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.</p> </div>
<p>Impostazioni password</p>	<p>Impostazioni di sicurezza della password dell'account dell'Agente di Autenticazione. È inoltre possibile abilitare l'utilizzo della tecnologia SSO (Single Sign-On).</p> <p>La tecnologia SSO rende possibile l'utilizzo delle stesse credenziali per accedere ai dischi rigidi criptati e al sistema operativo.</p> <p>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.</p> <p>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'accesso ai dischi rigidi criptati e le credenziali dell'account utente del sistema operativo.</p>
<p>Testi della guida</p>	<p>Autenticazione. Testo della guida visualizzato nella finestra dell'Agente di Autenticazione quando si inseriscono le credenziali dell'account.</p> <p>Cambia password. Testo della guida visualizzato nella finestra dell'Agente di Autenticazione quando si modifica la password per l'account dell'Agente di Autenticazione.</p> <p>Ripristina password. Testo della guida visualizzato nella finestra dell'Agente di Autenticazione quando si ripristina la password per l'account dell'Agente di Autenticazione.</p>

Impostazioni del componente Crittografia unità BitLocker

Parametro	Descrizione
<p>Modalità di criptaggio</p>	<p>Cripta tutti i dischi rigidi. Se questo elemento è selezionato, l'applicazione cripta tutti i dischi rigidi quando viene applicato il criterio.</p>

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 questo elemento è selezionato, 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

Questa casella di controllo consente di abilitare o disabilitare l'utilizzo dell'autenticazione tramite 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

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 (Windows 8 e versioni successive)** 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.

	Questa casella di controllo è deselezionata per impostazione predefinita.
Impostazioni di autenticazione	<p>Usa password (sistema operativo Windows 8 e versioni successive)</p> <p>Se questa opzione è selezionata, Kaspersky Endpoint Security richiede una password quando si tenta di accedere a un'unità crittografata.</p> <p>Questa opzione può essere selezionata quando non viene utilizzato un Trusted Platform Module (TPM).</p> <p>Usa Trusted Platform Module (TPM)</p> <p>Se questa opzione è selezionata, BitLocker utilizza Trusted Platform Module (TPM).</p> <p>Per <i>Trusted Platform Module (TPM)</i> 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.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>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.</p> </div> <p>Un dispositivo dotato di un Trusted Platform Module può creare chiavi di criptaggio che possono essere deciptate 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.</p> <p>Questa azione è selezionata per impostazione predefinita.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. È possibile consentire all'utente di utilizzare il PIN avanzato. <i>PIN avanzato</i> consente di utilizzare altri caratteri oltre a quelli numerici: lettere latine maiuscole e minuscole, caratteri speciali e spazi. • Usa Trusted Platform Module (TPM). Se non è disponibile, usa la password. Se la casella di controllo è selezionata, l'utente può utilizzare una password per ottenere l'accesso alle chiavi di criptaggio quando un Trusted Platform Module non è disponibile. <p>Se la casella di controllo è deselezionata e TPM non è disponibile, il criptaggio dell'intero disco non verrà avviato.</p>

Criptaggio a livello di file

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 decipta 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 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.

Impostazioni del componente Criptaggio a livello di file

Parametro	Descrizione
Modalità di criptaggio	<p>Mantieni invariato. Se questo elemento è selezionato, Kaspersky Endpoint Security mantiene invariati i file e le cartelle, senza criptarli o decriptarli.</p> <p>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.</p> <p>Decripta tutto. Se questo elemento è selezionato, Kaspersky Endpoint Security decripta tutti i file e le cartelle criptati.</p>
Regole di criptaggio	<p>Questa scheda mostra le regole di criptaggio per i file archiviati nelle unità locali. È possibile aggiungere file come segue:</p> <ul style="list-style-type: none"> • Cartelle predefinite. Kaspersky Endpoint Security consente di aggiungere le seguenti aree: <ul style="list-style-type: none"> Documenti. File nella cartella <i>Documenti</i> standard del sistema operativo e relative sottocartelle. Preferiti. File nella cartella <i>Preferiti</i> standard del sistema operativo e relative sottocartelle. Desktop. File nella cartella <i>Desktop</i> 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.

	<p>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).</p> <ul style="list-style-type: none"> • 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 <i>Archivi</i>. È inoltre possibile aggiungere manualmente l'estensione del file.
Regole di 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.
Impostazioni password del pacchetto criptato	Requisiti di sicurezza della password da soddisfare durante la creazione di pacchetti criptati.

Criptaggio unità rimovibili

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:

- Criptaggio dell'intero disco (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").

- Criptaggio a livello di file (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. Decrypta 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

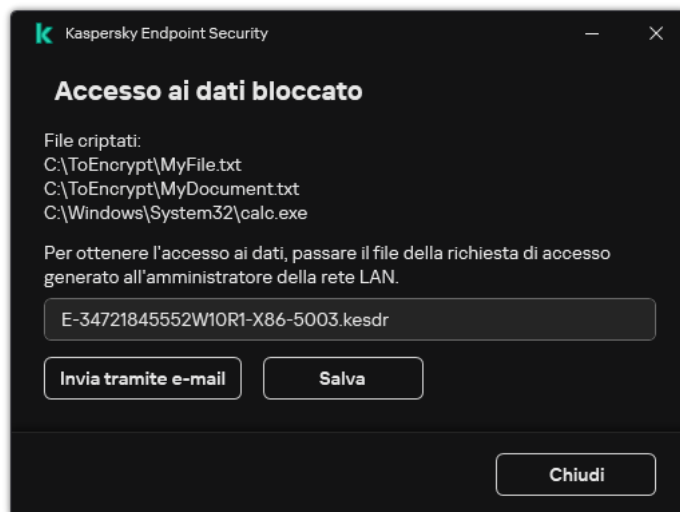
Criptaggio delle impostazioni dei componenti delle unità rimovibili

