kaspersky

# Kaspersky Endpoint Security 10 Service Pack 2 for Windows

# Sommario


Informazioni su Kaspersky Endpoint Security 10 Service Pack 2 for Windows
- Novità
- Kit di distribuzione
- Organizzazione della protezione del computer
- Requisiti hardware e software

Installazione e rimozione dell'applicazione
- Installazione dell'applicazione
  - Informazioni sulle modalità di installazione dell'applicazione
  - Installazione dell'applicazione tramite l'Installazione guidata
    - Passaggio 1. Verifica dei requisiti di installazione
    - Passaggio 2. Pagina iniziale della procedura di installazione
    - Passaggio 3. Visualizzazione del Contratto di licenza
    - Passaggio 4. Selezione del tipo di installazione
    - Passaggio 5. Selezione dei componenti dell'applicazione da installare
    - Passaggio 6. Selezione della cartella di destinazione
    - Passaggio 7. Aggiunta di esclusioni dalla scansione virus
    - Passaggio 8. Preparazione per l'installazione dell'applicazione
    - Passaggio 9. Installazione dell'applicazione
  - Installazione dell'applicazione dalla riga di comando
  - Installazione remota dell'applicazione tramite System Center Configuration Manager
  - Descrizione delle impostazioni di installazione del file setup.ini
  - Configurazione iniziale guidata
    - Attivazione dell'applicazione
    - Attivazione con un codice di attivazione
    - Attivazione tramite un file chiave
    - Selezione delle funzioni da attivare
    - Completamento dell'attivazione
    - Analisi del sistema operativo
    - Completamento della configurazione iniziale dell'applicazione
    - Informativa di Kaspersky Security Network
  - Informazioni sulle modalità di aggiornamento di una versione precedente dell'applicazione
- Rimozione dell'applicazione
  - Informazioni sulle modalità di rimozione dell'applicazione
  - Rimozione dell'applicazione tramite l'Installazione guidata
    - Passaggio 1. Salvataggio dei dati dell'applicazione per il riutilizzo
    - Passaggio 2. Conferma della rimozione dell'applicazione
    - Passaggio 3. Rimozione dell'applicazione. Completamento della rimozione
  - Rimozione dell'applicazione dalla riga di comando
  - Rimozione degli oggetti e dei dati rimanenti in seguito all'operazione di verifica dell'agente di autenticazione

Interfaccia dell'applicazione
- Icona dell'applicazione nell'area di notifica della barra delle applicazioni
- Menu di scelta rapida dell'icona dell'applicazione
- Finestra principale dell'applicazione
- Scheda Configura le impostazioni dell'applicazione
- Scheda Protezione e controllo

Licensing dell'applicazione

Informazioni sul Contratto di licenza con l'utente finale
Informazioni sulla licenza
Informazioni sul certificato di licenza
Informazioni sull'abbonamento
Informazioni sul codice di attivazione
Informazioni sulla chiave
Informazioni sul file chiave
Informazioni sulla trasmissione dei dati
Visualizzazione delle informazioni sulla licenza
Acquisto di una licenza
Rinnovo di una licenza
Rinnovo dell'abbonamento
Apertura del sito Web del fornitore del servizio
Informazioni sui metodi di attivazione dell'applicazione
Utilizzo dell'Attivazione guidata per attivare l'applicazione
Attivazione dell'applicazione dalla riga di comando
Avvio e arresto dell'applicazione
Abilitazione e disabilitazione dell'avvio automatico dell'applicazione
Avvio e arresto manuale dell'applicazione
Sospensione e ripresa della protezione e del controllo del computer
Protezione del file system del computer. Anti-Virus File
Informazioni su Anti-Virus File
Abilitazione e disabilitazione di Anti-Virus File
Sospensione automatica di Anti-Virus File
Configurazione di Anti-Virus File
Modifica del livello di protezione
Modifica dell'azione di Anti-Virus File da eseguire sui file infetti
Modifica dell'ambito di protezione di Anti-Virus File
Utilizzo dell'analizzatore euristico con Anti-Virus File
Utilizzo delle tecnologie di scansione durante l'esecuzione di Anti-Virus File
Ottimizzazione della scansione dei file
Scansione dei file compositi
Modifica della modalità di scansione
Protezione dei messaggi e-mail. Anti-Virus Posta
Informazioni su Anti-Virus Posta
Abilitazione e disabilitazione di Anti-Virus Posta
Configurazione di Anti-Virus Posta
Modifica del livello di protezione per i messaggi e-mail
Modifica dell'azione da eseguire sui messaggi e-mail infetti
Modifica dell'ambito di protezione di Anti-Virus Posta
Scansione dei file compositi allegati ai messaggi e-mail
Filtro degli allegati dei messaggi e-mail
Scansione dei messaggi e-mail in Microsoft Office Outlook
Configurazione della scansione dei messaggi in Outlook
Configurazione della scansione dei messaggi tramite Kaspersky Security Center
Protezione del computer su Internet. Anti-Virus Web
Informazioni su Anti-Virus Web
Abilitazione e disabilitazione di Anti-Virus Web

- Configurazione di Anti-Virus Web
  - Modifica del livello di protezione del traffico Web
  - Modifica dell'azione da eseguire sugli oggetti dannosi del traffico Web
  - Verifica delle URL tramite i database di indirizzi Web dannosi e di phishing con Anti-Virus Web
  - Utilizzo dell'analizzatore euristico con Anti-Virus Web
  - Modifica dell'elenco di URL attendibili
- Protezione del traffico dei client IM. Anti-Virus IM
  - Informazioni su Anti-Virus IM
  - Abilitazione e disabilitazione di Anti-Virus IM
  - Configurazione di Anti-Virus IM
    - Creazione dell'ambito di protezione di Anti-Virus IM
    - Scansione delle URL rispetto ai database delle URL dannose e di phishing con Anti-Virus IM
- System Watcher
  - Informazioni su System Watcher
  - Abilitazione e disabilitazione di System Watcher
  - Configurazione di System Watcher
    - Abilitazione e disabilitazione della protezione dagli exploit
    - Scelta dell'azione da eseguire in caso di rilevamento di attività dannose in un programma
    - Abilitazione e disabilitazione del rollback delle azioni del malware durante la disinfezione
- Firewall
  - Informazioni su Firewall
  - Abilitazione o disabilitazione di Firewall
  - Informazioni sulle regole di rete
  - Informazioni sulla categoria della connessione di rete
  - Modifica della categoria della connessione di rete
  - Gestione delle regole per i pacchetti di rete
    - Creazione e modifica 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
  - Gestione delle regole di rete delle applicazioni
    - Creazione e modifica di una regola di rete per un'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
    - Informazioni su Monitor di Rete
    - Avvio di Monitor di Rete
- Prevenzione attacchi di rete
  - Informazioni su Prevenzione attacchi di rete
  - Abilitazione e disabilitazione di Prevenzione attacchi di rete
  - Impostazioni Prevenzione attacchi di rete
    - Modifica delle impostazioni utilizzate per il blocco di un computer che origina un attacco
    - Configurazione degli indirizzi delle esclusioni dal blocco
- Prevenzione Attacchi BadUSB
  - Informazioni su Prevenzione unità USB dannose
  - Installazione del componente Prevenzione Attacchi BadUSB
  - Abilitazione e disabilitazione di Prevenzione Attacchi BadUSB

Autorizzazione o divieto dell'utilizzo di Tastiera sullo schermo per l'autorizzazione
Autorizzazione tastiera
Controllo avvio applicazioni
Informazioni su Controllo avvio applicazioni
Abilitazione e disabilitazione di Controllo avvio applicazioni
Limitazioni delle funzionalità di Controllo avvio applicazioni
Informazioni sulle regole di Controllo avvio applicazioni
Gestione delle regole di Controllo avvio applicazioni
Aggiunta e modifica di una regola di Controllo avvio applicazioni
Aggiunta di una condizione di attivazione a una regola di Controllo avvio applicazioni
Modifica dello stato di una regola di Controllo avvio applicazioni
Verifica delle regole di Controllo avvio applicazioni
Modifica dei modelli dei messaggi di Controllo avvio applicazioni
Informazioni sulle modalità di esecuzione di Controllo avvio applicazioni
Selezione della modalità di Controllo avvio applicazioni
Gestione delle regole di Controllo avvio applicazioni tramite Kaspersky Security Center
Raccolta delle informazioni sulle applicazioni installate nei computer degli utenti
Creazione delle categorie di applicazioni
Creazione delle regole di Controllo avvio applicazioni tramite Kaspersky Security Center
Modifica dello stato di una regola di Controllo avvio applicazioni tramite Kaspersky Security Center
Controllo privilegi applicazioni
Informazioni su Controllo privilegi applicazioni
Limitazioni del controllo dei dispositivi audio e video
Abilitazione e disabilitazione di Controllo privilegi applicazioni
Gestione dei gruppi di attendibilità delle applicazioni
Configurazione delle impostazioni per l'assegnazione delle applicazioni ai gruppi di attendibilità
Modifica di un gruppo di attendibilità
Selezione di un gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security
Gestione delle regole di controllo applicazioni
Modifica delle regole di controllo applicazioni per gruppi di attendibilità e gruppi di applicazioni
Modifica di una regola di controllo delle applicazioni
Disabilitazione dei download e degli aggiornamenti delle regole di controllo delle applicazioni dal database di Kaspersky Security Network
Disabilitazione dell'ereditarietà delle restrizioni dal processo principale
Esclusione di specifiche azioni delle applicazioni dalle regole di controllo delle applicazioni
Rimozione delle regole di Controllo Applicazioni obsolete
Protezione delle risorse del sistema operativo e dei dati di identità
Aggiunta di una categoria di risorse protette
Aggiunta di una risorsa protetta
Disabilitazione della protezione di una risorsa
Monitor vulnerabilità
Informazioni su Monitor vulnerabilità
Abilitazione e disabilitazione di Monitor vulnerabilità
Controllo dispositivi
Informazioni su Controllo dispositivi
Abilitazione e disabilitazione di Controllo dispositivi
Informazioni sulle regole di accesso a dispositivi e bus di connessione
Informazioni sui dispositivi attendibili

- Decisioni standard sull'accesso ai dispositivi
- Modifica di una regola di accesso ai dispositivi
- Aggiunta o esclusione di record del registro eventi
- Aggiunta di una rete Wi-Fi all'elenco delle reti attendibili
- Modifica di una regola di accesso ai bus di connessione
- Azioni con i dispositivi attendibili
  - Aggiunta di un dispositivo all'elenco Attendibili dall'interfaccia dell'applicazione
  - Aggiunta di un dispositivo all'elenco Attendibili in base al modello o all'ID del dispositivo
  - Aggiunta di un dispositivo all'elenco Attendibili in base alla maschera per l'ID del dispositivo
  - Configurazione dell'accesso utente a un dispositivo attendibile
  - Rimozione di un dispositivo dall'elenco dei dispositivi attendibili
- Modifica dei modelli dei messaggi di Controllo dispositivi
- Ottenimento dell'accesso a un dispositivo bloccato
- Creazione di una chiave per l'accesso a dispositivo bloccato tramite Kaspersky Security Center

Controllo Web
- Informazioni su Controllo Web
- Abilitazione e disabilitazione di Controllo Web
- Categorie di contenuti delle risorse Web
- Informazioni sulle regole di accesso alle risorse Web
- Azioni con le regole di accesso alle risorse Web
  - Aggiunta e modifica di una regola di accesso alle risorse Web
  - Assegnazione di priorità alle regole di accesso alle risorse Web
  - Verifica delle regole di accesso alle risorse Web
  - Abilitazione e disabilitazione di una regola di accesso alle risorse Web
- Migrazione delle regole di accesso alle risorse Web da versioni precedenti dell'applicazione
- Esportazione e importazione dell'elenco di indirizzi delle risorse Web
- Modifica delle maschere per gli indirizzi di risorse Web
- Modifica dei modelli dei messaggi di Controllo Web

KATA Endpoint Sensor
- Informazioni su KATA Endpoint Sensor
- Abilitazione e disabilitazione del componente KATA Endpoint Sensor

Criptaggio dei dati
- Abilitazione della visualizzazione delle impostazioni di criptaggio nel criterio di Kaspersky Security Center
- Informazioni sul criptaggio dei dati
- Limitazioni della funzionalità di criptaggio
- Modifica dell'algoritmo di criptaggio
- Abilitazione della tecnologia Single Sign-On (SSO)
- Considerazioni speciali sul criptaggio dei file
- Criptaggio dei 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
  - Estrazione di pacchetti criptati
- Criptaggio delle unità rimovibili
  - Avvio del criptaggio delle unità rimovibili

Aggiunta di una regola di criptaggio per le unità rimovibili
Modifica di una regola di criptaggio per le unità rimovibili
Abilitazione della modalità portatile per l'accesso ai file criptati nelle unità rimovibili
Decriptaggio delle unità rimovibili
Criptaggio dei dischi rigidi
Informazioni sul criptaggio dei dischi rigidi
Criptaggio dei dischi rigidi tramite la tecnologia Kaspersky Disk Encryption
Criptaggio dei dischi rigidi tramite la tecnologia BitLocker Drive Encryption
Creazione di un elenco di dischi rigidi esclusi dal criptaggio
Decriptaggio dei dischi rigidi
Gestione dell'agente di autenticazione
Utilizzo di un token o una smart card con l'agente di autenticazione
Modifica dei messaggi della Guida dell'agente di autenticazione
Supporto limitato per i caratteri nei messaggi della Guida dell'agente di autenticazione
Selezione del livello di traccia per l'agente di autenticazione
Gestione degli account per l'agente di autenticazione
Aggiunta di un comando per la creazione di un account per l'agente di autenticazione
Aggiunta di un comando di modifica dell'account per l'agente di autenticazione
Aggiunta di un comando per l'eliminazione di un account per l'agente di autenticazione
Ripristino delle credenziali dell'account per l'agente di autenticazione
Risposta a una richiesta utente per il ripristino delle credenziali dell'account per l'agente di autenticazione
Visualizzazione dei dettagli sul criptaggio dei dati
Informazioni sullo stato di criptaggio
Visualizzazione dello stato di criptaggio
Visualizzazione delle statistiche sul criptaggio nei riquadri dei dettagli di Kaspersky Security Center
Visualizzazione degli errori di criptaggio dei file nelle unità locali del computer
Visualizzazione del rapporto sul criptaggio dei dati
Gestione dei file criptati con funzionalità limitate di criptaggio dei file
Accesso ai file criptati senza una connessione a Kaspersky Security Center
Concessione dell'accesso utente ai file criptati senza una connessione a Kaspersky Security Center
Modifica dei modelli di messaggi per l'accesso ai file criptati
Utilizzo dei dispositivi criptati quando non è possibile accedervi
Ottenimento dell'accesso ai dispositivi criptati tramite l'interfaccia dell'applicazione
Concessione dell'accesso utente ai dispositivi criptati
Invio a un utente di una chiave di ripristino per i dischi rigidi criptati con BitLocker
Creazione del file eseguibile dell'utilità di ripristino
Ripristino dei dati nei dispositivi criptati utilizzando l'utilità di ripristino
Risposta a una richiesta utente per il ripristino dei dati nei dispositivi criptati
Ripristino dell'accesso ai dati criptati dopo un errore del sistema operativo
Creazione di un Rescue Disk del sistema operativo
Protezione della rete
Informazioni sulla protezione della rete
Configurazione delle impostazioni per il monitoraggio del traffico 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
Aggiornamento di database e moduli software dell'applicazione
Informazioni sugli aggiornamenti di database e moduli dell'applicazione

Informazioni sulle sorgenti degli aggiornamenti
Configurazione delle impostazioni di aggiornamento
Aggiunta di una sorgente degli aggiornamenti
Selezione della nazione del server degli aggiornamenti
Configurazione degli aggiornamenti da una cartella condivisa
Selezione della modalità di esecuzione dell'attività di aggiornamento
Avvio di un'attività di aggiornamento tramite i diritti di un account utente differente
Configurazione degli aggiornamenti dei moduli dell'applicazione
Avvio e arresto di un'attività di aggiornamento
Rollback dell'ultimo aggiornamento
Configurazione delle impostazioni del server proxy
Scansione del computer
Informazioni sulle attività di scansione
Avvio o arresto di un'attività di scansione
Configurazione delle impostazioni di un'attività di scansione
Modifica del livello di protezione
Modifica dell'azione da eseguire sui file infetti
Generazione di un elenco di oggetti da esaminare
Selezione del tipo di file da esaminare
Ottimizzazione della scansione dei file
Scansione dei file compositi
Utilizzo dei metodi di scansione
Utilizzo delle tecnologie di scansione
Selezione della modalità di esecuzione per l'attività di scansione
Avvio di un'attività di scansione tramite un account utente differente
Scansione delle unità rimovibili quando vengono connesse al computer
Gestione dei file non elaborati
Informazioni sui file non elaborati
Gestione dell'elenco dei file non elaborati
Avvio di un'attività Scansione Personalizzata per i file non elaborati
Eliminazione di file dall'elenco dei file non elaborati
Scansione Vulnerabilità
Visualizzazione delle informazioni sulle vulnerabilità delle applicazioni in esecuzione
Informazioni sull'attività Scansione Vulnerabilità
Avvio o arresto dell'attività Scansione Vulnerabilità
Configurazione delle impostazioni di Scansione Vulnerabilità
Creazione dell'ambito della scansione delle vulnerabilità
Selezione della modalità di esecuzione per l'attività Scansione Vulnerabilità
Avvio dell'attività Scansione Vulnerabilità tramite i diritti di un account utente differente
Gestione dell'elenco delle vulnerabilità
Informazioni sull'elenco delle vulnerabilità
Ripetizione dell'attività Scansione Vulnerabilità
Correzione di una vulnerabilità
Occultamento delle voci nell'elenco delle vulnerabilità
Filtro dell'elenco delle vulnerabilità in base al livello di gravità
Filtro dell'elenco delle vulnerabilità in base ai valori Corrette e Nascoste
Controllo dell'integrità dei moduli dell'applicazione
Informazioni sull'attività Controllo integrità

Avvio o arresto di un'attività Controllo integrità
Selezione della modalità di esecuzione per l'attività Controllo integrità
Gestione dei rapporti
Principi di gestione dei rapporti
Configurazione delle impostazioni dei rapporti
Configurazione del periodo massimo di archiviazione dei rapporti
Configurazione della dimensione massima dei file del rapporto
Visualizzazione dei rapporti
Visualizzazione di informazioni sugli eventi in un rapporto
Salvataggio di un rapporto in un file
Eliminazione dei rapporti
Servizio di notifica
Informazioni sulle notifiche di Kaspersky Endpoint Security
Configurazione del 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
Gestione di Quarantena e Backup
Informazioni su Quarantena e Backup
Configurazione delle impostazioni di Quarantena e Backup
Configurazione del periodo massimo di archiviazione per i file in Quarantena e le copie dei file in Backup
Configurazione della dimensione massima di Quarantena e Backup
Gestione della quarantena
Abilitazione e disabilitazione della scansione dei file in Quarantena dopo un aggiornamento
Avvio di un'attività Scansione Personalizzata per i file in quarantena
Ripristino di file dalla quarantena
Eliminazione di file dalla quarantena
Gestione di Backup
Ripristino di file da Backup
Eliminazione delle copie di backup dei file da Backup
Impostazioni avanzate dell'applicazione
Creazione e utilizzo di un file di configurazione
Area attendibile
Informazioni sull'area attendibile
Creazione di un'esclusione dalla scansione
Modifica di un'esclusione dalla scansione
Eliminazione di un'esclusione dalla scansione
Abilitazione e disabilitazione di un'esclusione dalla scansione
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
Auto-Difesa di Kaspersky Endpoint Security
Informazioni sulla funzionalità Auto-Difesa di Kaspersky Endpoint Security
Abilitazione o disabilitazione di Auto-Difesa
Abilitazione o disabilitazione di Difesa controllo remoto
Supporto delle applicazioni di amministrazione remota
Prestazioni di Kaspersky Endpoint Security e compatibilità con altre applicazioni
Informazioni sulle prestazioni di Kaspersky Endpoint Security e sulla compatibilità con altre applicazioni