Parametro	Descrizione
<p>Gestire il criptaggio</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<p>Modalità portatile</p>	<p>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.</p> <p>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.</p> <p>La modalità portatile è disponibile per le modalità Cripta tutti i file o Cripta solo i nuovi file.</p>
<p>Cripta solo lo spazio su disco utilizzato</p>	<p>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.</p> <p>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.</p> <p>Se la casella di controllo è deselezionata, viene criptata l'intera unità, inclusi i frammenti residui dei file precedentemente eliminati e modificati.</p> <p>La possibilità di criptare esclusivamente lo spazio occupato è disponibile solo per la modalità Cripta intera unità rimovibile.</p>

	<p>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.</p>
Regole di criptaggio per i dispositivi selezionati	<p>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:</p> <ul style="list-style-type: none"> • Aggiungere un'unità rimovibile dall'elenco dei dispositivi attendibili per Controllo dispositivi. • Aggiungere manualmente un'unità rimovibile: <ul style="list-style-type: none"> • Per ID dispositivo (ID hardware o HWID) • Per modello dispositivo: ID fornitore (VID) e un ID prodotto (PID)
Consenti il criptaggio delle unità rimovibili in modalità offline	<p>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.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non cripta le unità rimovibili senza una connessione a Kaspersky Security Center.</p>
Impostazioni password modalità portatile	<p>Impostazioni di sicurezza della password per Portable File Manager.</p>

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:

- **A.** 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.** 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.

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. 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](#).

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 di scansione](#).

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 esamina 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. Tuttavia, un'applicazione che è stata aggiunta all'elenco delle applicazioni attendibili viene esclusa dalle scansioni da parte di Kaspersky Endpoint Security.

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. Durante la scansione verranno ignorati gli oggetti utilizzati da questa applicazione.

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.

L'esclusione dalla scansione delle applicazioni attendibili consente di evitare problemi di compatibilità tra Kaspersky Endpoint Security e altri programmi, ad esempio il problema della doppia scansione del traffico di rete di un computer di terze parti da parte di Kaspersky Endpoint Security e di un'altra applicazione anti-virus, nonché di migliorare le prestazioni del computer, aspetto di fondamentale importanza quando si utilizzano applicazioni server.

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.

Parametro	Descrizione
Tipi di oggetti rilevati	<p>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.</p> <ul style="list-style-type: none">• Virus e worm 

Sottocategoria: virus e worm (Viruses_and_Worms)

Livello di pericolosità: 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 sovrascrittura* 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 parassiti* 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 collegamento*, *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.

		<p>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.</p>
IM-Worm	Worm del client IM	<p>Si diffondono attraverso client IM.</p> <p>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.</p>
IRC-Worm	Worm di chat Internet	<p>Penetrano nei computer attraverso le Internet Relay Chat, sistemi utilizzati per comunicare con altre persone in tempo reale via Internet.</p> <p>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.</p>
Net-Worm	Worm di rete	<p>Questi worm si propagano tramite le reti di computer.</p> <p>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.</p>
P2P-Worm	Worm di file sharing	<p>Si propagano attraverso le reti peer-to-peer di file sharing.</p> <p>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.</p> <p>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.</p>
Worm	Altri tipi di worm	<p>Gli altri tipi di worm includono:</p> <ul style="list-style-type: none"> • 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 \(compreso il ransomware\)](#)²

Sottocategoria: Trojan

Livello di pericolosità: 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"	<p>Una volta decompressi, questi archivi aumentano di dimensioni al punto tale da compromettere il funzionamento del computer.</p> <p>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.</p>
Backdoor	Programmi Trojan di amministrazione remota	<p>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.</p> <p>Si installano senza che l'utente ne sia consapevole e consentono a un intruso di gestire il computer in remoto.</p>
Programma Trojan	Trojan	<p>Includono le seguenti applicazioni dannose:</p> <ul style="list-style-type: none">• 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

		<p>reti. Non dispongono delle caratteristiche avanzate di altri tipi di programmi Trojan descritti in questa tabella.</p> <ul style="list-style-type: none"> • Programmi Trojan versatili. Dispongono delle caratteristiche avanzate tipiche di diversi tipi di programmi Trojan.
Trojan-Ransom	Trojan ransom	<p>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.</p>
Trojan-Clicker	Trojan clicker	<p>Accedono a pagine Web dal computer dell'utente, inviando direttamente comandi al browser o sostituendo gli indirizzi Web specificati nei file del sistema operativo.</p> <p>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.</p>
Trojan-Downloader	Trojan downloader	<p>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.</p>
Trojan-Dropper	Trojan dropper	<p>Contengono altri programmi Trojan che copiano nel disco rigido e quindi installano nel computer.</p> <p>Gli intrusi possono utilizzare i Trojan dropper per:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>
Trojan-Proxy	Trojan proxy	<p>Consentono all'intruso di accedere in modo anonimo alle pagine Web utilizzando il computer dell'utente e vengono spesso utilizzati per inviare posta spam.</p>
Trojan-PSW	Password-stealing-ware	<p>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.</p> <p>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).</p>
Trojan-Spy	Programmi Trojan per lo spionaggio dell'utente	<p>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.</p>
Trojan-DDoS	Programmi Trojan per l'esecuzione di attacchi di rete	<p>Inviando 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.</p>

		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	Invisano 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	<p>Un <i>exploit</i> 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.</p> <p>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.</p> <p>Gli exploit vengono utilizzati per propagare i worm di rete. Gli exploit Nuker sono pacchetti di rete che rendono i computer non operativi.</p>

FileCryptor	Strumenti di criptaggio	Criptano altre applicazioni dannose per nascondere alle applicazioni anti-virus.
Flooder	Programmi per il flooding delle reti	<p>Invisano numerosi messaggi tramite i canali di rete. Questi strumenti comprendono ad esempio i programmi utilizzati per il flooding delle Internet Relay Chat.</p> <p>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).</p>
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.
Spoofing	Strumenti di spoofing	Invisano 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 nascondere alle applicazioni anti-virus.
Email-Flooder	Programmi per il flooding degli indirizzi e-mail	Invisano 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	Invisano 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	Invisano numerosi messaggi SMS ai telefoni cellulari.

con messaggi SMS

- [Adware](#) 

Sottocategoria: software pubblicitario (adware);

Livello di pericolosità: 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 legale utilizzabile da utenti 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.
Dialer	Auto-Dialer	Questi programmi sono in grado di stabilire connessioni telefoniche nascoste tramite un modem.
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.

- Rileva altro software utilizzabile da intrusi per danneggiare il computer o i dati personali [?](#)

Sottocategoria: software legale utilizzabile da utenti 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.
Dialer	Auto-Dialer	Questi programmi sono in grado di stabilire connessioni telefoniche nascoste tramite un modem.
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** [?](#)

Kaspersky Endpoint Security esamina gli oggetti compressi e il modulo dell'utilità di decompressione contenuti negli archivi autoestraenti.

Per nascondere i programmi pericolosi ai software anti-virus, gli hacker li comprimono utilizzando appositi programmi di compressione o creano file con compressione multipla.

Gli analisti anti-virus di Kaspersky hanno identificato i programmi di compressione più diffusi tra gli hacker.

Se Kaspersky Endpoint Security rileva un programma di compressione di questo tipo in un file, è probabile che il file contenga un'applicazione dannosa o che potrebbe essere utilizzata da utenti malintenzionati per danneggiare il computer o i dati personali.

Kaspersky Endpoint Security identifica i seguenti tipi di programmi:

- *File compressi potenzialmente pericolosi* – utilizzati per la compressione di malware, come virus, worm e programmi Trojan.
- *File con compressione multipla* (livello di pericolosità medio) – oggetti compressi tre volte con uno o più programmi di compressione.

- **Oggetti con compressione multipla** [?](#)

Kaspersky Endpoint Security esamina gli oggetti compressi e il modulo dell'utilità di decompressione contenuti negli archivi autoestraenti.

Per nascondere i programmi pericolosi ai software anti-virus, gli hacker li comprimono utilizzando appositi programmi di compressione o creano file con compressione multipla.

Gli analisti anti-virus di Kaspersky hanno identificato i programmi di compressione più diffusi tra gli hacker.

Se Kaspersky Endpoint Security rileva un programma di compressione di questo tipo in un file, è probabile che il file contenga un'applicazione dannosa o che potrebbe essere utilizzata da utenti malintenzionati per danneggiare il computer o i dati personali.

Kaspersky Endpoint Security identifica i seguenti tipi di programmi:

- *File compressi potenzialmente pericolosi* – utilizzati per la compressione di malware, come virus, worm e programmi Trojan.
- *File con compressione multipla* (livello di pericolosità medio) – oggetti compressi tre volte con uno o più programmi di compressione.

<p>Esclusioni</p>	<p>Questa tabella contiene informazioni sulle esclusioni dalla scansione.</p> <p>È possibile escludere gli oggetti dalle scansioni utilizzando i seguenti metodi:</p> <ul style="list-style-type: none"> • Specificare il percorso del file o della cartella. • Immettere l'hash dell'oggetto. • Utilizzare le maschere: <ul style="list-style-type: none"> • Il carattere <code>*</code> (asterisco), che sostituisce qualsiasi set di caratteri, eccetto i caratteri <code>\</code> e <code>/</code> (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera <code>C:**.txt</code> includerà tutti i percorsi dei file con l'estensione TXT situata in cartelle sull'unità C:, ma non nelle sottocartelle. • Due caratteri <code>*</code> consecutivi sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome del file o della cartella, compresi i caratteri <code>\</code> e <code>/</code> (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera <code>C:\Folder***.txt</code> includerà tutti i percorsi dei file con l'estensione TXT situati nella cartella denominata <code>Cartella</code> e nelle relative sottocartelle. La maschera deve includere almeno un livello di nidificazione. La maschera <code>C:***.txt</code> non è una maschera valida. • Il carattere <code>?</code> (punto interrogativo), che sostituisce qualsiasi carattere singolo, eccetto i caratteri <code>\</code> e <code>/</code> (i delimitatori dei nomi di file e cartelle nei percorsi di file e cartelle). Ad esempio, la maschera <code>C:\Folder\???.txt</code> includerà i percorsi di tutti i file che si trovano nella cartella denominata <code>Cartella</code> con l'estensione TXT e un nome composto da tre caratteri. • Immettere il nome del tipo di oggetto in base alla classificazione dell'Enciclopedia Kaspersky (ad esempio <code>Email-Worm</code>, <code>Rootkit</code> o <code>RemoteAdmin</code>). È possibile utilizzare maschere con il carattere <code>?</code> (sostituisce un singolo carattere) e il carattere <code>*</code> (sostituisce un numero qualsiasi di caratteri). Se ad esempio viene specificata la maschera <code>Client*</code>, Kaspersky Endpoint Security esclude gli oggetti <code>Client-IRC</code>, <code>Client-P2P</code> e <code>Client-SMTP</code> dalle scansioni.
<p>Applicazioni attendibili</p>	<p>In questa tabella sono elencate le applicazioni attendibili, le cui attività non vengono monitorate da Kaspersky Endpoint Security durante l'esecuzione.</p> <p>Il componente Controllo applicazioni gestisce l'avvio di ogni applicazione indipendentemente dal fatto che questa sia inclusa o meno nella tabella delle applicazioni attendibili.</p>
<p>Unisci i valori quando vengono ereditati</p> <p><i>(disponibile solo in Kaspersky Security Center Console)</i></p>	<p>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.</p> <p>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.</p> <p>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.</p>

	<p>Se gli elementi negli elenchi del criterio padre e figlio corrispondono, questi elementi vengono visualizzati come lo stesso elemento del criterio padre.</p> <p>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.</p>
<p>Consenti l'utilizzo delle esclusioni locali/Consenti l'utilizzo delle applicazioni attendibili locali</p> <p><i>(disponibile solo in Kaspersky Security Center Console)</i></p>	<p><i>Esclusioni locali e applicazioni attendibili locali (area attendibile locale):</i> 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.</p> <p>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.</p> <p>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.</p>
<p>Archivio di certificati di sistema attendibili</p>	<p>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 <i>Attendibili</i>.</p> <p>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.</p>