Selezione dei tipi di oggetti rilevabili
Abilitazione o disabilitazione della tecnologia avanzata di disinfezione per le workstation
Abilitazione o disabilitazione della tecnologia avanzata di disinfezione per i file server
Abilitazione o disabilitazione della modalità di risparmio energetico
Abilitazione o disabilitazione della concessione di risorse ad altre applicazioni
Protezione tramite password
Informazioni sulla limitazione dell'accesso a Kaspersky Endpoint Security
Abilitazione e disabilitazione della protezione tramite password
Modifica della password di accesso a Kaspersky Endpoint Security
Informazioni sull'utilizzo di una password provvisoria
Creazione di una password provvisoria tramite Kaspersky Security Center Administration Console
Applicazione di una password provvisoria nell'interfaccia di Kaspersky Endpoint Security
Amministrazione remota dell'applicazione tramite Kaspersky Security Center
Informazioni sulla gestione dell'applicazione tramite Kaspersky Security Center
Considerazioni speciali in caso di utilizzo di versioni diverse dei plug-in di amministrazione
Avvio e arresto di Kaspersky Endpoint Security in un computer client
Configurazione delle impostazioni di Kaspersky Endpoint Security
Gestione delle attività
Informazioni sulle attività per Kaspersky Endpoint Security
Configurazione della modalità di gestione delle attività
Creazione di un'attività locale
Creazione di un'attività di gruppo
Creazione di un'attività per una selezione di dispositivi
Avvio, arresto, sospensione e ripresa di un'attività
Modifica delle impostazioni delle attività
Gestione dei criteri
Informazioni sui criteri
Creazione di un criterio
Modifica delle impostazioni dei criteri
Selezione delle impostazioni da visualizzare nel criterio di Kaspersky Security Center
Invio dei messaggi degli utenti al server di Kaspersky Security Center
Visualizzazione dei messaggi degli utenti nell'archivio di eventi di Kaspersky Security Center
Partecipazione a Kaspersky Security Network
Informazioni sulla partecipazione a Kaspersky Security Network
Abilitazione e disabilitazione dell'utilizzo di Kaspersky Security Network
Verifica della connessione a Kaspersky Security Network
Controllo della reputazione di un file in Kaspersky Security Network
Protezione avanzata con Kaspersky Security Network
Fonti di informazioni sull'applicazione
Come contattare l'assistenza tecnica
Come ottenere assistenza tecnica
Assistenza tecnica telefonica
Assistenza tecnica tramite Kaspersky CompanyAccount
Raccolta di informazioni per l'assistenza tecnica
Creazione di un file di traccia
Contenuto e archiviazione dei file di traccia
Abilitazione o disabilitazione della trasmissione a Kaspersky dei file di dump e di traccia
Invio di file al server dell'assistenza tecnica

Abilitazione e disabilitazione della protezione dei file di dump e di traccia
Glossario
Administration Server
Agente di Autenticazione
Aggiornamento
Ambito della scansione
Ambito di protezione
Analisi delle firme
Analisi euristica
Archivio
Attività
Autorità di emissione del certificato
Backup
Blacklist di indirizzi
Certificato
Certificato di licenza
Chiave attiva
Chiave di riserva
Connettore per Network Agent
Database anti-virus
Database di indirizzi Web dannosi
Database di indirizzi Web di phishing
Disinfezione
Exploit
Falso allarme
File infettabile
File infetto
File potenzialmente infetto
Forma normalizzata dell'indirizzo di una risorsa Web
Gruppo di amministrazione
Identificazione personale certificato
Impostazioni dell'applicazione
Impostazioni delle attività
Maschera file
Moduli dell'applicazione
Network Agent
Oggetto del certificato
Oggetto OLE
Patch
Phishing
Portable File Manager
Quarantena
Servizio di rete
Spostamento dei file in Quarantena
Trusted Platform Module
Informazioni sul codice di terze parti
Note relative ai marchi

# Informazioni su Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Questa sezione descrive le funzioni, i componenti e il kit di distribuzione di Kaspersky Endpoint Security e fornisce un elenco di requisiti hardware e software di Kaspersky Endpoint Security.

## Novità

Kaspersky Endpoint Security 10 Service Pack 2 for Windows include i seguenti miglioramenti e funzionalità:

1. Controllo avvio applicazioni:
   - Supporta i sistemi operativi server.
   - Controlla i download di moduli DLL e driver.
   - Gestisce l'elenco degli oggetti nell'attività di inventario (moduli DLL e file di script).
   - Controlla gli oggetti in base a un nuovo criterio: gli attributi dei certificati di firma digitale.
   - Genera un rapporto sugli avvii di prova delle applicazioni bloccate.
   - Supporta due modalità operative per Controllo avvio applicazioni: "Blacklist" e "Whitelist".
   - Utilizza l'hash SHA256 per il controllo e l'inventario degli oggetti.
   - Controlla l'esecuzione degli script dall'interprete PowerShell.
   - Usa l'archivio di certificati di sistema attendibili.
2. L'amministrazione di Microsoft BitLocker consente il criptaggio dei dischi rigidi con il supporto della tecnologia BitLocker di Microsoft:
   - Gestione remota del criptaggio.
   - Monitoraggio dei dispositivi criptati.
   - Creazione di rapporti sul criptaggio dei dispositivi.
   - Ripristino dell'accesso ai dispositivi criptati.
3. Kaspersky Disk Encryption:
   - Supporto per l'immissione delle credenziali nell'ambiente di preavvio dell'agente di autenticazione tramite una tastiera virtuale.
   - Supporto per la modalità di criptaggio solo dello spazio occupato in un dispositivo.
   - Supporto per il criptaggio nei tablet (Microsoft Surface versioni 3 e 4).
4. Controllo privilegi applicazioni:
   - Controlla l'accesso delle applicazioni ai dispositivi di registrazione audio e video.

5. Controllo Web:

   - Configura regole di accesso alle risorse Web per ulteriori categorie di risorse Web.

6. Controllo dispositivi:

   - Registra gli eventi associati all'eliminazione e al salvataggio di file nei dispositivi USB.
   - Genera un elenco di reti Wi-Fi attendibili in base alle seguenti impostazioni: nome, tipo di criptaggio e tipo di autenticazione.
   - Gestisce i diritti di accesso degli utenti per le operazioni di lettura e scrittura di file su dischi CD/DVD.

7. Anti-Virus Posta:

   - Supporta l'eliminazione e la ridenominazione di specifici tipi di file all'interno degli archivi per la scansione tramite Anti-Virus Posta.

8. Kaspersky Security Network:

   - Visualizza KSN come motivo per una decisione relativa al metodo di elaborazione dell'oggetto nei rapporti di Kaspersky Endpoint Security e di Kaspersky Security Center.
   - Invia una richiesta a KSN riguardo alla reputazione di un file selezionato.
   - Visualizza lo stato di disponibilità dei server KSN per i computer client in cui è installato Kaspersky Endpoint Security.

## Kit di distribuzione

Il kit di distribuzione di Kaspersky Endpoint Security contiene i seguenti file:

- I file necessari per l'installazione dell'applicazione con uno dei metodi disponibili:
- File di pacchetti di aggiornamento utilizzati durante l'installazione dell'applicazione.
- Il file klcfginst.msi per l'installazione del plug-in di amministrazione di Kaspersky Endpoint Security tramite Kaspersky Security Center.
- Il file ksn_<ID lingua>.txt, che contiene le condizioni di adesione a Kaspersky Security Network.
- Il file license.txt, che contiene il Contratto di licenza con l'utente finale.
- Il file incompatible.txt che contiene un elenco di software incompatibile.
- Il file installer.ini, che contiene le impostazioni interne del kit di distribuzione.

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

È necessario decomprimere il kit di distribuzione per accedere ai file.

# Organizzazione della protezione del computer

Kaspersky Endpoint Security assicura una protezione completa del computer da vari tipi di minacce, dagli attacchi di rete e di phishing.

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

Oltre alla protezione in tempo reale garantita dai componenti dell'applicazione, è consigliabile eseguire periodicamente una *scansione* alla ricerca di virus e altre minacce. In questo modo è possibile 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.

Per mantenere aggiornato Kaspersky Endpoint Security, è necessario *aggiornare* i database e i moduli utilizzati dall'applicazione. Per impostazione predefinita, l'impostazione viene aggiornata automaticamente, ma è possibile aggiornare manualmente i database e i moduli dell'applicazione, se necessario.

I seguenti componenti dell'applicazione sono componenti di controllo:

- **Controllo avvio applicazioni**. Questo componente tiene traccia dei tentativi dell'utente di avviare le applicazioni e gestisce l'avvio delle applicazioni.

- **Controllo privilegi applicazioni**. Questo componente registra le operazioni delle applicazioni nel sistema operativo e regola l'attività delle applicazioni in base al relativo gruppo di attendibilità. Per ciascun gruppo di applicazioni viene specificato un set di regole. Queste regole stabiliscono l'accesso delle applicazioni ai dati dell'utente e alle risorse del sistema operativo. Questi dati includono i file dell'utente (la cartella Documenti, i cookie, le informazioni sull'attività dell'utente) e file, cartelle e chiavi di registro che contengono impostazioni e informazioni importanti delle applicazioni utilizzate più di frequente.

- **Monitor vulnerabilità**. Il componente Monitor vulnerabilità esegue una scansione in tempo reale delle vulnerabilità nelle applicazioni avviate dall'utente o in esecuzione nel computer di quest'ultimo.

- **Controllo dispositivi**. Questo componente consente di impostare flessibili restrizioni per l'accesso a dispositivi di archiviazione dei dati (come unità disco rigido, unità rimovibili, unità nastro e CD/DVD), apparecchiature per la trasmissione dei dati (come i modem), apparecchiature per la conversione di informazioni in copie cartacee (come le stampanti) o interfacce per la connessione di dispositivi ai computer (come USB, Bluetooth e infrarossi).

- **Controllo Web**. Questo componente consente di impostare flessibili restrizioni per l'accesso alle risorse Web per diversi gruppi di utenti.

L'esecuzione dei componenti di controllo si basa sulle seguenti regole:

- Controllo avvio applicazioni utilizza le regole di Controllo avvio applicazioni.

- Controllo privilegi applicazioni utilizza le regole di Controllo applicazioni.

- Controllo dispositivi utilizza le regole di accesso ai dispositivi e le regole di accesso ai bus di connessione.

- Controllo Web utilizza le regole di accesso alle risorse Web.

I seguenti componenti dell'applicazione sono componenti della protezione:

- **Anti-Virus File**. Questo componente protegge il file system del computer dalle infezioni. Anti-Virus File viene avviato all'avvio di Kaspersky Endpoint Security, rimane attivo in modo permanente nella memoria del computer ed esamina tutti i file che vengono aperti, salvati o eseguiti nel computer e in tutte le unità connesse. Anti-Virus File intercetta ogni tentativo di accedere a un file e ne esegue la scansione allo scopo di individuare virus o altre minacce.

- **System Watcher**. Questo componente registra le attività delle applicazioni nel computer e fornisce queste informazioni agli altri componenti per assicurare una protezione più efficace del computer.

- **Anti-Virus Posta**. Questo componente esamina tutti i messaggi e-mail in entrata e in uscita allo scopo di individuare virus e altre minacce.

- **Anti-Virus Web**. Questo componente esamina il traffico ricevuto dal computer dell'utente tramite i protocolli HTTP e FTP, verificando se le URL sono elencate come indirizzi Web dannosi o di phishing.

- **Anti-Virus IM**. Questo componente esamina il traffico ricevuto dal computer tramite i protocolli dei client di messaggistica istantanea. Il componente consente di utilizzare in modo sicuro numerosi clienti di messaggistica.

- **Firewall**. Questo componente protegge i dati memorizzati nel computer e blocca la maggior parte delle possibili minacce per il sistema operativo mentre il computer è connesso a Internet o alla rete LAN. Il componente filtra tutta l'attività di rete secondo regole di due tipi: regole di rete per le applicazioni e regole per i pacchetti di rete.

- **Monitor di Rete**. Questo componente consente di visualizzare l'attività di rete del computer in tempo reale.

- **Prevenzione attacchi di rete**. Questo componente esamina il traffico di rete in entrata alla ricerca di attività tipiche degli attacchi di rete. Quando viene rilevato un tentativo di attacco di rete contro il computer in uso, Kaspersky Endpoint Security blocca l'attività di rete dal computer che ha originato l'attacco.

Le seguenti attività sono incluse in Kaspersky Endpoint Security:

- **Scansione Completa**. Kaspersky Endpoint Security esegue una scansione del sistema operativo, inclusi RAM, oggetti caricati all'avvio, archivio di backup del sistema operativo e tutte le unità disco rigido e le unità rimovibili.

- **Scansione Personalizzata**. Kaspersky Endpoint Security esegue la scansione degli oggetti selezionati dall'utente.

- **Scansione delle aree critiche**. Kaspersky Endpoint Security esegue la scansione degli oggetti caricati all'avvio del sistema operativo, della RAM e degli oggetti che possono essere colpiti da rootkit.

- **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.

- **Scansione Vulnerabilità**. Kaspersky Endpoint Security esamina il sistema operativo e il software installato allo scopo di individuarne le vulnerabilità. Questa scansione garantisce il rilevamento tempestivo e la rimozione dei potenziali problemi che potrebbero essere sfruttati da utenti malintenzionati.

La funzionalità di criptaggio dei file consente di criptare file e cartelle archiviati nelle unità locali del computer. La funzionalità di criptaggio delle unità consente di criptare dischi rigidi e unità rimovibili.

## Amministrazione remota tramite Kaspersky Security Center

Kaspersky Security Center consente di avviare e interrompere in remoto Kaspersky Endpoint Security in un computer client e di gestire e configurare in remoto le impostazioni dell'applicazione.

## Funzioni di servizio dell'applicazione

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

- **Rapporti**. Durante l'esecuzione, l'applicazione mantiene un rapporto su ogni componente e attività dell'applicazione. Il rapporto contiene un elenco degli eventi di Kaspersky Endpoint Security e di 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.

- **Archiviazione dei dati**. Se vengono rilevati file infetti o potenzialmente infetti durante la scansione del computer alla ricerca di virus e altre minacce, l'applicazione blocca tali file. I file potenzialmente infetti vengono spostati in una speciale area di archiviazione denominata *Quarantena*. Le copie dei file disinfettati o eliminati vengono archiviate in *Backup*. I file che non vengono elaborati per qualsiasi motivo vengono spostati nell'*elenco dei file non elaborati*. È possibile esaminare i file, ripristinare i file nelle cartelle originali e svuotare l'archiviazione dei dati.

- **Servizio di notifica**. Il servizio di notifica mantiene l'utente informato sullo stato di protezione corrente del computer e sul funzionamento 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 la raccolta in tempo reale di informazioni sulla reputazione di file, risorse Web e software 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 telefonicamente o 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 del servizio di Assistenza tecnica per richiedere assistenza. È possibile inviare una richiesta tramite la Pagina personale nel sito Web dell'Assistenza tecnica.

Se l'applicazione restituisce un errore 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.

L'applicazione riceve informazioni sugli errori e sui blocchi del sistema ricorrenti utilizzando appositi algoritmi definiti dagli esperti di Kaspersky.

## 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

- Processore con una velocità di clock di 1 GHz (che supporti il set di istruzioni SSE2)

- RAM:
  - 1 GB per un sistema operativo a 32 bit;
  - 2 GB per un sistema operativo a 64 bit;

Sistemi operativi supportati per PC:

- 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/Education/Enterprise.

Per informazioni dettagliate sul supporto per il sistema operativo Microsoft Windows 10, fare riferimento alla Knowledge Base dell'Assistenza tecnica.

Sistemi operativi supportati per i file server:

- Windows Small Business Server 2008 Standard/Premium (64 bit);
- Windows Small Business Server 2011 Essentials/Standard (64 bit);
- Windows MultiPoint Server 2011 (64 bit);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 o versioni successive;
- 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.

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.

# Installazione e rimozione dell'applicazione

Questa sezione contiene informazioni sull'installazione di Kaspersky Endpoint Security nel computer, l'esecuzione della configurazione iniziale, l'aggiornamento di una versione precedente dell'applicazione e la rimozione dell'applicazione dal computer.

# Installazione dell'applicazione

In questa sezione viene descritto come installare Kaspersky Endpoint Security nel computer ed eseguire la configurazione iniziale dell'applicazione.

# Informazioni sulle modalità di installazione dell'applicazione

Kaspersky Endpoint Security 10 for Windows può essere installato in locale (direttamente nel computer dell'utente) o in remoto dalla workstation dell'amministratore.

L'installazione locale di Kaspersky Endpoint Security 10 for Windows può essere eseguita in una delle modalità seguenti:

- In modalità interattiva, utilizzando l'Installazione guidata dell'applicazione.

  La modalità interattiva richiede l'input dell'utente durante l'installazione.

- In modalità invisibile all'utente, dalla riga di comando.

  Una volta avviata l'installazione in modalità invisibile all'utente, l'intervento dell'utente nel processo di installazione non è necessario.

L'applicazione può essere installata in remoto nei computer della rete tramite:

- Il software Kaspersky Security Center (vedere la *Guida all'implementazione di Kaspersky Security Center*).
- L'Editor Criteri di gruppo di Microsoft Windows (vedere i file della Guida del sistema operativo).
- System Center Configuration Manager.

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

# Installazione dell'applicazione tramite l'Installazione guidata

L'interfaccia dell'Installazione guidata dell'applicazione è composta da una sequenza di finestre corrispondenti ai passaggi di installazione dell'applicazione. È possibile spostarsi tra le pagine dell'Installazione guidata utilizzando i pulsanti **Indietro** e **Avanti**. Per chiudere l'Installazione guidata al termine dell'attività, fare clic sul pulsante **Termina**. Per interrompere l'Installazione guidata in qualsiasi momento, fare clic sul pulsante **Annulla**.

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

1. Eseguire il file setup.exe incluso nel kit di distribuzione.

   Verrà avviata l'Installazione guidata.

2. Attenersi alle istruzioni dell'Installazione guidata.

Quando il file setup.exe viene avviato, Kaspersky Endpoint Security verifica che nel computer non sia presente software incompatibile. Per impostazione predefinita, se viene rilevato software incompatibile il processo di installazione viene interrotto e viene visualizzato l'elenco delle applicazioni incompatibili con Kaspersky Endpoint Security. Per continuare l'installazione, rimuovere queste applicazioni dal computer.