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

Impostazioni applicazione

Parametro	Descrizione
<p>Avvia Kaspersky Endpoint Security for Windows all'avvio del computer</p>	<p>Quando la casella di controllo è selezionata, Kaspersky Endpoint Security viene avviato dopo il caricamento del sistema operativo, proteggendo il computer durante l'intera sessione.</p> <p>Quando la casella di controllo 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.</p>
<p>Utilizza la</p>	<p>Se la casella è selezionata, viene visualizzata una notifica pop-up quando viene rilevata</p>

<p>tecnologia Disinfezione avanzata (richiede una quantità considerevole di risorse del computer)</p>	<p>un'attività dannosa nel sistema operativo. Nella notifica, Kaspersky Endpoint Security propone all'utente di eseguire la disinfezione avanzata del computer. Dopo l'approvazione di questa procedura da parte dell'utente, Kaspersky Endpoint Security neutralizza la minaccia. Una volta completata la procedura avanzata di disinfezione, Kaspersky Endpoint Security esegue il riavvio del computer. La tecnologia avanzata di disinfezione utilizza considerevoli risorse di elaborazione, pertanto potrebbe rallentare le altre applicazioni.</p> <p>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.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>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 <i>Scansione virus</i>. Quindi, è necessario avviare l'attività <i>Scansione virus</i>.</p> </div>
<p>Usa Kaspersky Security Center come server proxy per l'attivazione <i>(disponibile solo in Kaspersky Security Center Console)</i></p>	<p>Se la casella di controllo è selezionata, Kaspersky Security Center Administration Server viene utilizzato come server proxy durante l'attivazione dell'applicazione.</p>
<p>Abilita Auto-Difesa</p>	<p>Quando la casella di controllo è selezionata, 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.</p>
<p>Consenti la gestione delle impostazioni di Kaspersky Endpoint Security tramite le applicazioni di controllo remoto</p>	<p>Se la casella di controllo è selezionata, le applicazioni di amministrazione remota attendibili (come TeamViewer, LogMeIn Pro e Remotely Anywhere) possono modificare le impostazioni di Kaspersky Endpoint Security.</p> <p>Le applicazioni di amministrazione remota non attendibili non possono modificare le impostazioni di Kaspersky Endpoint Security neanche quando la casella di controllo è selezionata.</p>
<p>Abilita il controllo esterno dei servizi</p>	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security consente la gestione dei servizi dell'applicazione da un computer remoto. Quando viene effettuato un tentativo di gestione dei servizi dell'applicazione in remoto, viene visualizzata una notifica nella barra delle applicazioni di Microsoft Windows (se il servizio di notifica non è stato disabilitato dall'utente).</p>
<p>Rimanda attività pianificate</p>	<p>Se la casella di controllo è selezionata, la modalità di risparmio energetico è abilitata. Le attività pianificate vengono rimandate. È possibile avviare manualmente le attività di scansione e aggiornamento, se necessario.</p>

durante l'alimentazione a batteria	
Concedi risorse alle 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 <i>modalità per trasferire le risorse ad altre applicazioni</i> . 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 concedere risorse ad altre applicazioni.
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 <i>(disponibile solo in Kaspersky Security Center Console)</i>	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 gli stati <i>OK</i> , <i>Avviso</i> e <i>Critico</i> .

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\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\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 associato alle soluzioni Kaspersky Sandbox e Kaspersky Endpoint 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](#) e la [Guida di Kaspersky Endpoint Detection and Response Expert](#).

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.

Impostazioni di rapporti e archivi

Parametro	Descrizione
Mantieni i rapporti per non più di N 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 N 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.
Mantieni gli oggetti per non più di N 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 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 100 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	Dimensione massima della quarantena in MB. Ad esempio, è possibile impostare la dimensione massima della quarantena su 200 MB. Quando la Quarantena raggiunge la

<p>della Quarantena a N MB.</p> <p><i>(disponibile solo in Web Console)</i></p>	<p>dimensione massima, Kaspersky Endpoint Security invia l'evento corrispondente 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.</p>
<p>Invia notifica quando l'archivio Quarantena raggiunge N percento.</p> <p><i>(disponibile solo in Web Console)</i></p>	<p>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.</p>
<p>Trasferimento dei dati ad Administration Server</p> <p><i>(disponibile solo in Kaspersky Security Center)</i></p>	<p>Categorie di eventi nei computer client le cui informazioni devono essere trasmesse ad Administration Server.</p>

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 le scansioni delle connessioni criptate.

Opzioni di rete

Parametro	Descrizione
Limita il traffico sulle connessioni a consumo	<p>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.</p> <p>Limitazione traffico di rete funziona nei computer che eseguono Windows 8 o versioni successive.</p>
Inocula script nel traffico Web per interagire con le pagine Web	<p>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.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>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.</p> </div>
Server proxy	Impostazioni del server proxy utilizzato per l'accesso a Internet degli utenti dei computer

	<p>client. Kaspersky Endpoint Security utilizza queste impostazioni per determinati componenti della protezione, oltre che per l'aggiornamento dei database e dei moduli dell'applicazione.</p> <p>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.</p>
<p>Ignora il server proxy per gli indirizzi locali</p>	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security non utilizza un server proxy durante un aggiornamento da una cartella condivisa.</p>
<p>Porte monitorate</p>	<p>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, Protezione minacce di posta) monitorano i flussi di dati trasmessi tramite qualsiasi porta di rete aperta del computer.</p> <p>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.</p> <p>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.</p> <p>Monitorare tutte le porte per le applicazioni specificate. Viene utilizzato un elenco di applicazioni le cui porte di rete sono monitorate da Kaspersky Endpoint Security.</p>
<p>Scansione delle connessioni criptate</p>	<p>Kaspersky Endpoint Security esamina il traffico di rete criptato trasmesso tramite i seguenti protocolli:</p> <ul style="list-style-type: none"> • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. <p>Kaspersky Endpoint Security supporta le seguenti modalità di scansione delle connessioni criptate:</p> <ul style="list-style-type: none"> • Non esaminare le connessioni criptate. Kaspersky Endpoint Security non avrà accesso ai contenuti dei siti Web i cui indirizzi iniziano con <code>https://</code>. • 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 file, 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.