## Passaggio 1. Verifica dei requisiti di installazione

Prima di installare Kaspersky Endpoint Security 10 for Windows in un computer o di aggiornare una versione precedente dell'applicazione, vengono verificate le seguenti condizioni:

- Se il sistema operativo e il Service Pack soddisfano o meno i requisiti software per l'installazione del prodotto.
- 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 10 Service Pack 2 for Windows e la versione precedente dell'applicazione viene rimossa automaticamente. Questo si applica alle seguenti versioni dell'applicazione:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows

## Passaggio 2. Pagina iniziale della procedura di installazione

Se tutti i requisiti per l'installazione dell'applicazione sono soddisfatti, viene visualizzata una pagina di benvenuto dopo l'avvio del pacchetto di installazione. La pagina iniziale segnala l'avvio dell'installazione di Kaspersky Endpoint Security nel computer.

Per procedere con l'Installazione guidata, fare clic sul pulsante **Avanti**.

## Passaggio 3. Visualizzazione del Contratto di licenza

Durante questo passaggio viene richiesto di visualizzare il contratto di licenza che intercorre tra l'utente e Kaspersky.

Leggere attentamente il contratto di licenza e, se si accettano tutte le condizioni, selezionare la casella di controllo **Accetto i termini del Contratto di Licenza**.

Per tornare al passaggio precedente dell'Installazione guidata, fare clic sul pulsante **Indietro**. Per procedere con l'Installazione guidata, fare clic sul pulsante **Avanti**. Per interrompere l'Installazione guidata, fare clic sul pulsante **Annulla**.

## Passaggio 4. Selezione del tipo di installazione

Durante questo passaggio è possibile selezionare il tipo di installazione di Kaspersky Endpoint Security più adatto per le proprie esigenze:

- **Installazione di base**. Se si seleziona questo tipo di installazione, vengono installati nel computer i componenti della protezione Controllo privilegi applicazioni e Monitor vulnerabilità con le impostazioni consigliate dagli specialisti di Kaspersky.
- **Installazione standard**. Se si seleziona questo tipo di installazione, vengono installati nel computer i componenti della protezione e di controllo con le impostazioni consigliate da Kaspersky.
- **Installazione personalizzata**. Se si seleziona questo tipo di installazione, viene richiesto di selezionare i componenti da installare e di specificare la cartella di destinazione per l'applicazione.

  Questo tipo di installazione consente di installare i componenti che non sono inclusi nelle installazioni di base e standard.

Per impostazione predefinita, è selezionata l'installazione standard.

Per tornare al passaggio precedente dell'Installazione guidata, fare clic sul pulsante **Indietro**. Per procedere con l'Installazione guidata, fare clic sul pulsante **Avanti**. Per interrompere l'Installazione guidata, fare clic sul pulsante **Annulla**.

## Passaggio 5. Selezione dei componenti dell'applicazione da installare

Questo passaggio viene eseguito se si seleziona l'*installazione personalizzata* dell'applicazione.

Durante questo passaggio, è possibile selezionare i componenti di Kaspersky Endpoint Security da installare. Anti-Virus File è un componente obbligatorio per l'installazione. Non è possibile annullarne l'installazione.

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

- Prevenzione unità USB dannose.
- Criptaggio unità.

- Criptaggio dei file.
- Microsoft BitLocker Manager.
- KATA Endpoint Sensor.

*Microsoft BitLocker Manager* esegue le seguenti funzioni:

- Gestisce le funzionalità di criptaggio di BitLocker incorporate nel sistema operativo Windows.
- Configura le impostazioni del criterio di criptaggio e ne verifica l'applicabilità per il computer gestito.
- Avvia i processi di criptaggio e decriptaggio.
- Monitora lo stato del criptaggio nel computer gestito.
- Archivia in modo centralizzato le chiavi di ripristino in Kaspersky Security Center Administration Server.

*KATA Endpoint Sensor* è un componente di Kaspersky Anti Targeted Attack Platform. Questa soluzione è progettata per il rilevamento rapido di minacce come gli attacchi mirati. Il componente monitora continuamente i processi, le connessioni di rete attive e i file modificati, quindi passa queste informazioni a Kaspersky Anti Targeted Attack Platform.

Per selezionare un componente da installare, fare clic sull'icona accanto al nome del componente per visualizzare il menu di scelta rapida, quindi selezionare **La funzionalità verrà installata sul disco rigido locale**. Per ulteriori dettagli sulle attività eseguite dal componente selezionato e sullo spazio su disco necessario per installare il componente, fare riferimento alla parte inferiore della pagina corrente dell'Installazione guidata.

Per visualizzare informazioni dettagliate sullo spazio disponibile nelle unità disco locali, fare clic sul pulsante **Volume**. Le informazioni saranno mostrate nella finestra **Spazio su disco disponibile** visualizzata.

Per annullare l'installazione del componente, selezionare l'opzione **La funzionalità non sarà disponibile** nel menu di scelta rapida.

Per tornare all'elenco dei componenti installati per impostazione predefinita, fare clic sul pulsante **Reimposta**.

Per tornare al passaggio precedente dell'Installazione guidata, fare clic sul pulsante **Indietro**. Per procedere con l'Installazione guidata, fare clic sul pulsante **Avanti**. Per interrompere l'Installazione guidata, fare clic sul pulsante **Annulla**.

## Passaggio 6. Selezione della cartella di destinazione

Questo passaggio è disponibile se si seleziona l'*installazione personalizzata* dell'applicazione.

In questa fase è possibile specificare il percorso della cartella di destinazione in cui installare l'applicazione. Per selezionare la cartella di destinazione per l'applicazione, fare clic sul pulsante **Sfoglia**.

Per visualizzare informazioni sullo spazio disponibile nelle unità disco locali, fare clic sul pulsante **Volume**. Le informazioni sono mostrate nella finestra **Requisiti di spazio su disco** visualizzata.

Per tornare al passaggio precedente dell'Installazione guidata, fare clic sul pulsante **Indietro**. Per procedere con l'Installazione guidata, fare clic sul pulsante **Avanti**. Per interrompere l'Installazione guidata, fare clic sul pulsante **Annulla**.

## Passaggio 7. Aggiunta di esclusioni dalla scansione virus

Questo passaggio è disponibile se si seleziona l'*installazione personalizzata* dell'applicazione.

In questa fase è possibile specificare le esclusioni dalla scansione virus da aggiungere alle impostazioni dell'applicazione.

Le caselle di controllo **Escludi dall'ambito della scansione virus le aree raccomandate da Microsoft** / **Escludi dall'ambito della scansione virus le aree raccomandate da Kaspersky** consentono rispettivamente di escludere dall'area attendibile le aree raccomandate da Microsoft o da Kaspersky.

Se una di queste caselle di controllo è selezionata, Kaspersky Endpoint Security include, rispettivamente, le aree raccomandate da Microsoft o Kaspersky nell'area attendibile. Kaspersky Endpoint Security non esegue la scansione di queste aree alla ricerca di virus e di altre minacce.

La casella di controllo **Escludi dall'ambito della scansione virus le aree raccomandate da Microsoft** è disponibile quando Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

Per tornare al passaggio precedente dell'Installazione guidata, fare clic sul pulsante **Indietro**. Per procedere con l'Installazione guidata, fare clic sul pulsante **Avanti**. Per interrompere l'Installazione guidata, fare clic sul pulsante **Annulla**.

## Passaggio 8. Preparazione per l'installazione dell'applicazione

È consigliabile proteggere il processo di installazione perché il computer potrebbe essere infettato da programmi dannosi che possono interferire con l'installazione di Kaspersky Endpoint Security 10 for Windows.

La protezione del processo di installazione è abilitata per impostazione predefinita.

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. In questo caso, interrompere l'installazione e avviare di nuovo l'Installazione guidata dell'applicazione. Durante il passaggio "Preparazione per l'installazione dell'applicazione", deselezionare la casella di controllo **Proteggi il processo di installazione**.

La casella di controllo **Garantisci la compatibilità con i servizi di provisioning Citrix** consente di abilitare o disabilitare la funzione per l'installazione dei driver in modalità di compatibilità Citrix PVS.

Selezionare questa casella di controllo solo se si utilizzano i servizi di provisioning Citrix.

La casella di controllo **Aggiungere il percorso del file avp.com alla variabile di sistema %PATH%** consente di abilitare o disabilitare un'opzione che aggiunge il percorso del file avp.com alla variabile di sistema %PATH%.

Se la casella di controllo è selezionata, l'avvio di Kaspersky Endpoint Security o di una delle relative attività dalla riga di comando non richiede l'immissione del percorso del file eseguibile. È sufficiente immettere il nome del file eseguibile e il comando per avviare una particolare attività.

Per tornare al passaggio precedente dell'Installazione guidata, fare clic sul pulsante **Indietro**. Per installare il programma, fare clic sul pulsante **Installa**. Per interrompere l'Installazione guidata, fare clic sul pulsante **Annulla**.

Durante l'installazione dell'applicazione nel computer è possibile che le connessioni di rete correnti vengano terminate. La maggior parte delle connessioni terminate viene ripristinata dopo il completamento dell'installazione dell'applicazione.

## Passaggio 9. Installazione dell'applicazione

L'installazione dell'applicazione può richiedere alcuni minuti. Attenderne il completamento.

Se si sta eseguendo l'aggiornamento di una versione precedente dell'applicazione, questo passaggio include anche la migrazione delle impostazioni e la rimozione della versione precedente dell'applicazione.

Al termine dell'installazione di Kaspersky Endpoint Security, viene avviata la Configurazione iniziale guidata.

## Installazione dell'applicazione dalla riga di comando

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 invisibile all'utente, l'intervento dell'utente nel processo di installazione non è necessario. Per installare l'applicazione in modalità automatica, utilizzare le chiavi `/s` e `/qn`.

*Per installare l'applicazione o eseguire l'upgrade della versione 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|0] [/pADDLOCAL=<componente>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/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|0] [ADDLOCAL=<componente>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<nome utente> KLPASSWD=<password> KLPASSWDAREA=<ambito della password>] [ENABLETRACES=1|0 TRACESLEVEL=<livello di traccia>] /qn
   ```

| | |
|---|---|
| `EULA` | Accettazione o rifiuto delle condizioni del Contratto di licenza con l'utente finale. Valori disponibili:<br>• `1` – accettazione delle condizioni del Contratto di licenza con l'utente finale.<br>• `0` – rifiuto delle condizioni del Contratto di licenza con l'utente finale. |

| | |
|---|---|
| | Il testo del Contratto di licenza è incluso nel kit di distribuzione di Kaspersky Endpoint Security. L'accettazione delle condizioni del Contratto di licenza con l'utente finale è necessaria per installare l'applicazione o eseguire l'aggiornamento della versione. |
| `PRIVACYPOLICY` | Accettazione o rifiuto dell'Informativa sulla privacy. Valori disponibili:<br>• `1` – accettazione dell'Informativa sulla privacy.<br>• `0` – rifiuto dell'Informativa sulla privacy.<br>Il testo dell'Informativa sulla privacy è incluso nel kit di distribuzione di Kaspersky Endpoint Security. Per installare l'applicazione o eseguire l'upgrade della versione dell'applicazione, è necessario accettare la Gestione dei dati personali. |
| `KSN` | 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:<br>• `1` – accettazione della partecipazione a KSN.<br>• `0` – rifiuto della partecipazione a KSN (valore predefinito).<br>Il pacchetto di distribuzione di Kaspersky Endpoint Security è ottimizzato per l'utilizzo con Kaspersky Security Network. Se si è scelto di non per partecipare a Kaspersky Security Network, è necessario aggiornare Kaspersky Endpoint Security subito dopo il completamento dell'installazione. |
| `ALLOWREBOOT=1` | Riavvio automatico del computer, se necessario dopo l'installazione o l'upgrade dell'applicazione. Se non viene impostato alcun valore per questo parametro, il riavvio automatico del computer viene bloccato.<br>Non è richiesto un riavvio durante l'installazione di Kaspersky Endpoint Security. È richiesto un riavvio solo se è necessario rimuovere applicazioni incompatibili prima dell'installazione. Potrebbe essere necessario un riavvio anche durante l'aggiornamento della versione dell'applicazione. |
| `ADDLOCAL` | Selezionare i componenti aggiuntivi per l'installazione. Per impostazione predefinita, tutti i componenti dell'applicazione sono selezionati per l'installazione eccetto i seguenti componenti: Prevenzione Attacchi BadUSB, Criptaggio a livello di file, Criptaggio dell'intero disco, Gestione BitLocker e KATA Endpoint Sensor. Valori disponibili:<br>• `MSBitLockerFeature`. Viene installato il componente BitLocker Manager.<br>• `AntiAPTFeature`. Viene installato il componente KATA Endpoint Sensor. |
| `SKIPPRODUCTCHECK=1` | 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. |
| `SKIPPRODUCTUNINSTALL=1` | 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. |
| KLLOGIN | Impostare il nome utente per l'accesso alle funzionalità e alle impostazioni di Kaspersky Endpoint Security (componente Protezione tramite password). Il nome utente viene impostato insieme ai parametri KLPASSWD e KLPASSWDAREA. Il nome utente predefinito è KLAdmin. |
| KLPASSWD | Specificare una password per accedere a funzionalità e impostazioni di Kaspersky Endpoint Security (la password è specificata insieme ai parametri KLLOGIN e KLPASSWDAREA).<br>Se è stata specificata una password, ma non è stato specificato un nome utente con il parametro KLLOGIN, per impostazione predefinita viene utilizzato il nome utente KLAdmin. |
| KLPASSWDAREA | Specificare l'ambito della password per accedere a Kaspersky Endpoint Security. Quando un utente tenta di eseguire un'azione inclusa in questo ambito, Kaspersky Endpoint Security richiede le credenziali dell'account utente (parametri KLLOGIN e KLPASSWD). Utilizzare il carattere ";" per specificare più valori. Valori disponibili:<br>• SET – modifica delle impostazioni dell'applicazione.<br>• EXIT – uscita dall'applicazione.<br>• DISPROTECT – disabilitazione dei componenti della protezione e arresto delle attività di scansione.<br>• DISPOLICY – disabilitazione del criterio di Kaspersky Security Center.<br>• UNINST – rimozione dell'applicazione dal computer.<br>• DISCTRL – disabilitazione dei componenti di controllo.<br>• REMOVELIC – rimozione della chiave.<br>• REPORTS – visualizzazione dei rapporti. |
| ENABLETRACES | Abilitazione o disabilitazione delle tracce dell'applicazione. Dopo l'avvio, Kaspersky Endpoint Security salva i file di traccia nella cartella %ProgramData%/Kaspersky Lab. Valori disponibili:<br>• 1 – le tracce sono abilitate.<br>• 0 – le tracce sono disabilitate (valore predefinito). |
| TRACESLEVEL | Livello di dettaglio delle tracce. Valori disponibili:<br>• 100 (critico). Solo i messaggi di errore critici.<br>• 200 (alto). Messaggi su tutti gli errori, inclusi gli errori irreversibili.<br>• 300 (diagnostico). Messaggi su tutti gli errori e una selezione di messaggi contenenti avvisi.<br>• 400 (importante). Tutti gli avvisi e i messaggi di errore normali e critici, oltre ad alcuni messaggi con informazioni aggiuntive. |

- `500` (normale). Tutti gli avvisi e i messaggi sugli errori normali e critici, nonché i messaggi con informazioni dettagliate sul funzionamento standard dell'applicazione (valore predefinito).
- `600` (basso). Tutti i messaggi possibili.

Esempio:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Dopo l'installazione dell'applicazione, Kaspersky Endpoint Security attiva la licenza di prova a meno che non sia stato indicato 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 una licenza commerciale.

Durante l'installazione dell'applicazione o l'upgrade della versione dell'applicazione in modalità invisibile all'utente, è supportato l'utilizzo dei seguenti file:

- setup.ini – impostazioni di configurazione generali dell'applicazione;
- install.cfg – impostazioni locali 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.

## 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, nella sezione **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 kit di distribuzione di Kaspersky Endpoint Security.

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

   c. Nella sezione **Applicazione 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 di amministratore**.

   d. Nella sezione **Requisiti**:

   - Selezionare la casella di controllo **Esegui 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 client specificate** nella sezione **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 quando si installa l'applicazione dalla riga di comando o 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.

Il file setup.ini è composto dalle seguenti sezioni:

- `[Setup]` - opzioni generali di 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. Anti-Virus File è un componente obbligatorio ed è installato nel computer indipendentemente dalle impostazioni indicate in questa sezione.
- `[Tasks]` – selezione di attività da includere nell'elenco delle attività di Kaspersky Endpoint Security. Se non viene specificata alcuna attività, vengono incluse tutte le attività nell'elenco di attività di Kaspersky Endpoint Security.

In alternativa al valore `1`, è possibile utilizzare i valori `yes`, `on`, `enable` 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` | Accettazione o rifiuto delle condizioni del Contratto di licenza con l'utente finale. Valori disponibili:<br>• `1` – accettazione delle condizioni del Contratto di licenza con l'utente finale. |

| | | |
|---|---|---|
| | | • `0` – rifiuto delle condizioni del Contratto di licenza con l'utente finale.<br>Il testo del Contratto di licenza è incluso nel kit di distribuzione di Kaspersky Endpoint Security.<br>L'accettazione delle condizioni del Contratto di licenza con l'utente finale è necessaria per installare l'applicazione o eseguire l'aggiornamento della versione. |
| | `PrivacyPolicy` | Accettazione o rifiuto dell'Informativa sulla privacy. Valori disponibili:<br>• `1` – accettazione dell'Informativa sulla privacy.<br>• `0` – rifiuto dell'Informativa sulla privacy.<br>Il testo dell'Informativa sulla privacy è incluso nel kit di distribuzione di Kaspersky Endpoint Security. Per installare l'applicazione o eseguire l'upgrade della versione dell'applicazione, è necessario accettare la Gestione dei dati personali. |
| | `KSN` | 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:<br>• `1` – accettazione della partecipazione a KSN.<br>• `0` – rifiuto della partecipazione a KSN (valore predefinito).<br>Il pacchetto di distribuzione di Kaspersky Endpoint Security è ottimizzato per l'utilizzo con Kaspersky Security Network. Se si è scelto di non per partecipare a Kaspersky Security Network, è necessario aggiornare Kaspersky Endpoint Security subito dopo il completamento dell'installazione. |
| | `Login` | Impostare il nome utente per l'accesso alle funzionalità e alle impostazioni di Kaspersky Endpoint Security (componente Protezione tramite password). Il nome utente viene impostato insieme alle impostazioni `Password` e `PasswordArea`. Il nome utente predefinito è KLAdmin. |
| | `Password` | Specificare una password per accedere a funzionalità e impostazioni di Kaspersky Endpoint Security (la password è specificata insieme ai parametri `Login` e `PasswordArea`).<br>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. |
| | | |

| | | |
|---|---|---|
| | `PasswordArea` | Specificare l'ambito della password per accedere a Kaspersky Endpoint Security. Quando un utente tenta di eseguire un'azione inclusa in questo ambito, Kaspersky Endpoint Security richiede le credenziali dell'account utente (parametri `Login` e `Password`). Utilizzare il carattere "`;`"per specificare più valori. Valori disponibili:<br>• `SET` – modifica delle impostazioni dell'applicazione.<br>• `EXIT` – uscita dall'applicazione.<br>• `DISPROTECT` – disabilitazione dei componenti della protezione e arresto delle attività di scansione.<br>• `DISPOLICY` – disabilitazione del criterio di Kaspersky Security Center.<br>• `UNINST` – rimozione dell'applicazione dal computer.<br>• `DISCTRL` – disabilitazione dei componenti di controllo.<br>• `REMOVELIC` – rimozione della chiave.<br>• `REPORTS` – visualizzazione dei rapporti. |
| | `SelfProtection` | Abilitazione o disabilitazione del meccanismo di protezione dell'installazione dell'applicazione. Valori disponibili:<br>• `1` – il meccanismo di protezione dell'installazione dell'applicazione è abilitato.<br>• `0` – il meccanismo di protezione dell'installazione dell'applicazione è disabilitato.<br>È possibile abilitare la protezione dell'installazione. La protezione dell'installazione include la protezione dallo spoofing del pacchetto di distribuzione con malware, il blocco dell'accesso alla cartella di installazione di Kaspersky Endpoint Security e il blocco dell'accesso all'hive 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. |
| | `Reboot=1` | Riavvio automatico del computer, se necessario dopo l'installazione o l'upgrade dell'applicazione. Se non viene impostato alcun valore per questo parametro, il riavvio automatico del computer viene bloccato. |

| | | |
|---|---|---|
| | | Non è richiesto un riavvio durante l'installazione di Kaspersky Endpoint Security. È richiesto un riavvio solo se è necessario rimuovere applicazioni incompatibili prima dell'installazione. Potrebbe essere necessario un riavvio anche durante l'aggiornamento della versione dell'applicazione. |
| | `AddEnvironment` | Consente di aggiungere alla variabile di sistema %PATH% il percorso dei file eseguibili contenuti nella cartella di installazione di Kaspersky Endpoint Security. Valori disponibili:<br>• `1` – alla variabile di sistema %PATH% viene aggiunto il percorso dei file eseguibili contenuti nella cartella di installazione di Kaspersky Endpoint Security.<br>• `0` – alla variabile di sistema %PATH% non viene aggiunto il percorso dei file eseguibili contenuti nella cartella di installazione di Kaspersky Endpoint Security. |
| | `AMPPL` | Consente di abilitare o disabilitare la protezione del servizio Kaspersky Endpoint Security tramite la tecnologia AM-PPL (Antimalware Protected Process Light). Valori disponibili:<br>• `1` – la protezione del servizio Kaspersky Endpoint Security tramite la tecnologia AM-PPL è abilitata.<br>• `0` – la protezione del servizio Kaspersky Endpoint Security tramite la tecnologia AM-PPL è disabilitata. |
| | `SetupReg` | Consente la scrittura delle chiavi del Registro di sistema del file setup.reg nel Registro di sistema. Valore del parametro `SetupReg: setup.reg`. |
| | `EnableTraces` | Abilitazione o disabilitazione delle tracce di installazione dell'applicazione. Kaspersky Endpoint Security salva i file di traccia nella cartella %ProgramData%/Kaspersky Lab. Valori disponibili:<br>• `1` – le tracce di installazione dell'applicazione sono abilitate.<br>• `0` – le tracce di installazione dell'applicazione sono disabilitate (valore predefinito). |
| | `TracesLevel` | Livello di dettaglio delle tracce. Valori disponibili:<br>• `100` (critico). Solo i messaggi di errore critici.<br>• `200` (alto). Messaggi su tutti gli errori, inclusi gli errori irreversibili.<br>• `300` (diagnostico). Messaggi su tutti gli errori e una selezione di messaggi contenenti avvisi. |

| | | |
|---|---|---|
| | | • `400` (importante). Tutti gli avvisi e i messaggi di errore normali e critici, oltre ad alcuni messaggi con informazioni aggiuntive.<br>• `500` (normale). Tutti gli avvisi e i messaggi sugli errori normali e critici, nonché i messaggi con informazioni dettagliate sul funzionamento standard dell'applicazione (valore predefinito).<br>• `600` (basso). Tutti i messaggi possibili. |
| `[Components]` | `ALL` | Installare tutti i componenti. Se è specificato il valore del parametro `1`, saranno installati tutti i componenti indipendentemente dalle impostazioni di installazione dei singoli componenti. |
| | `MailAntiVirus` | Anti-Virus Posta. |
| | `IMAntiVirus` | Anti-Virus IM. |
| | `WebAntiVirus` | Anti-Virus Web. |
| | `ApplicationPrivilegeControl` | Controllo privilegi applicazioni. |
| | `SystemWatcher` | System Watcher. |
| | `Firewall` | Firewall. |
| | `NetworkAttackBlocker` | Prevenzione attacchi di rete. |
| | `WebControl` | Controllo Web. |
| | `DeviceControl` | Controllo dispositivi. |
| | `ApplicationStartupControl` | Controllo avvio applicazioni. |
| | `FileEncryption` | Librerie di Criptaggio a livello di file. |
| | `DiskEncryption` | Librerie di Criptaggio dell'intero disco. |
| | `VulnerabilityAssessment` | Monitor vulnerabilità. |
| | `KeyboardAuthorization` | Prevenzione unità USB dannose. |
| | `AntiAPT` | KATA Endpoint Sensor. |
| | `MSBitLocker` | Microsoft BitLocker Manager. |
| | `AdminKitConnector` | Connettore per Network Agent per l'amministrazione remota dell'applicazione tramite Kaspersky Security Center. Valori disponibili:<br>• `1` – Connettore per Network Agent viene installato.<br>• `0` – Connettore per Network Agent non viene installato. |
| `[Tasks]` | `ScanMyComputer` | Attività Scansione completa. Valori disponibili:<br>• `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:<br>• `1` – l'attività viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security.<br>• `0` – l'attività non viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security. |
| | `Updater` | Attività di aggiornamento. Valori disponibili:<br>• `1` – l'attività viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security.<br>• `0` – l'attività non viene inclusa nell'elenco delle attività di Kaspersky Endpoint Security. |

## Configurazione iniziale guidata

La Configurazione iniziale guidata di Kaspersky Endpoint Security viene avviata al termine della procedura di installazione dell'applicazione. La Configurazione iniziale guidata consente di attivare l'applicazione e di raccogliere informazioni sulle applicazioni incluse nel sistema operativo. Queste applicazioni vengono aggiunte all'elenco delle applicazioni attendibili, le cui azioni nel sistema operativo non sono soggette ad alcuna restrizione.

L'interfaccia della Configurazione iniziale guidata è costituita da una sequenza di pagine (passaggi). È possibile spostarsi tra le pagine della Configurazione iniziale guidata utilizzando i pulsanti **Indietro** e **Avanti**. Per completare la Configurazione iniziale guidata, fare clic sul pulsante **Termina**. Per interrompere la Configurazione iniziale guidata in qualsiasi momento, fare clic su **Annulla**.

Se la Configurazione iniziale guidata viene interrotta, le impostazioni già specificate non vengono salvate. Al successivo tentativo di utilizzare l'applicazione, verrà nuovamente avviata la Configurazione iniziale guidata e sarà necessario riconfigurare completamente le impostazioni.

## Attivazione dell'applicazione

L'applicazione deve essere attivata in un computer con la data e l'ora di sistema correnti. Se la data e l'ora di sistema vengono modificate dopo l'attivazione dell'applicazione, la chiave diventa inutilizzabile. L'applicazione passa a una modalità di esecuzione senza aggiornamenti e Kaspersky Security Network non è disponibile. La chiave può essere nuovamente utilizzabile solo reinstallando il sistema operativo.

Durante questo passaggio, selezionare una delle seguenti opzioni di attivazione di Kaspersky Endpoint Security:

- **Attiva con un codice di attivazione**. Per attivare l'applicazione con un codice di attivazione, selezionare questa opzione e immettere un codice di attivazione.
- **Attiva con un file chiave**. Selezionare questa opzione per attivare l'applicazione con un file chiave.

- **Attiva la versione di prova**. Per attivare la versione di prova dell'applicazione, selezionare questa opzione. Sarà possibile utilizzare tutte le funzionalità dell'applicazione per il periodo definito dalla licenza per la versione di prova dell'applicazione. Allo scadere della licenza, le funzionalità dell'applicazione vengono bloccate e non è possibile attivare nuovamente la versione di prova.

- **Attiva successivamente**. Selezionare questa opzione per saltare la fase di attivazione di Kaspersky Endpoint Security. Sarà possibile utilizzare solo i componenti Anti-Virus File e Firewall. Sarà possibile aggiornare i database anti-virus e i moduli di Kaspersky Endpoint Security solo una volta dopo l'installazione. L'opzione **Attiva successivamente** è disponibile solo al primo avvio della Configurazione iniziale guidata, subito dopo l'installazione dell'applicazione.

È necessaria una connessione a Internet per attivare la versione di prova dell'applicazione o per attivare l'applicazione con un codice di attivazione.

Per continuare con la Configurazione iniziale guidata, selezionare un'opzione di attivazione, quindi fare clic sul pulsante **Avanti**. Per interrompere la Configurazione iniziale guidata, fare clic sul pulsante **Annulla**.

## Attivazione con un codice di attivazione

Questo passaggio è disponibile solo se si attiva l'applicazione utilizzando un codice di attivazione. Se si attiva la versione di prova dell'applicazione o durante l'attivazione dell'applicazione tramite un file chiave, questo passaggio viene saltato.

In questa fase Kaspersky Endpoint Security invia i dati al server di attivazione per verificare il codice di attivazione immesso:

- Se la verifica del codice di attivazione riesce, la Configurazione iniziale guidata procede automaticamente alla finestra successiva.

- Se la verifica del codice di attivazione non riesce, viene visualizzato un messaggio corrispondente. In questo caso, è consigliabile richiedere assistenza al fornitore del software da cui è stata acquistata la licenza di Kaspersky Endpoint Security.

- Se si supera il numero di attivazioni consentite per il codice di attivazione, viene visualizzata una notifica corrispondente. La Configurazione iniziale guidata viene interrotta e l'applicazione suggerisce di contattare l'Assistenza tecnica di Kaspersky.

Per tornare al passaggio precedente della Configurazione iniziale guidata, fare clic sul pulsante **Indietro**. Per interrompere la Configurazione iniziale guidata, fare clic sul pulsante **Annulla**.

## Attivazione tramite un file chiave

Questo passaggio è disponibile solo se si attiva l'applicazione utilizzando un file chiave.

Durante questo passaggio, specificare il percorso del file chiave. A tale scopo, fare clic sul pulsante **Sfoglia** e selezionare un file chiave nel formato `<ID file>.key`.

Dopo avere selezionato un file chiave, nella parte inferiore della finestra vengono visualizzate le seguenti informazioni:

- Chiave
- Tipo di licenza (commerciale o di prova) e numero di computer coperti dalla licenza
- Data di attivazione dell'applicazione nel computer
- Data di scadenza della licenza
- Funzionalità dell'applicazione disponibili nell'ambito della licenza
- Notifiche sugli eventuali problemi relativi alla chiave. Ad esempio, *Blacklist delle chiavi danneggiata*.

Per tornare al passaggio precedente della Configurazione iniziale guidata, fare clic sul pulsante **Indietro**. Per procedere con la Configurazione iniziale guidata, fare clic sul pulsante **Avanti**. Per interrompere la Configurazione iniziale guidata, fare clic sul pulsante **Annulla**.

## Selezione delle funzioni da attivare

Questo passaggio è disponibile solo durante l'attivazione della versione di prova dell'applicazione.

Durante questo passaggio è possibile selezionare le funzionalità che diventeranno disponibili dopo l'attivazione dell'applicazione:

- **Installazione di base**. Se questa opzione è selezionata, dopo l'attivazione dell'applicazione saranno disponibili solo i componenti della protezione, Controllo privilegi applicazioni e Monitor vulnerabilità.
- **Installazione standard**. Se questa opzione è selezionata, dopo l'attivazione dell'applicazione saranno disponibili solo i componenti della protezione e controllo.
- **Installazione completa**. Se questa opzione è selezionata, dopo l'attivazione dell'applicazione saranno disponibili tutti i componenti dell'applicazione installata, inclusa la funzionalità di criptaggio dei dati.

Se durante l'installazione si selezionano più componenti di quelli consentiti dalla licenza acquistata, dopo attivazione dell'applicazione i componenti che sono non disponibili in base alla licenza saranno installati, ma non saranno operativi. Se la licenza acquistata consente l'utilizzo di più componenti rispetto a quelli attualmente installati, dopo l'attivazione dell'applicazione, i componenti non installati sono elencati nella sezione **Gestione delle licenze**.

Per impostazione predefinita, è selezionata l'installazione standard.

Per tornare al passaggio precedente della Configurazione iniziale guidata, fare clic sul pulsante **Indietro**. Per procedere con la Configurazione iniziale guidata, fare clic sul pulsante **Avanti**. Per interrompere la Configurazione iniziale guidata, fare clic sul pulsante **Annulla**.

## Completamento dell'attivazione

Durante questo passaggio, la Configurazione iniziale guidata conferma il completamento dell'attivazione di Kaspersky Endpoint Security. Sono disponibili le seguenti informazioni sulla licenza:

- Tipo di licenza (commerciale o di prova) e numero di computer coperti dalla licenza
- Data di scadenza della licenza
- Funzionalità dell'applicazione disponibili nell'ambito della licenza

Per procedere con la Configurazione iniziale guidata, fare clic sul pulsante **Avanti**. Per interrompere la Configurazione iniziale guidata, fare clic sul pulsante **Annulla**.

## Analisi del sistema operativo

Durante questo passaggio vengono raccolte informazioni sulle applicazioni incluse nel sistema operativo. Queste applicazioni vengono aggiunte all'elenco delle applicazioni attendibili, le cui azioni nel sistema operativo non sono soggette ad alcuna restrizione.

Le altre applicazioni vengono analizzate al primo avvio dopo l'installazione di Kaspersky Endpoint Security.

Per interrompere la Configurazione iniziale guidata, fare clic sul pulsante **Annulla**.

## Completamento della configurazione iniziale dell'applicazione

La finestra di completamento della Configurazione iniziale guidata contiene informazioni sul completamento del processo di installazione di Kaspersky Endpoint Security.

Per avviare Kaspersky Endpoint Security, fare clic sul pulsante **Fine**.

Se si desidera chiudere la Configurazione iniziale guidata senza avviare Kaspersky Endpoint Security, deselezionare la casella di controllo **Avvia Kaspersky Endpoint Security 10 for Windows** e fare clic su **Fine**.

## Informativa di Kaspersky Security Network

Durante questo passaggio viene offerta la possibilità di partecipare a Kaspersky Security Network.

Leggere l'informativa di Kaspersky Security Network:

- Se si accettano tutte le condizioni, selezionare l'opzione **Accetto le condizioni di adesione al programma Kaspersky Security Network** nella finestra della Configurazione iniziale dell'applicazione.
- Se non si accettano le condizioni di adesione a Kaspersky Security Network, selezionare l'opzione **Non accetto le condizioni di adesione al programma Kaspersky Security Network** nella finestra della Configurazione iniziale dell'applicazione.

Per continuare la Configurazione iniziale dell'applicazione, fare clic su **OK**.

## Informazioni sulle modalità di aggiornamento di una versione precedente dell'applicazione

Per eseguire l'aggiornamento di una versione precedente dell'applicazione a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, decrittare tutte le unità disco rigido criptate.

È possibile eseguire l'aggiornamento delle seguenti applicazioni a Kaspersky Endpoint Security 10 Service Pack 2 for Windows:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 (build 6.0.4.1424) / MP4 CF2 (build 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (build 6.0.4.1424) / MP4 CF2 (build 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (build 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (build 10.2.2.10535 (MR1))
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (build 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (build 10.2.5.3201).

Quando si esegue l'aggiornamento di una delle applicazioni elencate in precedenza a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, il contenuto di Quarantena e Backup non viene trasferito.

È possibile aggiornare la versione precedente dell'applicazione nei modi seguenti:

- Localmente in modalità interattiva, utilizzando l'Installazione guidata dell'applicazione.
- Localmente in modalità non interattiva, dalla riga di comando
- In remoto tramite il software Kaspersky Security Center (vedere la *Guida all'implementazione di Kaspersky Security Center*)
- In remoto tramite l'Editor Criteri di gruppo di Microsoft Windows (vedere i file della Guida del sistema operativo)

Quando si esegue l'aggiornamento di una versione precedente dell'applicazione a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, non è necessario rimuovere la versione precedente dell'applicazione. È consigliabile chiudere tutte le applicazioni in esecuzione prima di avviare l'aggiornamento della versione precedente dell'applicazione.

## Rimozione dell'applicazione

In questa sezione viene descritto come rimuovere Kaspersky Endpoint Security dal computer.

## Informazioni sulle modalità di rimozione dell'applicazione

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

Kaspersky Endpoint Security può essere rimosso dal computer in diversi modi:

- Localmente in modalità interattiva, utilizzando l'Installazione guidata
- Localmente in modalità non interattiva, dalla riga di comando
- In remoto tramite il software Kaspersky Security Center (per informazioni dettagliate, vedere la *Guida all'implementazione di Kaspersky Security Center*)
- In remoto tramite l'Editor Criteri di gruppo di Microsoft Windows (vedere i file della Guida del sistema operativo)

## Rimozione dell'applicazione tramite l'Installazione guidata

*Per rimuovere Kaspersky Endpoint Security tramite l'Installazione guidata:*

1. Dal menu **Start** selezionare **Applicazioni** → **Kaspersky Endpoint Security 10 for Windows** → **Modifica, Ripristina o Rimuovi**.

   Verrà avviata l'Installazione guidata.

2. Nella finestra **Modifica, ripristino o rimozione dell'applicazione** dell'Installazione guidata fare clic sul pulsante **Rimuovi**.

3. Attenersi alle istruzioni dell'Installazione guidata.

## Passaggio 1. Salvataggio dei dati dell'applicazione per il riutilizzo

Durante questo passaggio è possibile specificare i dati dell'applicazione che si desidera mantenere per riutilizzarli nel corso della successiva installazione dell'applicazione (ad esempio, quando si installa una nuova versione). Se non si specifica alcun dato, l'applicazione verrà rimossa completamente.

*Per salvare i dati dell'applicazione per il riutilizzo:*

Selezionare le caselle di controllo accanto ai tipi di dati che si desidera salvare:

- **Dati di attivazione** - dati che eliminano l'esigenza di attivare l'applicazione installata successivamente. L'applicazione viene attivata automaticamente utilizzando la licenza corrente, a condizione che la licenza non sia scaduta al momento dell'installazione.
- **File di backup e in quarantena** - file esaminati dall'applicazione e spostati nel backup o in quarantena.

  Ai file di backup e in quarantena 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 e in quarantena dopo la rimozione dell'applicazione, è necessario ripristinare tali oggetti dagli archivi prima di rimuovere l'applicazione. Tuttavia, gli esperti di Kaspersky sconsigliano di ripristinare i file da Backup e Quarantena, perché potrebbero danneggiare il computer.

- **Impostazioni operative dell'applicazione** - valori delle impostazioni dell'applicazione selezionati durante la configurazione dell'applicazione.

- **Archivio locale delle chiavi di criptaggio** - dati che consentono di accedere direttamente ai file e ai dispositivi che sono stati criptati prima della rimozione dell'applicazione. È possibile accedere direttamente ai file e alle unità criptati dopo la reinstallazione dell'applicazione con la funzionalità di criptaggio.

  Questa casella di controllo è selezionata per impostazione predefinita.

Per procedere con l'Installazione guidata, fare clic sul pulsante **Avanti**. Per interrompere l'Installazione guidata, fare clic sul pulsante **Annulla**.

## Passaggio 2. Conferma della rimozione dell'applicazione

Dal momento che la rimozione dell'applicazione mette a rischio la protezione del computer, viene richiesto di confermare la rimozione. A tale scopo, fare clic sul pulsante **Rimuovi**.

Per interrompere la rimozione dell'applicazione in qualsiasi momento, fare clic sul pulsante **Annulla**.

## Passaggio 3. Rimozione dell'applicazione. Completamento della rimozione

Durante questo passaggio l'Installazione guidata rimuove l'applicazione dal computer. Attendere il completamento della rimozione dell'applicazione.

Durante la rimozione dell'applicazione, può essere necessario un riavvio il sistema operativo. Se si decide di non eseguire immediatamente il riavvio, la procedura di rimozione dell'applicazione resterà incompleta finché il sistema operativo non verrà riavviato o il computer non verrà spento e riacceso.

## Rimozione dell'applicazione dalla riga di comando

È possibile avviare il processo di disinstallazione dell'applicazione dalla riga di comando. La disinstallazione viene eseguita in modalità interattiva o invisibile all'utente (senza avviare l'Installazione guidata dell'applicazione).

*Per avviare il processo di disinstallazione dell'applicazione in modalità interattiva:*

Nella riga di comando digitare `setup.exe /x` o `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Verrà avviata l'Installazione guidata. Attenersi alle istruzioni dell'Installazione guidata.

*Per avviare il processo di disinstallazione dell'applicazione in modalità invisibile all'utente:*

Nella riga di comando digitare `setup.exe /s /x` o `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Il processo di disinstallazione dell'applicazione verrà avviato in modalità invisibile all'utente (senza avviare l'Installazione guidata).

Se l'operazione di disinstallazione dell'applicazione è protetta tramite password, è necessario immettere il nome utente e la password corrispondente nella riga di comando.

*Per rimuovere l'applicazione dalla riga di comando in modalità interattiva quando sono impostati il nome utente e la password per l'autenticazione della rimozione, della modifica o del ripristino di Kaspersky Endpoint Security:*

Nella riga di comando digitare `setup.exe /pKLLOGIN=<Nome utente> /pKLPASSWD=***** /x` oppure