	<p>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.</p>
<p>Certificati radice attendibili</p>	<p>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.</p>
<p>Quando si visita un dominio con un certificato non attendibile</p>	<ul style="list-style-type: none"> • 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 <i>Non attendibile</i>. 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 connessione. 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.
<p>Quando si verificano errori durante la scansione delle connessioni criptate</p>	<ul style="list-style-type: none"> • Blocca connessione. Se questo elemento è selezionato, quando si verifica un errore di scansione delle connessioni criptate, Kaspersky Endpoint Security blocca la connessione di rete. • Aggiungi dominio alle esclusioni. Se questo elemento è selezionato, quando 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 connessione. Kaspersky Endpoint Security genera anche un evento per l'errore di scansione della connessione criptata.
<p>Blocca le connessioni SSL 2.0 (opzione consigliata)</p>	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security blocca le connessioni di rete stabilite tramite il protocollo SSL 2.0.</p>

	<p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non blocca le connessioni di rete stabilite tramite il protocollo SSL 2.0 e non monitora il traffico di rete trasmesso mediante queste connessioni.</p>
<p>Decripta le connessioni criptate con i siti Web che utilizzano certificati EV</p>	<p>I certificati EV (Extended Validation) 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.</p> <p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security decripta e monitora le connessioni criptate con siti Web che utilizzano un certificato EV.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security 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 <code>https://bing.com</code>.</p> <p>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.</p>
<p>Indirizzi attendibili</p>	<p>Viene utilizzato un elenco di indirizzi Web per cui Kaspersky Endpoint Security non esamina le connessioni di rete. È possibile immettere un nome di dominio o un indirizzo IP. Kaspersky Endpoint Security supporta il carattere <code>*</code> per l'immissione di una maschera nel nome di dominio.</p> <div data-bbox="373 943 1493 1133" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security non supporta le maschere per gli indirizzi IP. È possibile immettere un intervallo di indirizzi IP nell'interfaccia dell'applicazione locale (ad esempio 198.51.100.0/24). Non è possibile immettere un intervallo di indirizzi IP in Kaspersky Security Center Console.</p> </div> <p>Esempi:</p> <ul style="list-style-type: none"> • <code>domain.com</code> - Il record comprende i seguenti indirizzi: <code>https://domain.com</code>, <code>https://www.domain.com</code>, <code>https://domain.com/page123</code>. Il record è esclusivo dei sottodomini (ad esempio, <code>subdomain.domain.com</code>). • <code>subdomain.domain.com</code> - Il record comprende i seguenti indirizzi: <code>https://subdomain.domain.com</code>, <code>https://subdomain.domain.com/page123</code>. Il record è esclusivo del dominio <code>domain.com</code>. • <code>*.domain.com</code> - Il record comprende i seguenti indirizzi: <code>https://movies.domain.com</code>, <code>https://images.domain.com/page123</code>. Il record è esclusivo del dominio <code>domain.com</code>.
<p>Applicazioni attendibili</p>	<p>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 <code>*</code> e <code>?</code> durante l'immissione di una maschera.</p>
<p>Utilizza l'archivio certificati selezionato per eseguire la scansione delle connessioni</p>	<p>Se questa casella di controllo è selezionata, Kaspersky Endpoint Security 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.</p>

criptate nelle applicazioni Mozilla

(disponibile solo nell'interfaccia di Kaspersky Endpoint Security)

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, Kaspersky Endpoint Security non esamina il traffico nel browser Mozilla Firefox e nel client di posta Thunderbird.



Kaspersky Endpoint Security 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.

- **Usa archivio certificati Windows (consigliato).** Il certificato radice di Kaspersky viene aggiunto a questo archivio durante l'installazione di Kaspersky Endpoint Security.
- **Usa archivio certificati Mozilla.** 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.

Impostazioni dell'interfaccia

Parametro	Descrizione
Interazione con l'utente (disponibile solo in Kaspersky Security Center Console)	<p>Con 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 visualizza inoltre le notifiche sopra l'icona dell'applicazione.</p> <p>Con interfaccia 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.</p> <p>Nascondi sezione Monitor attività applicazioni. Sul computer client, nella finestra principale di Kaspersky Endpoint Security, il pulsante Monitor attività applicazioni non è disponibile. <i>Monitor attività applicazioni</i> è uno strumento progettato per la visualizzazione in tempo reale di informazioni sulle attività delle applicazioni nel computer di un utente.</p> <p>Nessuna interfaccia. 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.</p>
Impostazioni di notifica	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.
Impostazioni delle notifiche via e-mail	Impostazioni del server SMTP per l'invio delle notifiche sugli eventi registrati durante il funzionamento dell'applicazione.
Mostra lo stato dell'applicazione	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.

nell'area di notifica	
Notifiche dello stato dei database anti-virus locali	Impostazioni delle notifiche sui database anti-virus non aggiornati utilizzati dall'applicazione.
Protezione tramite password	<p>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.</p> <p>Dopo l'abilitazione di Protezione tramite password, Kaspersky Endpoint Security richiede all'utente di impostare una password per eseguire le operazioni.</p>
Risorse Web dell'Assistenza tecnica <i>(disponibile solo in Kaspersky Security Center Console)</i>	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.
Messaggio per l'utente <i>(disponibile solo in Kaspersky Security Center Console)</i>	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 in qualsiasi momento le impostazioni consigliate da Kaspersky per Endpoint Security. 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.

Gli aggiornamenti periodici richiedono una licenza valida. Se non è disponibile alcuna licenza, è possibile eseguire un aggiornamento una sola volta.

La principale sorgente degli aggiornamenti per Kaspersky Endpoint Security è costituita dai server degli aggiornamenti Kaspersky.

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.

I file della Guida sensibile al contesto possono essere aggiornati insieme agli aggiornamenti dei moduli dell'applicazione.

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](#).

Impostazioni di aggiornamento dei database e dei moduli dell'applicazione

Parametro	Descrizione
Pianificazione aggiornamento database	<p>Automaticamente. In questa modalità, Kaspersky Endpoint Security 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.</p> <p>Manualmente. Questa modalità di esecuzione dell'attività di aggiornamento consente di avviare manualmente l'attività.</p> <p>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.</p>
Esegui attività non effettuate	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security avvia l'attività di aggiornamento ignorata appena possibile. L'attività di aggiornamento può ad esempio essere ignorata se il computer è spento all'orario impostato per l'avvio dell'attività di aggiornamento.</p> <p>Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non avvia le attività di aggiornamento ignorate. Viene invece eseguita l'attività di aggiornamento successiva, in base alla pianificazione corrente.</p>
Sorgente degli aggiornamenti	<p>Una <i>sorgente degli aggiornamenti</i> è una risorsa che contiene gli aggiornamenti per i database e i moduli dell'applicazione di Kaspersky Endpoint Security.</p> <p>Le sorgenti degli aggiornamenti includono il server Kaspersky Security Center, i server degli aggiornamenti Kaspersky e cartelle di rete o locali.</p> <p>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.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security non supporta gli aggiornamenti dai server HTTPS, a meno che non si tratti dei server degli aggiornamenti Kaspersky.</p> </div> <p>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.</p>
Esegui aggiornamenti dei database come	<p>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 di Kaspersky Endpoint Security è possibile specificare un utente che dispone di tali diritti e avviare l'attività di aggiornamento di Kaspersky Endpoint Security utilizzando tale account utente.</p>
Scarica aggiornamenti	<p>Download degli aggiornamenti del modulo dell'applicazione con gli aggiornamenti del database dell'applicazione.</p>

<p>dei moduli dell'applicazione</p>	<p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>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.</p> </div> <p>Questa casella di controllo è selezionata per impostazione predefinita.</p>
<p>Copia aggiornamenti nella cartella</p>	<p>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\Update distribution\.</p>
<p>Server proxy per gli aggiornamenti <i>(disponibile solo nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>Impostazioni del server proxy per l'accesso a Internet degli utenti dei computer client per aggiornare i moduli e i database dell'applicazione.</p> <p>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.</p>
<p>Ignora il server proxy per gli indirizzi locali <i>(disponibile solo nell'interfaccia di Kaspersky Endpoint Security)</i></p>	<p>Se la casella di controllo è selezionata, Kaspersky Endpoint Security non utilizza un server proxy durante un aggiornamento da una cartella condivisa.</p>

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:

- **Attendibile.** 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

eml – messaggio e-mail Microsoft Outlook Express

nws – nuovo messaggio di posta elettronica Microsoft Outlook Express

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

eml – messaggio e-mail Microsoft Outlook Express

nws – nuovo messaggio di posta elettronica Microsoft Outlook Express

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, xlsxm per i modelli di Microsoft Office Excel 2007 con supporto per le macro, 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

Appendice 5. Impostazioni di rete per l'interazione con servizi esterni

Kaspersky Endpoint Security utilizza le seguenti impostazioni di rete per interagire con i servizi esterni.

Impostazioni di Rete

Indirizzo	Descrizione
activation- v2.kaspersky.com/activation-service/activation-service.svc Protocollo: HTTPS Porta: 443	Attivazione dell'applicazione.
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	<ul style="list-style-type: none"> • Aggiornamento di database e moduli software dell'applicazione.

- Verifica dell'accessibilità dei server Kaspersky. Se l'accesso ai server tramite il DNS di sistema non è possibile, l'applicazione utilizza il DNS pubblico. Ciò è necessario per assicurarsi che i database anti-virus siano aggiornati e che il livello di sicurezza sia garantito per il computer. 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 gli indirizzi dei domini e l'indirizzo IP pubblico dell'utente perché 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, il trattamento dei dati è disciplinato dall'informativa sulla privacy del servizio pertinente. Se si desidera impedire a Kaspersky Endpoint Security di utilizzare un server DNS pubblico, contattare l'Assistenza tecnica per richiedere una patch privata.

<p>touch.kaspersky.com</p> <p>Protocollo: HTTP</p>	<ul style="list-style-type: none"> • Ricezione dell'ora attendibile per il controllo del periodo di validità del certificato (connessione TLS). • Avviso relativo al rifiuto dell'accesso a una risorsa Web nel browser (Protezione minacce Web e Controllo Web).
<p>p00.upd.kaspersky.com</p> <p>p01.upd.kaspersky.com</p> <p>p02.upd.kaspersky.com</p> <p>p03.upd.kaspersky.com</p> <p>p04.upd.kaspersky.com</p> <p>p05.upd.kaspersky.com</p> <p>p06.upd.kaspersky.com</p> <p>p07.upd.kaspersky.com</p> <p>p08.upd.kaspersky.com</p> <p>p09.upd.kaspersky.com</p> <p>p10.upd.kaspersky.com</p> <p>p11.upd.kaspersky.com</p> <p>p12.upd.kaspersky.com</p> <p>p13.upd.kaspersky.com</p> <p>p14.upd.kaspersky.com</p> <p>p15.upd.kaspersky.com</p> <p>p16.upd.kaspersky.com</p> <p>p17.upd.kaspersky.com</p> <p>p18.upd.kaspersky.com</p> <p>p19.upd.kaspersky.com</p> <p>downloads.kaspersky-labs.com</p> <p>cm.k.kaspersky-labs.com</p> <p>Protocollo: HTTP</p> <p>Porta: 80</p>	<p>Aggiornamento di database e moduli software dell'applicazione.</p>
<p>ds.kaspersky.com</p> <p>Protocollo: HTTPS</p> <p>Porta: 443</p>	<p>Utilizzo di Kaspersky Security Network.</p>
<p>ksn-a-stat-geo.kaspersky-labs.com</p> <p>ksn-file-geo.kaspersky-labs.com</p> <p>ksn-verdict-geo.kaspersky-labs.com</p> <p>ksn-url-geo.kaspersky-labs.com</p> <p>ksn-a-p2p-geo.kaspersky-labs.com</p> <p>ksn-info-geo.kaspersky-labs.com</p>	<p>Utilizzo di Kaspersky Security Network.</p>