```
msiexec.exe KLLOGIN=<Nome utente> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-
56E6EF762275}.
```

Verrà avviata l'Installazione guidata. Attenersi alle istruzioni dell'Installazione guidata.

*Per rimuovere l'applicazione dalla riga di comando in modalità invisibile all'utente quando sono impostati il nome utente e la password per l'autenticazione della rimozione, della modifica o del ripristino di Kaspersky Endpoint Security:*

Nella riga di comando digitare `setup.exe /pKLLOGIN=<Nome utente> /pKLPASSWD=***** /s /x` oppure

```
msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<Nome utente>
KLPASSWD=***** /qn.
```

## Rimozione degli oggetti e dei dati rimanenti in seguito all'operazione di verifica 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 nei dischi rigidi del sistema in seguito all'operazione di verifica dell'agente di autenticazione in due modi:

- Utilizzo del criterio di Kaspersky Security Center.
- Utilizzo dell'utilità di ripristino.

*Per utilizzare un criterio di Kaspersky Security Center per rimuovere gli oggetti e i dati rimanenti dopo l'operazione di verifica dell'agente di autenticazione:*

1. Applicare al computer un criterio di Kaspersky Security Center con impostazioni configurate per il decriptaggio di tutti i dischi rigidi del computer.
2. Avviare Kaspersky Endpoint Security.

*Per utilizzare l'utilità di ripristino per rimuovere gli oggetti e i dati rimanenti dopo l'operazione di verifica dell'agente di autenticazione:*

1. Avviare l'utilità di ripristino eseguendo il file eseguibile fdert.exe creato utilizzando Kaspersky Endpoint Security nel computer con il disco rigido del sistema connesso con oggetti e dati rimanenti in seguito all'operazione di verifica dell'agente di autenticazione.

2. Nell'elenco a discesa **Seleziona dispositivo** della finestra dell'utilità di ripristino selezionare il disco rigido del sistema con gli oggetti e i dati da rimuovere.

3. Fare clic sul pulsante **Scansione**.

4. Fare clic sul pulsante **Elimina oggetti e dati dell'agente di autenticazione**.

   Verrà avviato il processo di rimozione degli oggetti e dei dati rimanenti in seguito all'operazione di verifica dell'agente di autenticazione.

Al termine della rimozione degli oggetti e dei dati rimanenti in seguito all'operazione di verifica dell'agente di autenticazione potrebbe essere necessario rimuovere le informazioni sull'incompatibilità dell'applicazione con l'agente di autenticazione.

*Per rimuovere le informazioni sull'incompatibilità dell'applicazione con l'agente di autenticazione,*

Digitare il comando `avp pbatestreset` nella riga di comando.

I componenti di criptaggio devono essere installati perché il comando `avp pbatestreset` venga eseguito.

# Interfaccia dell'applicazione

Questa sezione descrive gli elementi principali dell'interfaccia dell'applicazione.

# 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.

## Indicazione dell'attività dell'applicazione

L'icona dell'applicazione è un indicatore dell'attività dell'applicazione:

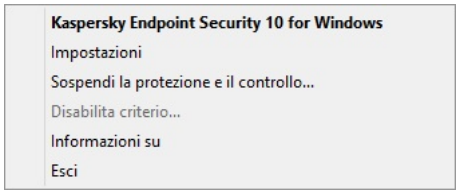
- L'icona indica che tutti i componenti della protezione dell'applicazione sono abilitati.
- L'icona indica che durante l'esecuzione di Kaspersky Endpoint Security si sono verificati eventi importanti che richiedono l'attenzione dell'utente. Ad esempio, Anti-Virus File è disabilitato o i database delle applicazioni non sono aggiornati.
- L'icona indica che durante l'esecuzione di Kaspersky Endpoint Security si sono verificati eventi critici. Ad esempio, un errore durante l'esecuzione di un componente o il danneggiamento dei database dell'applicazione.

# Menu di scelta rapida dell'icona dell'applicazione

Il menu di scelta rapida dell'icona dell'applicazione contiene i seguenti elementi:

- **Kaspersky Endpoint Security 10 for Windows**. Apre la scheda **Protezione e controllo** della finestra principale dell'applicazione. La scheda **Protezione e controllo** consente di regolare il funzionamento dei componenti e delle attività dell'applicazione e di visualizzare le statistiche relative ai file elaborati e alle minacce rilevate.
- **Impostazioni**. Apre la scheda **Impostazioni** della finestra principale dell'applicazione. La scheda **Impostazioni** consente di modificare le impostazioni predefinite dell'applicazione.
- **Sospendi la protezione e il controllo** / **Riprendi la protezione e il controllo**. Consente di sospendere temporaneamente o riprendere l'esecuzione dei componenti della protezione e controllo. Questa voce del menu di scelta rapida non influisce sulle attività di aggiornamento e scansione, perché è disponibile solo quando il criterio di Kaspersky Security Center è disabilitato.
- **Disabilita criterio** / **Abilita criterio**. Consente di disabilitare o abilitare il criterio di Kaspersky Security Center. Questa voce del menu di scelta rapida è disponibile quando Kaspersky Endpoint Security viene eseguito in base a un criterio ed è stata impostata una password per la disabilitazione del criterio di Kaspersky Security Center.
- **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

È possibile aprire il menu di scelta rapida dell'icona dell'applicazione posizionando il puntatore sull'icona dell'applicazione nell'area di notifica della barra delle applicazioni di Microsoft Windows, quindi facendo clic con il pulsante destro del mouse.

## Finestra principale dell'applicazione

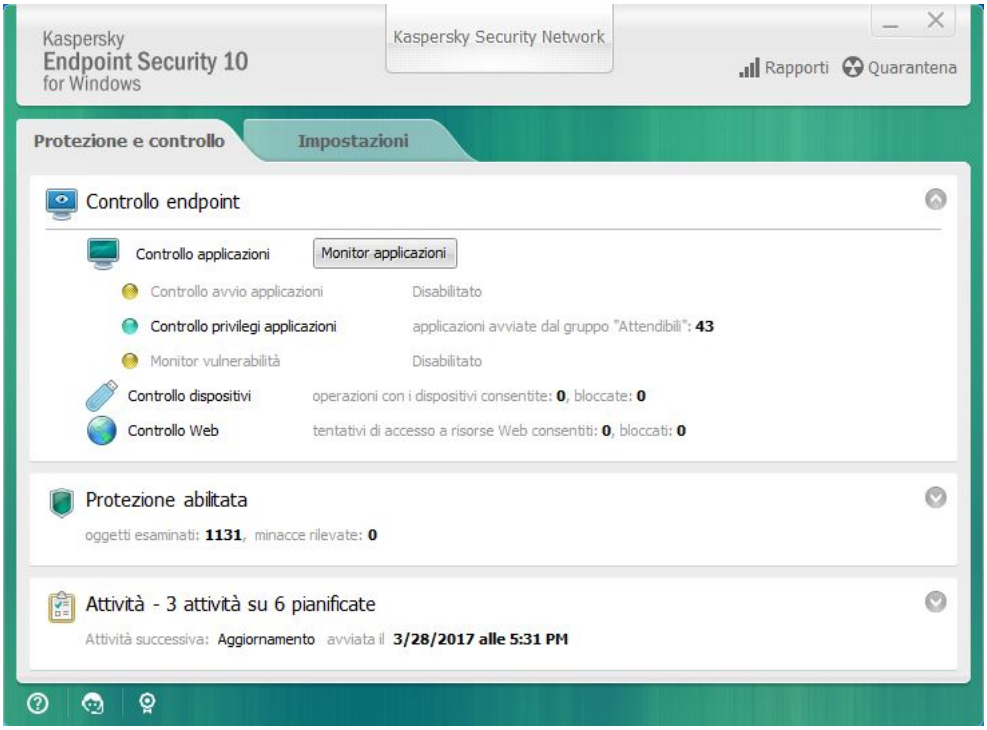
La finestra principale di Kaspersky Endpoint Security contiene gli elementi di interfaccia che permettono di accedere a tutte le funzionalità principali dell'applicazione.

La finestra principale dell'applicazione è suddivisa in quattro parti (vedere la figura seguente):

- La parte superiore della finestra contiene gli elementi dell'interfaccia che consentono di visualizzare le seguenti informazioni:
  - Dettagli sull'applicazione
  - Statistiche di Kaspersky Security Network
  - Elenco dei file non elaborati
  - Elenco delle vulnerabilità rilevate
  - Elenco dei file in quarantena
  - Archivio delle copie dei file infetti eliminati dall'applicazione
  - Rapporti sugli eventi che si sono verificati durante il funzionamento dell'applicazione in generale o dei singoli componenti oppure durante l'esecuzione delle attività
- La scheda **Protezione e controllo** consente di regolare l'esecuzione dei componenti dell'applicazione e il completamento delle attività. La scheda **Protezione e controllo** viene visualizzata all'apertura della finestra principale dell'applicazione.
- La scheda **Impostazioni** consente di modificare le impostazioni predefinite dell'applicazione.
- La parte inferiore della finestra contiene i seguenti elementi:
  - **Pulsante** . Questo pulsante visualizza la Guida di Kaspersky Endpoint Security.
  - **Pulsante** . Questo pulsante apre la finestra **Assistenza**, che contiene informazioni sul sistema operativo, la versione corrente di Kaspersky Endpoint Security e collegamenti a risorse informative di Kaspersky.
  - **Pulsante** / . Questo pulsante apre la finestra **Gestione delle licenze**, che contiene le informazioni sulla licenza corrente.

- **Pulsante** / / Questo pulsante apre la finestra **Eventi**, che contiene informazioni sugli aggiornamenti disponibili e sulle richieste di accesso a file e dispositivi criptati.

  Il pulsante è disponibile solo quando sono presenti richieste di accesso o aggiornamenti disinstallati.




Finestra principale dell'applicazione

*Per aprire la finestra principale di Kaspersky Endpoint Security, eseguire una delle seguenti operazioni:*

- Fare clic sull'icona dell'applicazione nell'area di notifica della barra delle applicazioni di Microsoft Windows.
- Selezionare **Kaspersky Endpoint Security 10 for Windows** nel menu di scelta rapida dell'icona dell'applicazione.

## Scheda Configura le impostazioni dell'applicazione

Nella scheda delle impostazioni di Kaspersky Endpoint Security è possibile configurare le impostazioni generali dell'applicazione, singoli componenti, rapporti e archivi, attività di scansione, attività di aggiornamento, attività di scansione delle vulnerabilità e la comunicazione con i server Kaspersky Security Network.

La scheda delle impostazioni dell'applicazione si compone di due parti (vedere la figura seguente):

- La parte sinistra contiene i componenti dell'applicazione, le attività e una sezione di impostazioni avanzate che comprende varie sottosezioni.
- La parte destra contiene elementi di controllo che è possibile utilizzare per configurare le impostazioni dell'attività o del componente selezionato nella parte sinistra della finestra, nonché le impostazioni avanzate.


Scheda Configura le impostazioni dell'applicazione

*Per aprire la scheda delle impostazioni dell'applicazione, eseguire una delle seguenti operazioni:*

- Nella finestra principale dell'applicazione selezionare la scheda **Impostazioni**.
- Dal menu di scelta rapida dell'icona dell'applicazione selezionare **Impostazioni**.

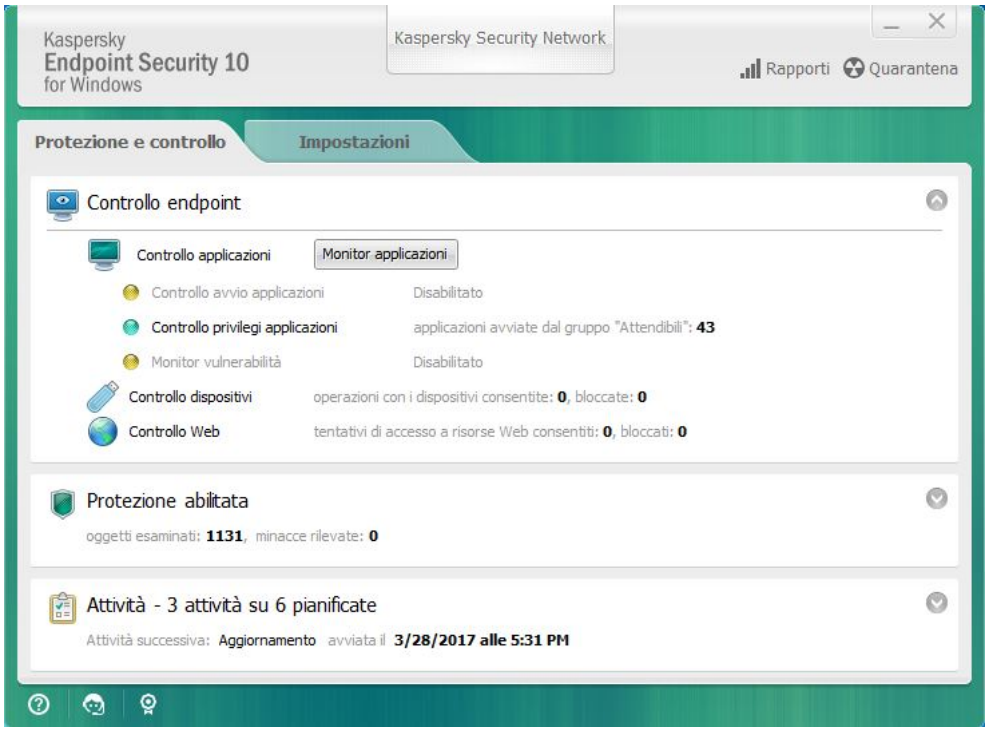
## Scheda Protezione e controllo

La scheda Protezione e controllo di Kaspersky Endpoint Security fornisce informazioni generali sulle prestazioni di tutte le attività e l'esecuzione di tutti i componenti dell'applicazione. In questa scheda è inoltre possibile gestire l'esecuzione dei componenti e le prestazioni delle attività.

La scheda Protezione e controllo si compone di tre parti (vedere la figura seguente):

- La sezione **Controllo endpoint** contiene un elenco dei componenti di controllo.
- La sezione **Gestione protezione** contiene un elenco dei componenti della protezione anti-virus.
- La sezione **Attività** contiene un elenco delle attività locali in esecuzione nel computer.

Ogni sezione contiene elementi di controllo che è possibile utilizzare per abilitare o disabilitare l'esecuzione di un componente, accedere alle impostazioni per l'attività o il componente selezionato e visualizzare le statistiche sull'esecuzione dell'attività o del componente selezionato.




Scheda Protezione e controllo

*Per aprire la scheda Protezione e controllo, eseguire una delle seguenti operazioni:*

- Nella finestra principale dell'applicazione selezionare la scheda **Protezione e controllo**.
- Fare clic sull'icona dell'applicazione nell'area di notifica della barra delle applicazioni di Microsoft Windows.
- Selezionare **Kaspersky Endpoint Security 10 for Windows** nel menu di scelta rapida dell'icona dell'applicazione.

# Licensing dell'applicazione

Questa sezione fornisce informazioni su concetti generali legati alla gestione delle licenze dell'applicazione.

## 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. Il documento è incluso nel kit di distribuzione dell'applicazione.

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.

Una licenza valida consente di usufruire dei seguenti tipi di servizi:

- Utilizzo dell'applicazione in conformità alle condizioni del Contratto di licenza con l'utente finale
- Assistenza tecnica

L'ambito dei servizi e le 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:

- 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 di validità della licenza
- Data di scadenza della licenza o periodo di validità della licenza
- Tipo di licenza

## Informazioni sull'abbonamento

Un *abbonamento per Kaspersky Endpoint Security* è un ordine di acquisto per l'applicazione con specifici parametri (data di scadenza dell'abbonamento, 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.

Nel caso di un abbonamento limitato, dopo la scadenza può essere offerto un periodo di pre-sospensione per il rinnovo dell'abbonamento, durante il quale l'applicazione mantiene le proprie funzionalità. Il fornitore del servizio decide se concedere o meno un periodo di pre-sospensione e, nel caso, ne determina la durata.

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 è installata. La chiave attiva definisce la licenza per l'utilizzo dell'applicazione con l'abbonamento. Una chiave di riserva può essere installata solo utilizzando un codice di attivazione (non tramite un file chiave o con un abbonamento).

Le funzionalità dell'applicazione disponibili con abbonamento possono corrispondere a funzionalità dell'applicazione per i seguenti tipi di licenze commerciali: Standard, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Le licenze di questo tipo consentono la protezione di file server, workstation e dispositivi mobili e supportano l'utilizzo dei componenti di controllo in workstation e dispositivi mobili.

Le opzioni possibili per la gestione dell'abbonamento possono variare a seconda del fornitore del servizio. Il fornitore del servizio potrebbe non offrire un periodo di pre-sospensione per il rinnovo dell'abbonamento, durante il quale l'applicazione mantiene le proprie funzionalità.

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

## Informazioni sul codice di attivazione

Il *codice di attivazione* è una sequenza alfanumerica univoca di venti lettere dell'alfabeto latino e numeri che si riceve acquistando una licenza commerciale per 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 è attivata tramite un codice di attivazione, viene installata la chiave attiva. Una chiave di riserva può essere installata solo utilizzando un codice di attivazione (non tramite un file chiave o con un abbonamento).

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 registrarsi per un Kaspersky CompanyAccount. Per ripristinare un codice di attivazione, è necessario contattare l'Assistenza tecnica di Kaspersky.

## Informazioni sulla chiave

Una *chiave* è una sequenza alfanumerica univoca. La chiave consente di utilizzare l'applicazione in base alle condizioni indicate nel certificato di licenza (tipo di licenza, periodo di validità della licenza, restrizioni della licenza).

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

È possibile aggiungere una chiave all'applicazione mediante un codice di attivazione o un file chiave.

È possibile aggiungere, modificare o eliminare le chiavi. 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 inserita nella blacklist, è necessario aggiungere una chiave diversa per continuare a utilizzare l'applicazione.

Se una chiave per una licenza scaduta è stata eliminata, le funzionalità dell'applicazione non sono disponibili. Non è possibile aggiungere nuovamente tale chiave dopo averla eliminata.

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. Alla scadenza 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 inserita nella blacklist, le funzionalità dell'applicazione definite dalla licenza con cui è stata attivata l'applicazione restano disponibili per otto giorni. Kaspersky Security Network e gli aggiornamenti dei moduli dell'applicazione sono disponibili senza restrizioni. L'applicazione notifica all'utente che la chiave è stata inserita nella blacklist. Dopo otto giorni, le funzionalità dell'applicazione diventano limitate al livello di funzionalità disponibile dopo la scadenza della licenza: l'applicazione viene eseguita senza aggiornamenti e Kaspersky Security Network non è disponibile.

## Informazioni sul file chiave

Un *file chiave* è un file con estensione .key che si riceve da Kaspersky in seguito all'acquisto di Kaspersky Endpoint Security. Lo scopo di un file chiave è quello di aggiungere una chiave per l'attivazione dell'applicazione.

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 produttore 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 licenza aggiuntiva può essere aggiunta solo utilizzando un file chiave e non può essere aggiunta tramite un codice di attivazione.

## Informazioni sulla trasmissione dei dati

Accettando il Contratto di licenza con l'utente finale, l'utente accetta di trasferire automaticamente informazioni sull'utilizzo del prodotto, nonché il tipo, la versione e la localizzazione del programma installato, l'identificatore univoco del programma di installazione, il tipo di installazione e i dati su chiavi attive e di riserva (inclusi il tipo di licenza, il periodo di validità, la data di attivazione del programma e la data di scadenza della licenza, il numero della licenza, lo stato corrente della licenza, la versione del protocollo per l'interazione con il server di attivazione).

Se il programma è attivato con un codice di attivazione, per ricevere informazioni statistiche sulla distribuzione e l'utilizzo dei prodotti del titolare della licenza, l'utente accetta di fornire automaticamente la versione del programma in uso (inclusi le informazioni sugli aggiornamenti del software installati, l'identificatore del programma di installazione e le informazioni sulle licenze), la versione del sistema operativo e gli identificatori dei componenti del programma attivi al momento dell'invio delle informazioni.

Le informazioni ricevute sono protette da Kaspersky in conformità alla legge e ai requisiti e alle normative applicabili di Kaspersky.

Kaspersky utilizza le informazioni ricevute in modo completamente anonimo e solo come dati statistici generali. Le statistiche generali vengono generate automaticamente utilizzando le informazioni raccolte originariamente e non contengono dati personali o altre informazioni riservate. Le informazioni raccolte originariamente vengono distrutte man mano che si accumulano (una volta all'anno). I dati statistici generali sono archiviati a tempo indeterminato.

Leggere il Contratto di licenza con l'utente finale e visitare il sito Web di Kaspersky per informazioni su come vengono raccolte, 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 KSN. I file license.txt e ksn.txt, che contengono il Contratto di licenza con l'utente finale e l'Informativa KSN, sono inclusi nel pacchetto di distribuzione del programma.

## Visualizzazione delle informazioni sulla licenza

*Per visualizzare le informazioni sulla licenza:*

1. Aprire la finestra principale dell'applicazione.
2. Fare clic sul pulsante / nella parte inferiore della finestra principale dell'applicazione.

   Verrà visualizzata la finestra **Gestione delle licenze**. Le informazioni sulla licenza vengono visualizzate nella sezione disponibile nella parte superiore della finestra **Gestione delle licenze**.

## Acquisto di una licenza

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

*Per acquistare una licenza:*

1. Aprire la finestra principale dell'applicazione.
2. Fare clic sul pulsante / nella parte inferiore della finestra principale dell'applicazione.

   Verrà visualizzata la finestra **Gestione delle licenze**.
3. Nella finestra **Gestione delle licenze** 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 di una licenza

Quando la licenza sta per scadere, è possibile rinnovarla. In questo modo è possibile assicurare la protezione del computer dopo la scadenza della licenza corrente e prima dell'attivazione dell'applicazione con una nuova licenza.

*Per rinnovare una licenza:*

1. Ricevere un nuovo codice di attivazione dell'applicazione o un file chiave.
2. Aggiungere una chiave di riserva con il codice di attivazione o il file chiave ricevuto.

   Come risultato, viene aggiunta una chiave di riserva. Questa chiave diventa attiva alla scadenza della licenza.

L'aggiornamento della chiave dallo stato "di riserva" allo stato "attiva" può richiedere un certo tempo per via della distribuzione del carico tra i server di attivazione di Kaspersky.

## 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, il giorno della scadenza dell'abbonamento (o del periodo di pre-sospensione dopo la scadenza dell'abbonamento, durante il quale è possibile effettuare il rinnovo), Kaspersky Endpoint Security visualizza una notifica corrispondente e interrompe i tentativi di rinnovare l'abbonamento automaticamente. 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.

È possibile aggiornare lo stato dell'abbonamento manualmente nella finestra **Gestione delle licenze**. Questo può essere necessario se l'abbonamento è stato rinnovato dopo la scadenza del periodo di pre-sospensione e l'applicazione non ha aggiornato lo stato dell'abbonamento automaticamente.