ksn-cinfo-geo.kaspersky-labs.com Protocollo: Qualsiasi Porta: 443,1443	
click.kaspersky.com redirect.kaspersky.com Protocollo: HTTPS	Seguire i collegamenti presenti nell'interfaccia.
cr1.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, 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 - Messaggio informativo (📄), 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.

Eventi critici

[Violazione del Contratto di licenza con l'utente finale](#) 

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)	

[Azione se viene rilevata una minaccia. È consigliabile 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 da 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 da 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)	✓




Connessione a un dominio con un certificato non attendibile stabilita

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 Prevenzione Exploit Scansione virus
ID evento di Windows	302
ID evento di Kaspersky Security Center	GNRL_EV_VIRUS_FOUND
Parametri dell'evento	<ul style="list-style-type: none"> 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, ad esempio Trojware. GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore). Tecnologie di rilevamento delle minacce (metodo). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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 Prevenzione Exploit Scansione virus
ID evento di Windows	302
ID evento di Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_BY_KSN
Parametri dell'evento	<ul style="list-style-type: none">• 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, ad esempio Trojware.• GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore). Tecnologie di rilevamento delle minacce (metodo). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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 Scansione virus
ID evento di Windows	312
ID evento di Kaspersky Security Center	GNRL_EV_OBJECT_NOTCURED
Parametri dell'evento	<ul style="list-style-type: none"> 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, ad esempio Trojware. GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore). Tecnologie di rilevamento delle minacce (metodo). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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 Scansione virus
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 virus
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 virus
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 virus
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	<ul style="list-style-type: none"> • 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, ad esempio Trojware. • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore). Tecnologie di rilevamento delle minacce (metodo). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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	<ul style="list-style-type: none"> • 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, ad esempio Trojware. • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore). Tecnologie di rilevamento delle minacce (metodo). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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	<ul style="list-style-type: none"> • 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, ad esempio Trojware. • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore). Tecnologie di rilevamento delle minacce (metodo). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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	<ul style="list-style-type: none"> • 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 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	<ul style="list-style-type: none"> • 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 12B012B012B012B012B012B012B0. • 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	<ul style="list-style-type: none"> • 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)	



[Il processo non consentito è stato 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 \(basi locali\)](#)

Stato	
Componente	Controllo Web
ID evento di Windows	752
ID evento di Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Parametri dell'evento	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	

Errore durante l'aggiornamento del componente

Stato	
Componente	Aggiornamento database
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 durante la distribuzione degli aggiornamenti del componente

Stato	
Componente	Aggiornamento database
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 database
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 della rete

Stato	
Componente	Aggiornamento database
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 database
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 database
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 database
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 database
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 dell'aggiornamento non riuscita

Stato	
Componente	Aggiornamento database
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 della patch non riuscita](#)

Stato	
Componente	Aggiornamento database
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 database
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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 di gestione degli account di Agente di Autenticazione è terminata 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)	✓


[Impossibile applicare il criterio](#)

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 \(per ulteriori informazioni, consultare la Guida in linea di Kaspersky Endpoint Security for Windows\)](#)

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 di 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	Kaspersky 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 \(Kaspersky Sandbox\)](#)

Stato	
Componente	Kaspersky 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	Kaspersky 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 Kaspersky Sandbox non valido](#)

Stato	
Componente	Kaspersky 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 Kaspersky Sandbox non è disponibile](#)

Stato	
Componente	Kaspersky 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)	✓


[Si è verificato un errore durante l'elaborazione dell'oggetto in Kaspersky Sandbox](#)

Stato	
Componente	Kaspersky 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)	✓

[Il carico massimo su Kaspersky Sandbox è stato superato](#)

Stato	
Componente	Kaspersky 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)	-


[IOC trovato](#)

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 Kaspersky Sandbox non riuscita](#)

Stato	
Componente	Kaspersky 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)	✓




[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 dello 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)	

[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)	

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 di 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 sta per scadere

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 Prevenzione Exploit Protezione minacce Web
ID evento di Windows	331
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	
Registro eventi di Kaspersky Security Center (predefinito)	–


Impossibile ripristinare l'oggetto 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)	✓