## Apertura del sito Web del fornitore del servizio

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

1. Aprire la finestra principale dell'applicazione.
2. Fare clic sul pulsante / nella parte inferiore della finestra principale dell'applicazione.

   Verrà visualizzata la finestra **Gestione delle licenze**.
3. Nella finestra **Gestione delle licenze** fare clic su **Contatta fornitore abbonamento**.

## Informazioni sui metodi di 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. Il processo di attivazione dell'applicazione implica l'aggiunta di una chiave.

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

- Durante l'installazione dell'applicazione tramite la Configurazione iniziale guidata. È possibile aggiungere la chiave attiva in questo modo.
- 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. In questo modo è possibile aggiungere sia la chiave attiva che la chiave di riserva.
- In remoto distribuendo ai computer client le chiavi e i codici di attivazione memorizzati nell'archivio delle chiavi di Kaspersky Security Center Administration Server (per informazioni dettagliate, consultare la *Guida dell'amministratore 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.

## Utilizzo dell'Attivazione guidata per attivare l'applicazione

*Per attivare Kaspersky Endpoint Security tramite l'Attivazione guidata:*

1. Fare clic sul pulsante / nella parte inferiore della finestra principale dell'applicazione.

   Verrà visualizzata la finestra **Gestione delle licenze**.

2. Nella finestra **Gestione delle licenze** fare clic sul pulsante **Attiva il prodotto con una nuova licenza**.

   Verrà avviata l'Attivazione guidata dell'applicazione.

3. Attenersi alle istruzioni dell'Attivazione guidata.

Per informazioni più dettagliate sulla procedura di attivazione dell'applicazione, vedere la sezione relativa alla Configurazione iniziale guidata.

## Attivazione dell'applicazione dalla riga di comando

*Per attivare l'applicazione dalla riga di comando:*

Digitare `avp.com license /add <codice di attivazione o file chiave> /password=<password>` nella riga di comando.

# Avvio e arresto dell'applicazione

In questa sezione viene descritto come è possibile configurare l'avvio automatico dell'applicazione, avviare o arrestare manualmente l'applicazione e sospendere o riprendere i componenti della protezione e controllo.

## Abilitazione e disabilitazione dell'avvio automatico dell'applicazione

La modalità di avvio automatico indica che Kaspersky Endpoint Security viene avviato immediatamente all'avvio del sistema operativo, senza l'intervento dell'utente. Questa opzione di avvio dell'applicazione è abilitata per impostazione predefinita.

Al termine dell'installazione, Kaspersky Endpoint Security viene avviato automaticamente per la prima volta. Successivamente, l'applicazione verrà avviata automaticamente all'avvio 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 caricato non determina una riduzione del livello di protezione del computer.

*Per abilitare o disabilitare l'avvio automatico dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Protezione anti-virus** a sinistra.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Eseguire una delle seguenti operazioni:
   - Se si desidera abilitare l'esecuzione automatica dell'applicazione, selezionare la casella di controllo **Avvia Kaspersky Endpoint Security 10 for Windows all'avvio del computer**.
   - Se si desidera disabilitare l'esecuzione automatica dell'applicazione, deselezionare la casella di controllo **Avvia Kaspersky Endpoint Security 10 for Windows all'avvio del computer**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Avvio e arresto manuale dell'applicazione

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.

Se è stato precedentemente disabilitato l'avvio automatico dell'applicazione, Kaspersky Endpoint Security deve essere avviato manualmente.

*Per avviare manualmente l'applicazione:*

Dal menu **Start** selezionare **Applicazioni** → **Kaspersky Endpoint Security 10 for Windows**.

*Per arrestare manualmente l'applicazione:*

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. Dal menu di scelta rapida selezionare **Esci**.

## 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 disabilitati.

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 e il controllo**.

   Verrà visualizzata la finestra **Sospendi la protezione**.
3. Selezionare una delle seguenti opzioni:
   - **Sospendi per il periodo di tempo specificato** - La protezione e il controllo del computer vengono ripresi al termine del periodo di tempo specificato nell'elenco a discesa sottostante.
   - **Sospendi fino al riavvio** - La protezione e il controllo del computer vengono ripresi dopo avere chiuso e riaperto l'applicazione o riavviato il sistema operativo. Per utilizzare questa opzione, deve essere abilitato l'avvio automatico dell'applicazione.
   - **Sospendi** - La protezione e il controllo del computer vengono ripresi quando l'utente decide di abilitarli nuovamente.
4. Se è stata selezionata l'opzione **Sospendi per il periodo di tempo specificato** durante il passaggio precedente, selezionare l'intervallo desiderato nell'elenco a discesa.

*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 **Riprendi la protezione e il controllo**.

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.

# Protezione del file system del computer. Anti-Virus File

Questa sezione contiene informazioni su Anti-Virus File e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Anti-Virus File

Anti-Virus File impedisce l'infezione del file system del computer. Per impostazione predefinita, Anti-Virus File viene avviato all'avvio di Kaspersky Endpoint Security, rimane attivo in modo permanente nella memoria del computer ed esamina tutti i file che vengono aperti, salvati o avviati nel computer e in tutte le unità ad esso collegate alla ricerca di virus e altre minacce.

Se viene rilevata una minaccia in un file, Kaspersky Endpoint Security esegue le seguenti operazioni:

1. Rileva il tipo di oggetto individuato nel file (ad esempio, un *virus* o un *Trojan*).
2. Contrassegna il file come *potenzialmente infetto* se durante la scansione non è possibile determinare se il file è infetto o meno. Il file può contenere una sequenza di codice tipica dei virus o di altro malware oppure un codice modificato di un virus conosciuto.
3. L'applicazione visualizza una notifica sull'oggetto dannoso rilevato nel file (se sono configurate le notifiche) ed elabora il file eseguendo l'azione specificata nelle impostazioni di Anti-Virus File.

## Abilitazione e disabilitazione di Anti-Virus File

Per impostazione predefinita, Anti-Virus File è abilitato e viene eseguito nella modalità consigliata dagli specialisti di Kaspersky. Se necessario, è possibile disabilitare Anti-Virus File.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Anti-Virus File nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Protezione**.

   Verrà aperta la sezione **Protezione**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente Anti-Virus File.

   Verrà visualizzato un menu per la selezione delle azioni sul componente.
5. Eseguire una delle seguenti operazioni:

- Per abilitare Anti-Virus File, selezionare **Avvia** dal menu.

  L'icona di stato del componente , visualizzata a sinistra nella riga **Anti-Virus File**, diventa .

- Per disabilitare Anti-Virus File, selezionare **Interrompi** dal menu.

  L'icona di stato del componente , visualizzata a sinistra nella riga **Anti-Virus File**, diventa .

*Per abilitare o disabilitare Anti-Virus File dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.
3. Eseguire una delle seguenti operazioni:

   - Per abilitare Anti-Virus File, selezionare la casella di controllo **Abilita Anti-Virus File**.
   - Per disabilitare Anti-Virus File, deselezionare la casella di controllo **Abilita Anti-Virus File**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Sospensione automatica di Anti-Virus File

È possibile configurare la sospensione automatica di Anti-Virus File a un orario specificato o durante l'esecuzione di programmi specifici.

La sospensione di Anti-Virus File in caso di conflitti con alcuni programmi rappresenta una misura di emergenza. In caso di conflitti durante l'esecuzione di un componente, è consigliabile contattare l'Assistenza tecnica di Kaspersky (https://companyaccount.kaspersky.com). Gli specialisti dell'Assistenza tecnica offriranno il supporto necessario per configurare Anti-Virus File per l'esecuzione con gli altri programmi installati nel computer.

*Per configurare la sospensione automatica di Anti-Virus File:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.
3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Anti-Virus File**.
4. Nella finestra **Anti-Virus File** selezionare la scheda **Avanzate**.
5. Nella sezione **Sospendi l'attività**:

   - Per configurare la sospensione automatica di Anti-Virus File a un orario specificato, selezionare la casella di controllo **In base alla pianificazione**, quindi fare clic sul pulsante **Pianificazione**.

Verrà visualizzata la finestra **Sospendi l'attività**.

- Per configurare la sospensione automatica di Anti-Virus File all'avvio delle applicazioni specificate, selezionare la casella di controllo **All'avvio dell'applicazione**, quindi fare clic sul pulsante **Seleziona**.

  Verrà visualizzata la finestra **Applicazioni**.

6. Eseguire una delle seguenti operazioni:

   - Se si sta configurando la sospensione automatica di Anti-Virus File a un orario specificato, nella finestra **Sospendi l'attività** utilizzare i campi **Sospendi l'attività alle** e **Riprendi l'attività alle** per specificare il periodo di tempo (nel formato HH:MM) per cui sospendere Anti-Virus File. Fare clic su **OK**.

   - Se si sta configurando la sospensione automatica di Anti-Virus File all'avvio delle applicazioni specificate, utilizzare i pulsanti **Aggiungi**, **Modifica** e **Rimuovi** nella finestra **Applicazioni** per creare un elenco di applicazioni durante la cui esecuzione sospendere Anti-Virus File. Fare clic su **OK**.

7. Nella finestra **Anti-Virus File** fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione di Anti-Virus File

È possibile eseguire le seguenti operazioni per configurare Anti-Virus File:

- Modificare il livello di protezione.

  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 protezione dei file, è possibile ripristinare in qualsiasi momento le impostazioni consigliate.

- Modificare l'azione eseguita da Anti-Virus File al rilevamento di un file infetto.

- Modificare l'ambito di protezione di Anti-Virus File.

  È possibile estendere o restringere l'ambito di protezione della scansione aggiungendo o rimuovendo oggetti da esaminare oppure modificando i tipi di file da esaminare.

- Configurare l'analizzatore euristico.

  Anti-Virus File utilizza una tecnica denominata analisi delle firme. Durante l'analisi delle firme, Anti-Virus File confronta l'oggetto rilevato con i record nei database anti-virus dell'applicazione. In base alle raccomandazioni degli specialisti di Kaspersky, l'analisi delle firme è sempre abilitata.

  Per aumentare l'efficacia della protezione, è possibile utilizzare l'analisi euristica. Durante l'analisi euristica, Anti-Virus File analizza l'attività degli oggetti nel sistema operativo. L'analisi euristica consente il rilevamento degli oggetti dannosi per cui al momento non sono presenti record nei database anti-virus dell'applicazione.

- Ottimizzare la scansione.

  È possibile ottimizzare la scansione dei file eseguita da Anti-Virus File riducendo il tempo di scansione e aumentando la velocità di esecuzione di Kaspersky Endpoint Security. Per ottenere questo risultato, è possibile eseguire la scansione solo dei file nuovi e modificati dopo l'ultima scansione. Questa modalità si applica sia ai file semplici che compositi.

  È inoltre possibile abilitare l'utilizzo delle tecnologie iChecker e iSwift, che ottimizzano la velocità di scansione dei file escludendo i file che non sono stati modificati dall'ultima scansione.

- Configurare la scansione dei file compositi.
- Modificare la modalità di scansione dei file.

## Modifica del livello di protezione

Per proteggere il file system del computer, Anti-Virus File applica diversi gruppi di impostazioni. Questi gruppi di impostazioni sono denominati *livelli di protezione*. Esistono tre livelli di protezione preimpostati: **Alto**, **Consigliato** e **Basso**. Le impostazioni del livello di protezione **Consigliato** sono considerate le impostazioni ottimali consigliate dagli esperti di Kaspersky.

*Per modificare un livello di protezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.
3. Nella sezione **Livello di sicurezza** eseguire una delle seguenti operazioni:
   - Se si desidera applicare uno dei livelli di protezione preimpostati (**Alto**, **Consigliato** o **Basso**), selezionarlo con il dispositivo di scorrimento.
   - Se si desidera configurare un livello protezione personalizzato, fare clic sul pulsante **Impostazioni**, quindi immettere le impostazioni personalizzate nella finestra **Anti-Virus File** visualizzata.

     Al termine della configurazione di un livello di protezione personalizzato, il nome del livello di protezione nella sezione **Livello di sicurezza** viene modificato in **Personalizzato**.
   - Se si desidera impostare il livello di protezione su **Consigliato**, fare clic sul pulsante **Predefinito**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica dell'azione di Anti-Virus File da eseguire sui file infetti

*Per modificare l'azione di Anti-Virus File da eseguire sui file infetti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.
3. Nella sezione **Azione se viene rilevata una minaccia** selezionare l'opzione desiderata:
   - **Seleziona azione automaticamente**.
   - **Esegui azione: Disinfetta. Elimina se la disinfezione fallisce**.
   - **Esegui azione: Disinfetta**.

Anche se è selezionata questa opzione, Kaspersky Endpoint Security applica l'azione **Rimuovi** ai file che fanno parte dell'applicazione Windows Store.

- **Esegui azione: Rimuovi**.
- **Esegui azione: Blocca**.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica dell'ambito di protezione di Anti-Virus 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 i tipi di file da esaminare sono proprietà dell'ambito di protezione di Anti-Virus File. Per impostazione predefinita, Anti-Virus File esamina solo i file infettabili archiviati in dischi rigidi, unità di rete o supporti rimovibili.

*Per creare l'ambito di protezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.
3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Anti-Virus File**.
4. Nella finestra **Anti-Virus File** selezionare la scheda **Generale**.
5. Nella sezione **Tipi di file** specificare i tipi di file che devono essere esaminati da Anti-Virus File:
   - Per esaminare tutti i file, selezionare **Tutti i file**.
   - Per esaminare i file nei formati che presentano la maggiore vulnerabilità alle infezioni, selezionare **Esamina i file per formato**.
   - Per esaminare i file con le estensioni che presentano la maggiore vulnerabilità alle infezioni, selezionare **Esamina i file per estensione**.

   Durante la selezione del tipo di file da esaminare, tenere presenti le seguenti informazioni:
   - Per alcuni formati di file (ad esempio, txt), la probabilità di penetrazione e attivazione di codice dannoso è piuttosto bassa. Altri formati di file, al contrario, contengono o possono contenere codice eseguibile (ad esempio, exe, dll, doc). Il rischio di penetrazione e attivazione di codice dannoso in tali file è piuttosto alto.
   - Un utente malintenzionato potrebbe inviare un virus o un altro programma dannoso al computer dell'utente in un file eseguibile rinominato con estensione txt. Se si seleziona la scansione dei file in base all'estensione, tale file verrà ignorato dalla scansione. Se si seleziona la scansione dei file in base al formato, indipendentemente dall'estensione, Anti-Virus File analizza l'intestazione del file. L'analisi può rivelare che il file è in formato exe. Un file di questo tipo viene esaminato in modo approfondito alla ricerca di virus e altro malware.

6. Nell'elenco **Ambito di protezione** eseguire una delle seguenti operazioni:

   - Per aggiungere un nuovo oggetto all'ambito della scansione, fare clic sul pulsante **Aggiungi**.
   - Per modificare la posizione di un oggetto, selezionare l'oggetto nell'ambito della scansione, quindi fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Selezione ambito di scansione**.

   - Se si desidera rimuovere un oggetto dall'elenco degli oggetti da esaminare, selezionare l'oggetto desiderato nell'elenco, quindi fare clic sul pulsante **Rimuovi**.

     Verrà visualizzata una finestra per la conferma dell'eliminazione.

7. Eseguire una delle seguenti operazioni:

   - Se si desidera aggiungere un nuovo oggetto o modificare la posizione di un oggetto nell'elenco degli oggetti da esaminare, selezionare l'oggetto nella finestra **Selezione ambito di scansione**, quindi fare clic sul pulsante **Aggiungi**.

     Tutti gli oggetti selezionati nella finestra **Selezione ambito di scansione** vengono visualizzati nella finestra **Anti-Virus File**, nell'elenco **Ambito di protezione**.

     Fare clic su **OK**.

   - Se si desidera rimuovere un oggetto, fare clic sul pulsante **Sì** nella finestra per la conferma della rimozione.

8. Se necessario, ripetere i passaggi 6-7 per aggiungere, spostare o rimuovere gli oggetti dall'elenco degli oggetti da esaminare.

9. Per escludere un oggetto dall'elenco degli oggetti da esaminare, deselezionare la casella di controllo accanto all'oggetto nell'elenco **Ambito di protezione**. L'oggetto rimane nell'elenco degli oggetti da esaminare, ma viene escluso dalla scansione da parte di Anti-Virus File.

10. Nella finestra **Anti-Virus File** fare clic su **OK**.

11. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Utilizzo dell'analizzatore euristico con Anti-Virus File

*Per configurare l'utilizzo dell'analizzatore euristico durante l'esecuzione di Anti-Virus File:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.

3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Anti-Virus File**.

4. Nella finestra **Anti-Virus File** selezionare la scheda **Prestazioni**.

5. Nella sezione **Metodi di scansione**:

- Se si desidera che Anti-Virus File utilizzi l'analisi euristica, selezionare la casella di controllo **Analisi euristica** e utilizzare il dispositivo di scorrimento per impostare il livello dell'analisi euristica: **Superficiale**, **Media** o **Approfondita**.

- Se non si desidera che Anti-Virus File utilizzi l'analisi euristica, deselezionare la casella di controllo **Analisi euristica**.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Utilizzo delle tecnologie di scansione durante l'esecuzione di Anti-Virus File

*Per configurare l'utilizzo delle tecnologie di scansione durante l'esecuzione di Anti-Virus File:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.

3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Anti-Virus File**.

4. Nella finestra **Anti-Virus File** selezionare la scheda **Avanzate**.

5. Nella sezione **Tecnologie di scansione**:

   - Selezionare le caselle di controllo accanto ai nomi delle tecnologie che si desidera utilizzare durante l'esecuzione di Anti-Virus File.