[Lo spazio nell'archivio Quarantena è 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 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 Prevenzione Intrusioni Host Scansione virus
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 virus
ID evento di Windows	314
ID evento di Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Parametri dell'evento	<ul style="list-style-type: none">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, ad esempio Trojware.GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore). Tecnologie di rilevamento delle minacce (metodo). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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 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 virus
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 Scansione virus
ID evento di Windows	303
ID evento di Kaspersky Security Center	GNRL_EV_SUSPICIOUS_OBJECT_FOUND
Parametri dell'evento	<ul style="list-style-type: none"> • 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, ad esempio Trojware.
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 Scansione virus
ID evento di Windows	303
ID evento di Kaspersky Security Center	GNRL_EV_SUSPICIOUS_OBJECT_FOUND
Parametri dell'evento	<ul style="list-style-type: none"> • 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, ad esempio Trojware.
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 Scansione virus
ID evento di Windows	307
ID evento di Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
Parametri dell'evento	<ul style="list-style-type: none"> • 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, ad esempio Trojware. • GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore). Tecnologie di rilevamento delle minacce (metodo). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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 virus
ID evento di Windows	306
ID evento di Kaspersky Security Center	GNRL_EV_OBJECT_CURED
Parametri dell'evento	<ul style="list-style-type: none"> 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, ad esempio Trojware. GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore).Tecnologie di rilevamento delle minacce (metodo).Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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 virus
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 Prevenzione Exploit Prevenzione Intrusioni Host Protezione minacce file Scansione virus
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 Prevenzione Exploit Scansione virus
ID evento di Windows	455
ID evento di Kaspersky Security Center	000001c7
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	<ul style="list-style-type: none"> 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, ad esempio Trojware. GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore?). Tecnologie di rilevamento delle minacce (metodo?). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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	<ul style="list-style-type: none"> 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, ad esempio Trojware. GNRL_EA_PARAM_9 sono informazioni aggiuntive sull'oggetto rilevato: Componente dell'applicazione (motore). Tecnologie di rilevamento delle minacce (metodo). Minaccia rilevata dall'istanza privata di KSN (lista vietati): 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 database
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
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	Sensore Endpoint
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	Sensore Endpoint
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 Kaspersky Anti Targeted Attack Platform dall'amministratore 

Stato	
Componente	Sensore Endpoint
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	Sensore Endpoint
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	Sensore Endpoint
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 (Kaspersky Sandbox) ⓘ

Stato	
Componente	Kaspersky 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	Kaspersky 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 processo 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)	



[Interruzione 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)	✓



[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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 del 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	

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 bloccato l'operazione relativa alle risorse dell'applicazione](#)

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 utilizza 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 Prevenzione Intrusioni Host Kaspersky Sandbox Scansione virus
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 virus
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 virus
ID evento di Windows	322
ID evento di Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Parametri dell'evento	<ul style="list-style-type: none"> 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 (motore). Tecnologie di rilevamento delle minacce (metodo). 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 virus
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 KSN Privato](#)

Stato	
Componente	Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Prevenzione Intrusioni Host Scansione virus
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 Scansione virus
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 virus
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 virus
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 virus
ID evento di Windows	318
ID evento di Kaspersky Security Center	-
Registro eventi di Windows (predefinito)	
Registro eventi di Kaspersky Security Center (predefinito)	-


[Oggetto compresso rilevato](#)

Stato	
Componente	Prevenzione Intrusioni Host Protezione minacce file Protezione minacce Web Protezione minacce di posta Protezione AMSI Scansione virus
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 database
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 database
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 KSN Privato](#)

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 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 database
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 database
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](#)

Stato	
Componente	Aggiornamento database
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 database
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 database
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 database
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 database
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 database
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 database
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](#)

Stato	
Componente	Aggiornamento database
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 database
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 database
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 database
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 database
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 database
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 database
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)	✓

[Sensore Endpoint connesso al server [?]](#)

Stato	
Componente	Sensore Endpoint
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	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 (Kaspersky Sandbox)

Stato	
Componente	Kaspersky 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 (Kaspersky Sandbox) ⓘ

Stato	ⓘ
Componente	Kaspersky 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 aggiunto a 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	Kaspersky 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	Kaspersky 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	Kaspersky 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	Kaspersky Sandbox
ID evento di Windows	2616
ID evento di Kaspersky Security Center	–
Registro eventi di Windows (predefinito)	
Registro eventi di Kaspersky Security Center (predefinito)	–



[Rilevamento Kaspersky Sandbox asincrono](#)

Stato	
Componente	Kaspersky Sandbox
ID evento di Windows	2619
ID evento di Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
Parametri dell'evento	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 corrisponde alle impostazioni del componente Kaspersky 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)	

[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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	

Informazioni sul codice di terze parti

Le informazioni sul codice di terze parti sono contenute nel file denominato legal_notices.txt, disponibile nella cartella di installazione dell'applicazione.

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 Systems Incorporated negli Stati Uniti e/o in altri paesi.

Apple, FireWire, iTunes e Safari sono marchi di Apple, Inc., registrati negli Stati Uniti e in altri paesi.

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 il logo Bluetooth sono di proprietà di Bluetooth SIG, Inc.

Borland è un marchio o un marchio registrato di Borland Software Corporation.

Android e Google Chrome sono marchi di Google, Inc.

Citrix e Citrix Provisioning Services e XenDesktop sono marchi di Citrix Systems, Inc. e/o di una o più delle relative filiali e possono essere registrati presso il Patent and Trademark Office degli Stati Uniti e in altri paesi.

Dell è un marchio di Dell, Inc. o delle relative filiali.

dBase è un marchio di dataBased Intelligence, Inc.

EMC è un marchio o un marchio registrato di EMC Corporation negli Stati Uniti e/o in altri paesi.

Foxit è un marchio registrato di Foxit Corporation.

Radmin è un marchio registrato di Famatech.

IBM è un marchio registrato di International Business Machines Corporation in diverse giurisdizioni di tutto il mondo.

Intel è un marchio di Intel Corporation negli Stati Uniti e/o in altri paesi.

IOS e Any Connect sono marchi registrati di Cisco Systems, Inc. e/o delle relative consociate negli Stati Uniti e in altri paesi.

Lenovo e 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, Inc. negli Stati Uniti e in altri paesi.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface e Hyper-V sono marchi di Microsoft Corporation negli Stati Uniti e in altri paesi.

Mozilla, Firefox e Thunderbird sono marchi di Mozilla Foundation.

Java e JavaScript sono marchi registrati di Oracle e/o delle relative consociate.

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 ESX, VMware ESXi e VMware Workstation sono marchi o marchi registrati di VMware, Inc. negli Stati Uniti e/o in altre giurisdizioni.

Tor è un marchio registrato di The Tor Project, n. di registrazione Stati Uniti 3.465.432.

Thawte è un marchio o un marchio registrato di Symantec Corporation o delle relative consociate negli Stati Uniti e in altri paesi.

SAMSUNG è un marchio di SAMSUNG negli Stati Uniti e in altri paesi.