   - Deselezionare le caselle di controllo accanto ai nomi delle tecnologie che non si desidera utilizzare durante l'esecuzione di Anti-Virus File.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Ottimizzazione della scansione dei file

*Per ottimizzare la scansione dei file:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.

3. Fare clic sul pulsante **Impostazioni**.

Verrà visualizzata la finestra **Anti-Virus File**.

4. Nella finestra **Anti-Virus File** selezionare la scheda **Prestazioni**.
5. Nella sezione **Ottimizzazione della scansione** selezionare la casella di controllo **Esamina solo i file nuovi e modificati**.
6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Scansione dei file compositi

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

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

Anti-Virus File disinfetta i file compositi nei formati RAR, ARJ, ZIP, CAB e LHA ed elimina i file in tutti gli altri formati (ad eccezione dei database di posta).

*Per configurare la scansione dei file compositi:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.
3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Anti-Virus File**.
4. Nella finestra **Anti-Virus File** selezionare la scheda **Prestazioni**.
5. Nella sezione **Scansione dei file compositi** specificare i tipi di file compositi di cui eseguire la scansione: archivi, pacchetti di installazione o file nei formati di Office.
6. Per eseguire la scansione solo dei file compositi nuovi e modificati, selezionare la casella di controllo **Esamina solo i file nuovi e modificati**.

   Anti-Virus File esaminerà solo i file compositi nuovi e modificati di tutti i tipi.
7. Fare clic sul pulsante **Avanzate**.

   Verrà visualizzata la finestra **File compositi**.
8. Nella sezione **Scansione in background** eseguire una delle seguenti operazioni:

- Per impedire ad Anti-Virus File di decomprimere i file compositi in background, deselezionare la casella di controllo **Decomprimi file compositi in background**.

- Per consentire ad Anti-Virus File di decomprimere i file compositi durante la scansione in background, selezionare la casella di controllo **Decomprimi file compositi in background**, quindi specificare il valore desiderato nel campo **Dimensioni minime dei file**.

9. Nella sezione **Dimensione massima** eseguire una delle seguenti operazioni:

   - Per impedire ad Anti-Virus File di decomprimere i file compositi di grandi dimensioni, selezionare la casella di controllo **Non decomprimere i file compositi molto grandi**, quindi specificare il valore desiderato nel campo **Dimensione massima dei file**. Anti-Virus File non decomprimerà i file compositi di dimensioni superiori al valore specificato.

   - Per consentire ad Anti-Virus File di decomprimere i file compositi di grandi dimensioni, deselezionare la casella di controllo **Non decomprimere i file compositi molto grandi**.

     Un file viene considerato di grandi dimensioni se le relative dimensioni superano il valore specificato nel campo **Dimensione massima dei file**.

   Anti-Virus File esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo **Non decomprimere i file compositi molto grandi** sia o meno selezionata.

10. Fare clic su **OK**.

11. Nella finestra **Anti-Virus File** fare clic su **OK**.

12. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica della modalità di scansione

La *modalità di scansione* rappresenta la condizione in base alla quale Anti-Virus File avvia la scansione dei file. Per impostazione predefinita, Kaspersky Endpoint Security esegue la scansione dei file in modalità Smart. In questa modalità di scansione, Anti-Virus 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. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus File**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus File.

3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Anti-Virus File**.

4. Nella finestra **Anti-Virus File** selezionare la scheda **Avanzate**.

5. Nella sezione **Modalità di scansione** selezionare la modalità desiderata:

- **Modalità Smart**.
- **In fase di accesso e modifica**.
- **In fase di accesso**.
- **In fase di esecuzione**.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Protezione dei messaggi e-mail. Anti-Virus Posta

Questo componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

Questa sezione contiene informazioni su Anti-Virus Posta e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Anti-Virus Posta

Anti-Virus Posta esamina tutti i messaggi e-mail in entrata e in uscita alla ricerca di virus e altre minacce. Viene avviato all'avvio di Kaspersky Endpoint Security, rimane attivo in modo permanente nella memoria del computer ed esamina tutti i messaggi inviati o ricevuti tramite i protocolli POP3, SMTP, IMAP, MAPI e NNTP. Se non vengono individuate minacce in un messaggio, questo viene reso disponibile e/o viene elaborato.

Se viene rilevata una minaccia in un messaggio e-mail, Anti-Virus Posta esegue le seguenti operazioni:

1. Identifica il tipo di oggetto individuato nel messaggio e-mail (ad esempio, un *Trojan*).
2. Ai messaggi e-mail viene assegnato uno dei seguenti stati:
   - *Potenzialmente infetto*. Questo stato viene assegnato se durante la scansione non è possibile determinare se il messaggio e-mail è infetto o meno. Il messaggio e-mail può contenere una sezione di codice tipica dei virus o di altro malware oppure un codice modificato di un virus conosciuto.
   - *Infetto*. Questo stato viene assegnato a un oggetto se durante la scansione di un messaggio e-mail viene individuata una sezione di codice di un virus noto, incluso nei database anti-virus di Kaspersky Endpoint Security.
   - *Non trovato*. Questo stato viene assegnato a un oggetto se durante la scansione di un messaggio e-mail non vengono rilevati virus o altre minacce.

L'applicazione blocca quindi il messaggio e-mail, visualizza una notifica in relazione all'oggetto rilevato (se specificato nelle impostazioni di notifica) ed esegue l'azione specificata nelle impostazioni di Anti-Virus Posta.

Questo componente interagisce con i client di posta installati nel computer. Per il client di posta Microsoft Office Outlook® è disponibile un'estensione incorporabile che consente di ottimizzare le impostazioni di scansione dei messaggi. L'estensione di Anti-Virus Posta è incorporata nel client di posta Microsoft Office Outlook durante l'installazione di Kaspersky Endpoint Security.

Il funzionamento di Anti-Virus Posta è indicato dall'icona dell'applicazione visualizzata nell'area di notifica della barra delle applicazioni. Quando Anti-Virus Posta sta eseguendo la scansione di un messaggio e-mail, l'icona dell'applicazione diventa  .

## Abilitazione e disabilitazione di Anti-Virus Posta

Per impostazione predefinita, Anti-Virus Posta è abilitato e viene eseguito nella modalità consigliata dagli specialisti di Kaspersky. Se necessario, è possibile disabilitare Anti-Virus Posta.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Anti-Virus Posta nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Protezione**.

   Verrà aperta la sezione **Protezione**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente Anti-Virus Posta.

   Verrà visualizzato un menu per la selezione delle azioni sul componente.
5. Eseguire una delle seguenti operazioni:
   - Per abilitare Anti-Virus Posta, selezionare **Avvia** dal menu.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Anti-Virus Posta**, diventa .
   - Per disabilitare Anti-Virus Posta, selezionare **Interrompi** dal menu.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Anti-Virus Posta**, diventa .

*Per abilitare o disabilitare Anti-Virus Posta dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Posta**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Posta.
3. Eseguire una delle seguenti operazioni:
   - Per abilitare Anti-Virus Posta, selezionare la casella di controllo **Abilita Anti-Virus Posta**.
   - Per disabilitare Anti-Virus Posta, deselezionare la casella di controllo **Abilita Anti-Virus Posta**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione di Anti-Virus Posta

È possibile eseguire le seguenti operazioni per configurare Anti-Virus Posta:

- Modificare il livello di protezione per i messaggi e-mail.

  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 protezione dei messaggi e-mail, è possibile ripristinare in qualsiasi momento le impostazioni consigliate.

- Modificare l'azione eseguita da Kaspersky Endpoint Security quando vengono rilevati messaggi infetti.
- Modificare l'ambito di protezione di Anti-Virus Posta.
- Configurare la scansione dei file compositi allegati ai messaggi e-mail.

  È possibile abilitare o disabilitare la scansione degli allegati dei messaggi, limitare la dimensione massima degli allegati dei messaggio da esaminare e limitare la durata massima della scansione degli allegati dei messaggi.
- Configurare il filtro in base al tipo di allegati dei messaggi e-mail.

  Il filtro degli allegati dei messaggi in base al tipo consente di rinominare o eliminare in modo automatico i file dei tipi specificati.
- Configurare l'analizzatore euristico.

  Per aumentare l'efficacia della protezione, è possibile utilizzare l'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 nei messaggi per cui al momento non sono presenti record nei database di Kaspersky Endpoint Security.
- Configurare la scansione dei messaggi e-mail in Microsoft Office Outlook.

  Per il client di posta Microsoft Office Outlook è disponibile un'estensione incorporabile che consente di configurare facilmente le impostazioni di scansione dei messaggi.

  Se si utilizzano altri client di posta, inclusi Microsoft Outlook Express®, Windows Mail e Mozilla™ Thunderbird™, il componente Anti-Virus Posta esamina il traffico dei protocolli di posta SMTP, POP3, IMAP e NNTP.

  > Se si utilizza il client di posta Mozilla Thunderbird, Anti-Virus Posta non esamina i messaggi trasmessi tramite il protocollo IMAP alla ricerca di virus e altri programmi dannosi se vengono utilizzati filtri per spostare i messaggi dalla cartella **Posta in arrivo**.

## Modifica del livello di protezione per i messaggi e-mail

Anti-Virus Posta applica diversi gruppi di impostazioni per proteggere i messaggi e-mail. Queste impostazioni sono denominate *livelli di protezione dei messaggi e-mail*. Esistono tre livelli di protezione dei messaggi e-mail: **Alto**, **Consigliato** e **Basso**. Il livello di protezione dei file **Consigliato** è considerato l'impostazione ottimale ed è consigliato da Kaspersky.

*Per modificare il livello di protezione dei messaggi e-mail:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Posta**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Posta.
3. Nella sezione **Livello di sicurezza** eseguire una delle seguenti operazioni:

   - Se si desidera applicare uno dei livelli preimpostati di protezione dei messaggi e-mail (**Alto**, **Consigliato** o **Basso**), utilizzare il dispositivo di scorrimento per selezionare il livello desiderato.

- Se si desidera configurare un livello personalizzato di protezione dei messaggi e-mail, fare clic sul pulsante **Impostazioni**, quindi specificare le impostazioni nella finestra **Anti-Virus Posta**.

  Al termine della configurazione di un livello personalizzato di protezione dei messaggi e-mail, il nome del livello di protezione nella sezione **Livello di protezione** viene modificato in **Personalizzato**.

- Se si desidera impostare il livello di protezione dei messaggi e-mail su **Consigliato**, fare clic sul pulsante **Predefinito**.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica dell'azione da eseguire sui messaggi e-mail infetti

*Per modificare l'azione da eseguire sui messaggi e-mail infetti:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Posta**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Posta.

3. Nella sezione **Azione se viene rilevata una minaccia** selezionare l'azione che deve essere eseguita da Kaspersky Endpoint Security quando viene rilevato un messaggio infetto:

   - **Seleziona azione automaticamente**.
   - **Esegui azione: Disinfetta. Elimina se la disinfezione fallisce**.
   - **Esegui azione: Disinfetta**.
   - **Esegui azione: Rimuovi**.
   - **Esegui azione: Blocca**.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica dell'ambito di protezione di Anti-Virus 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 di Anti-Virus Posta includono le impostazioni per l'integrazione di Anti-Virus Posta nei client di posta e il tipo di messaggi e protocolli e-mail per cui il traffico viene esaminato da Anti-Virus 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 di Anti-Virus Posta:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Posta**.

Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Posta.

3. Fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Anti-Virus Posta**.

4. Selezionare la scheda **Generale**.

5. Nella sezione **Ambito di protezione** eseguire una delle seguenti operazioni:

   - Se si desidera che Anti-Virus Posta esamini tutti i messaggi in entrata e in uscita nel computer, selezionare l'opzione **Messaggi in entrata e in uscita**.
   - Se si desidera che Anti-Virus Posta esamini solo i messaggi in entrata nel computer, selezionare l'opzione **Solo messaggi in entrata**.

     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.

6. Nella sezione **Connettività** eseguire una delle seguenti operazioni:

   - Se si desidera che Anti-Virus Posta esamini i messaggi trasferiti tramite i protocolli POP3, SMTP, NNTP e IMAP prima che vengano scaricati nel computer, selezionare la casella di controllo **Traffico POP3 / SMTP / NNTP / IMAP**.

     Se non si desidera che Anti-Virus Posta esamini i messaggi trasferiti tramite i protocolli POP3, SMTP, NNTP e IMAP prima che vengano scaricati nel computer, deselezionare la casella di controllo **Traffico POP3 / SMTP / NNTP / IMAP**. In questo caso, i messaggi vengono esaminati dall'estensione di Anti-Virus Posta incorporata nel client di posta Microsoft Office Outlook dopo la ricezione nel computer dell'utente se la casella di controllo **Componente aggiuntivo: estensione Microsoft Office Outlook** è selezionata.

     Se si utilizza un client di posta diverso da Microsoft Office Outlook, Anti-Virus Posta non esamina i messaggi e-mail trasferiti tramite i protocolli POP3, SMTP, NNTP e IMAP se la casella di controllo **Traffico POP3 / SMTP / NNTP / IMAP** è deselezionata.

   - Se si desidera rendere accessibili le impostazioni di Anti-Virus Posta in 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 **Componente aggiuntivo: estensione Microsoft Office Outlook**.

     Se si desidera bloccare l'accesso alle impostazioni di Anti-Virus Posta in 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 **Componente aggiuntivo: estensione Microsoft Office Outlook**.

     L'estensione di Anti-Virus Posta è incorporata nel client di posta Microsoft Office Outlook durante l'installazione di Kaspersky Endpoint Security.

7. Fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Scansione dei file compositi allegati ai messaggi e-mail

*Per configurare la scansione dei file compositi allegati ai messaggi e-mail:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Posta**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Posta.
3. Fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Anti-Virus Posta**.
4. Selezionare la scheda **Generale**.
5. Esegui le seguenti operazioni nella sezione **Scansione dei file compositi**:

   - Se si desidera che Anti-Virus Posta ignori gli archivi allegati ai messaggi, deselezionare la casella di controllo **Esamina gli archivi allegati**.
   - Se si desidera che Anti-Virus Posta ignori gli allegati dei messaggi di dimensioni superiori a N megabyte, selezionare la casella di controllo **Non esaminare gli archivi di dimensioni superiori a N MB**. Se si seleziona questa casella di controllo, specificare la dimensione massima degli archivi nel campo accanto al nome della casella di controllo.
   - Se si desidera che Anti-Virus Posta esamini gli allegati dei messaggi con un tempo di scansione superiore a N secondi, deselezionare la casella di controllo **Non esaminare gli archivi per più di N sec**.
6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Filtro degli allegati dei messaggi e-mail

I programmi dannosi possono essere distribuiti 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 programma dannoso.

*Per configurare il filtro degli allegati:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Posta**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Posta.
3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Anti-Virus Posta**.

4. Nella finestra **Anti-Virus Posta** selezionare la scheda **Filtro allegati**.

5. Eseguire una delle seguenti operazioni:

   - Se non si desidera che Anti-Virus Posta filtri gli allegati dei messaggi e-mail, selezionare l'opzione **Disattiva il filtro**.

   - Se si desidera che Anti-Virus Posta rinomini gli allegati dei messaggi dei **tipi specificati**, selezionare l'opzione **Rinomina i tipi di allegati specificati**.

Si tenga presente che il formato effettivo di un file potrebbe non corrispondere all'estensione del nome del file.

Se si abilita il filtro degli oggetti allegati ai messaggi e-mail, Anti-Virus 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 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 – estensione per i messaggi e-mail salvati in Microsoft Office Outlook

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. La nuova generazione di metafile di Microsoft Windows. I file EMF non sono supportati nelle versioni a 16 bit di Microsoft Windows.

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

- Se si desidera che Anti-Virus Posta elimini gli allegati dei messaggi dei tipi specificati, selezionare l'opzione **Elimina i tipi di allegati specificati**.

6. Se è stata selezionata l'opzione **Rinomina i tipi di allegati specificati** o l'opzione **Elimina i tipi di allegati specificati** durante il passaggio precedente, selezionare le caselle di controllo accanto ai tipi di file desiderati.

   È possibile modificare l'elenco dei tipi di file utilizzando i pulsanti **Aggiungi**, **Modifica** e **Rimuovi**.

7. Fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Scansione dei messaggi e-mail in Microsoft Office Outlook

Durante l'installazione di Kaspersky Endpoint Security, l'estensione di Anti-Virus Posta è incorporata in Microsoft Office Outlook (di seguito denominato anche Outlook). Tale estensione consente di aprire le impostazioni di Anti-Virus 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 Anti-Virus Posta per Outlook può eseguire la scansione dei messaggi in arrivo e in uscita trasmessi tramite i protocolli POP3, SMTP, NNTP, IMAP e MAPI.

Le impostazioni di Anti-Virus Posta possono essere configurate direttamente in Outlook se la casella di controllo **Componente aggiuntivo: estensione Microsoft Office Outlook** è selezionata nell'interfaccia di Kaspersky Endpoint Security.

In Outlook i messaggi in entrata vengono prima esaminati da Anti-Virus Posta (se la casella di controllo **Traffico POP3 / SMTP / NNTP / IMAP** è selezionata nell'interfaccia di Kaspersky Endpoint Security) e quindi dall'estensione di Anti-Virus Posta per Outlook. Se Anti-Virus Posta rileva un oggetto dannoso in un messaggio, l'evento viene segnalato all'utente.

L'azione selezionata nella finestra di notifica determina il componente che elimina la minaccia nel messaggio: Anti-Virus Posta o l'estensione di Anti-Virus Posta per Outlook.

- Se nella finestra di notifica si seleziona **Disinfetta** o **Rimuovi**, l'eliminazione della minaccia verrà eseguita da Anti-Virus Posta.
- Se nella finestra di notifica si seleziona **Ignora**, la minaccia verrà eliminata dall'estensione di Anti-Virus Posta per Outlook.

I messaggi in uscita vengono prima esaminati dall'estensione di Anti-Virus Posta per Outlook e quindi da Anti-Virus Posta.

## Configurazione della scansione dei messaggi in Outlook

*Per configurare le impostazioni di scansione dei messaggi in Outlook 2007:*

1. Aprire la finestra principale di Outlook 2007.
2. Selezionare **Servizio** → **Impostazioni** nella barra dei menu.

   Verrà visualizzata la finestra **Opzioni**.
3. Nella finestra **Opzioni** selezionare la scheda **Anti-Virus Posta**.

*Per configurare le impostazioni di scansione dei messaggi in Outlook 2010 / 2013:*

1. Aprire la finestra principale di Outlook.

   Selezionare la scheda **File** nell'angolo superiore sinistro.
2. Fare clic sul pulsante **Opzioni**.

   Verrà visualizzata la finestra **Opzioni Outlook**.
3. Selezionare la sezione **Componenti aggiuntivi**.

   Le impostazioni dei plug-in incorporati in Outlook sono visualizzate nella parte destra della finestra.
4. Fare clic sul pulsante **Opzioni componenti aggiuntivi**.

# Configurazione della scansione dei messaggi tramite Kaspersky Security Center

Se viene eseguita la scansione dei messaggi tramite l'estensione di Anti-Virus Posta per Outlook, è consigliabile utilizzare la modalità cache. Per informazioni più dettagliate sulla modalità cache di Exchange e raccomandazioni sul relativo utilizzo, fare riferimento alla Microsoft Knowledge Base: https://technet.microsoft.com/it-it/library/cc179175.aspx.

*Per configurare la modalità operativa dell'estensione di Anti-Virus Posta per Outlook tramite Kaspersky Security Center:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare la scansione dei messaggi.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Protezione anti-virus** selezionare la sottosezione **Anti-Virus Posta**.
7. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.
   Verrà visualizzata la finestra **Anti-Virus Posta**.
8. Nella sezione **Connettività** fare clic sul pulsante **Impostazioni**.
   Verrà visualizzata la finestra **Anti-Virus Posta**.
9. Nella finestra **Anti-Virus Posta**:
   - Selezionare la casella di controllo **Scansione alla ricezione** se si desidera che l'estensione di Anti-Virus Posta per Outlook esamini 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 Anti-Virus Posta per Outlook esamini messaggi in entrata quando l'utente li apre.
   - Selezionare la casella di controllo **Scansione all'invio** se si desidera che l'estensione di Anti-Virus Posta per Outlook esamini messaggi in uscita quando vengono inviati.
10. Nella finestra **Anti-Virus Posta** fare clic su **OK**.
11. Nella finestra **Anti-Virus Posta** fare clic su **OK**.
12. Applicare il criterio.

Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

# Protezione del computer su Internet. Anti-Virus Web

Questo componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

Questa sezione contiene informazioni su Anti-Virus Web e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Anti-Virus Web

Ogni volta che si esegue la connessione a Internet, si espongono le informazioni memorizzate nel computer al rischio di infezione da parte di virus e altro malware. I virus e il malware possono infiltrarsi nel computer durante il download di programmi gratuiti o l'esplorazione di siti Web compromessi da utenti malintenzionati. I worm di rete possono riuscire a penetrare nel computer non appena si stabilisce una connessione a Internet, anche prima di aprire una pagina Web o di scaricare un file.

Anti-Virus Web protegge i dati in entrata e in uscita inviati e ricevuti dal computer tramite i protocolli HTTP e FTP e controlla le URL rispetto all'elenco di indirizzi Web dannosi e di phishing.

Anti-Virus Web intercetta e analizza alla ricerca di virus o altre minacce ogni pagina Web o file a cui accede l'utente o un'applicazione tramite il protocollo HTTP o FTP: Vengono quindi eseguite le seguenti operazioni:

- Se nella pagina o nel file non viene rilevato alcun codice dannoso, l'elemento viene reso immediatamente accessibile all'utente.
- Se un utente accede a una pagina Web o a un file contenente codice dannoso, l'applicazione esegue l'azione specificata nelle impostazioni di Anti-Virus Web.

## Abilitazione e disabilitazione di Anti-Virus Web

Per impostazione predefinita, Anti-Virus Web è abilitato e viene eseguito nella modalità consigliata dagli specialisti di Kaspersky. Se necessario, è possibile disabilitare Anti-Virus Web.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Anti-Virus Web nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Protezione**.

   Verrà aperta la sezione **Protezione**.

4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente Anti-Virus Web.

   Verrà visualizzato un menu per la selezione delle azioni sul componente.

5. Eseguire una delle seguenti operazioni:

   - Per abilitare Anti-Virus Web, selezionare **Avvia** dal menu.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Anti-Virus Web**, diventa .

   - Per disabilitare Anti-Virus Web, selezionare **Interrompi** dal menu.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Anti-Virus Web**, diventa .

*Per abilitare o disabilitare Anti-Virus Web dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Web.

3. Eseguire una delle seguenti operazioni:

   - Per abilitare Anti-Virus Web, selezionare la casella di controllo **Abilita Anti-Virus Web**.
   - Per disabilitare Anti-Virus Web, deselezionare la casella di controllo **Abilita Anti-Virus Web**.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione di Anti-Virus Web

È possibile eseguire le seguenti operazioni per configurare Anti-Virus Web:

- Modificare il livello di protezione del traffico Web.

  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 protezione del traffico Web, è possibile ripristinare in qualsiasi momento le impostazioni consigliate.

- Modificare l'azione eseguita da Kaspersky Endpoint Security quando vengono rilevati oggetti dannosi del traffico Web.

  Se l'analisi di un oggetto HTTP indica che questo contiene codice dannoso, la risposta del componente Anti-Virus Web dipende dall'azione specificata dall'utente.

- Configurare Anti-Virus Web per la verifica delle URL tramite i database di indirizzi Web dannosi e di phishing.

- Configurare l'utilizzo dell'analisi euristica durante la scansione del traffico Web alla ricerca di virus e altri programmi dannosi.

  Per aumentare l'efficacia della protezione, è possibile utilizzare l'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.

- Configurare l'utilizzo dell'analisi euristica durante la scansione delle pagine Web allo scopo di individuare collegamenti di phishing.
- Ottimizzare Anti-Virus Web per la scansione del traffico Web inviato e ricevuto tramite i protocolli HTTP e FTP.
- Creare un elenco di URL attendibili.

  È possibile creare un elenco di URL di cui si ritengono attendibili i contenuti. Anti-Virus Web non analizza le informazioni ricevute dalle URL attendibili alla ricerca di virus o altre minacce. Questa opzione può ad esempio risultare utile nei casi in cui Anti-Virus 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.

## Modifica del livello di protezione del traffico Web

Per proteggere i dati che vengono ricevuti e trasmessi tramite i protocolli HTTP e FTP, Anti-Virus Web applica diversi gruppi di impostazioni. Questi gruppi di impostazioni sono denominati *livelli di protezione del traffico Web*. Esistono tre livelli di protezione del traffico Web preinstallati: **Alto**, **Consigliato** e **Basso**. Il livello di protezione del traffico Web **Consigliato** è considerato l'impostazione ottimale ed è consigliato da Kaspersky.

*Per modificare il livello di protezione del traffico Web:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Web.
3. Nella sezione **Livello di sicurezza** eseguire una delle seguenti operazioni:
   - Se si desidera applicare uno dei livelli preimpostati di protezione del traffico Web (**Alto**, **Consigliato** o **Basso**), utilizzare il dispositivo di scorrimento per selezionare il livello desiderato.
   - Se si desidera configurare un livello personalizzato di protezione del traffico Web, fare clic sul pulsante **Impostazioni**, quindi specificare le impostazioni nella finestra **Anti-Virus Web**.

     Al termine della configurazione di un livello personalizzato di protezione del traffico Web, il nome del livello di protezione nella sezione **Livello di sicurezza** viene modificato in **Personalizzato**.
   - Se si desidera impostare il livello di protezione del traffico Web su **Consigliato**, fare clic sul pulsante **Predefinito**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica dell'azione da eseguire sugli oggetti dannosi del traffico Web

*Per modificare l'azione da eseguire sugli oggetti dannosi del traffico Web:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Web.

3. Nella sezione **Azione se viene rilevata una minaccia** selezionare l'azione eseguita da Kaspersky Endpoint Security se vengono rilevati oggetti dannosi del traffico Web:

   - **Seleziona azione automaticamente**.
   - **Blocca il download**.
   - **Consenti il download**.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Verifica delle URL tramite i database di indirizzi Web dannosi e di phishing con Anti-Virus Web

La scansione dei collegamenti per verificare se sono inclusi nell'elenco degli indirizzi Web di phishing consente di evitare *attacchi di phishing*. Un attacco di phishing può ad esempio presentarsi sotto forma di un messaggio e-mail 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 posta elettronica ma anche da altre origini, come ad esempio i messaggi di ICQ, Anti-Virus Web monitora i tentativi di accesso a un sito Web di phishing a livello di traffico Web e blocca l'accesso a tali siti. Gli elenchi delle URL di phishing sono inclusi nel kit di distribuzione di Kaspersky Endpoint Security.

*Per configurare Anti-Virus Web per la verifica delle URL tramite i database di indirizzi Web dannosi e di phishing:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Web.

3. Fare clic sul pulsante **Impostazioni**.

   Viene visualizzata la finestra **Anti-Virus Web**.

4. Nella finestra **Anti-Virus Web** selezionare la scheda **Generale**.

5. Eseguire le seguenti operazioni:

   - Se si desidera che Anti-Virus Web verifichi le URL tramite i database di indirizzi Web dannosi, nella sezione **Metodi di scansione** selezionare la casella di controllo **Controllare se i collegamenti sono elencati nel database dei collegamenti dannosi**.
   - Se si desidera che Anti-Virus Web verifichi le URL tramite i database di indirizzi Web di phishing, nella sezione **Impostazioni dell'Anti-Phishing** selezionare la casella di controllo **Controllare se i collegamenti sono elencati nel database dei collegamenti di phishing** di phishing.

È anche possibile verificare i collegamenti tramite i database di reputazione di Kaspersky Security Network.

6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Utilizzo dell'analizzatore euristico con Anti-Virus Web

*Per configurare l'utilizzo dell'analisi euristica:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Web.
3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Viene visualizzata la finestra **Anti-Virus Web**.
4. Selezionare la scheda **Generale**.
5. Se si desidera che Anti-Virus Web utilizzi l'analisi euristica per eseguire la scansione del traffico Web alla ricerca di virus e altro malware, nella sezione **Metodi di scansione** selezionare la casella di controllo **Analisi euristica per il rilevamento dei virus** e utilizzare il dispositivo di scorrimento per impostare il livello dell'analisi euristica: **Superficiale**, **Media** o **Approfondita**.
6. Se si desidera che Anti-Virus Web utilizzi l'analisi euristica per eseguire la scansione delle pagine Web alla ricerca di collegamenti di phishing, nella sezione **Impostazioni dell'Anti-Phishing** selezionare la casella di controllo **Analisi euristica per il rilevamento dei collegamenti di phishing**.
7. Fare clic su **OK**.
8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica dell'elenco di URL attendibili

*Per creare un elenco di URL attendibili:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus Web.
3. Fare clic sul pulsante **Impostazioni**.

   Viene visualizzata la finestra **Anti-Virus Web**.

4. Selezionare la scheda **URL attendibili**.

5. Selezionare la casella di controllo **Non esaminare il traffico Web per gli indirizzi Web attendibili**.

6. Creare un elenco di URL o di pagine Web di cui si ritengono attendibili i contenuti. Per creare un elenco:

   a. Fare clic sul pulsante **Aggiungi**.

      Verrà visualizzata la finestra **Indirizzo Web/Maschera indirizzi Web**.

   b. Immettere l'indirizzo del sito Web o della pagina Web oppure una maschera per l'indirizzo di un sito o di una pagina Web.

   c. Fare clic su **OK**.

      Verrà visualizzato un nuovo record nell'elenco delle URL attendibili.

7. Fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Protezione del traffico dei client IM. Anti-Virus IM

Questo componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

Questa sezione contiene informazioni su Anti-Virus IM e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Anti-Virus IM

Anti-Virus IM analizza il traffico dei client di messaggistica istantanea (*client IM*).

Anti-virus IM non esamina i messaggi trasmessi tramite canali criptati.

I messaggi trasmessi tramite i client IM possono contenere i seguenti tipi di minacce per la protezione:

- URL che tentano di scaricare un programma dannoso nel computer
- URL a programmi dannosi e siti Web che utenti malintenzionati utilizzano per attacchi di phishing

  L'obiettivo degli attacchi di phishing è sottrarre i dati personali degli utenti, quali numeri di carte bancarie, dettagli del passaporto, password per sistemi bancari di pagamento e altri servizi online, come siti di social network o account e-mail.

I file possono essere trasmessi tramite i client IM. Quando si tenta di salvare questi file, i file vengono esaminati tramite il componente Anti-Virus File.

Anti-Virus IM intercetta tutti i messaggi inviati o ricevuti dall'utente tramite un client IM e ne esegue la scansione alla ricerca di collegamenti che possono costituire una minaccia per la protezione del computer:

- Se non vengono individuate URL pericolose in un messaggio, questo viene reso disponibile per l'utente.
- Se vengono individuati collegamenti pericolosi in un messaggio, Anti-Virus IM sostituisce il messaggio con informazioni sulla minaccia nella finestra del messaggio del client IM attivo.

## Abilitazione e disabilitazione di Anti-Virus IM

Per impostazione predefinita, Anti-Virus IM è abilitato e viene eseguito nella modalità consigliata dagli specialisti di Kaspersky. Se necessario, è possibile disabilitare Anti-Virus IM.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Anti-Virus IM nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Protezione**.

   Verrà aperta la sezione **Protezione**.
4. Fare clic con il pulsante destro del mouse sulla riga **Anti-Virus IM** per visualizzare il menu di scelta rapida delle azioni del componente.
5. Eseguire una delle seguenti operazioni:

   - Per abilitare Anti-Virus IM, selezionare **Avvia** dal menu di scelta rapida.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Anti-Virus IM**, diventa .
   - Per disabilitare Anti-Virus IM, selezionare **Interrompi** dal menu di scelta rapida.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Anti-Virus IM**, diventa .

*Per abilitare o disabilitare Anti-Virus IM dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus IM**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus IM.
3. Eseguire una delle seguenti operazioni:

   - Per abilitare Anti-Virus IM, selezionare la casella di controllo **Abilita Anti-Virus IM**.
   - Per disabilitare Anti-Virus IM, deselezionare la casella di controllo **Abilita Anti-Virus IM**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione di Anti-Virus IM

È possibile eseguire le seguenti azioni per configurare Anti-Virus IM:

- Configurare l'ambito di protezione.

  È possibile espandere o restringere l'ambito di protezione modificando il tipo di messaggi dei client IM da esaminare.
- Configurare la scansione da parte di Anti-Virus IM dei collegamenti nei messaggi dei client IM rispetto ai database degli indirizzi Web dannosi e di phishing.

## Creazione dell'ambito di protezione di Anti-Virus IM

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. Il tipo di scansione dei messaggi dei client IM, in entrata o in uscita, è una proprietà dell'ambito di protezione di Anti-Virus IM. Per impostazione predefinita, Anti-Virus IM esamina sia i messaggi in entrata che quelli in uscita. È possibile disabilitare la scansione del traffico in uscita.

*Per creare l'ambito di protezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus IM**.
   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus IM.
3. Nella sezione **Ambito di protezione** eseguire una delle seguenti operazioni:
   - Se si desidera che Anti-Virus IM esamini tutti i messaggi in entrata e in uscita dei client IM, selezionare l'opzione **Messaggi in entrata e in uscita**.
   - Se si desidera che Anti-Virus IM esamini solo i messaggi in entrata dei clienti IM, selezionare l'opzione **Solo messaggi in entrata**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Scansione delle URL rispetto ai database delle URL dannose e di phishing con Anti-Virus IM

*Per configurare Anti-Virus IM per la verifica delle URL tramite i database di indirizzi Web dannosi e di phishing:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Anti-Virus IM**.
   Nella parte destra della finestra sono visualizzate le impostazioni del componente Anti-Virus IM.
3. Nella sezione **Metodi di scansione** selezionare i metodi che dovranno essere utilizzati da Anti-Virus IM:
   - Se si desidera verificare i collegamenti nei messaggi dei client IM tramite il database degli indirizzi Web dannosi, selezionare la casella di controllo **Controllare se i collegamenti sono elencati nel database dei collegamenti dannosi**.
   - Se si desidera verificare i collegamenti nei messaggi dei client IM tramite il database degli indirizzi Web di phishing, selezionare la casella di controllo **Controllare se i collegamenti sono elencati nel database dei collegamenti di phishing**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# System Watcher

Questo componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

Questa sezione contiene informazioni su System Watcher e istruzioni su come configurare le impostazioni del componente.

## Informazioni su System Watcher

System Watcher raccoglie dati sulle azioni delle applicazioni nel computer e passa tali informazioni ad altri componenti per garantire una protezione più efficace.

### Behavior Stream Signatures

La tecnologia Behavior Stream Signatures (BSS) contiene sequenze di azioni delle applicazioni classificate come pericolose da Kaspersky Endpoint Security. Se l'attività di un'applicazione corrisponde a uno schema BSS, Kaspersky Endpoint Security esegue l'azione specificata. La funzionalità di Kaspersky Endpoint Security basata sugli schemi BSS assicura una difesa proattiva del computer.

Per impostazione predefinita, se l'attività di un'applicazione corrisponde a uno schema BSS, System Watcher sposta il file eseguibile di tale applicazione in Quarantena.

### Rollback delle azioni eseguite dal malware

In base alle informazioni raccolte da System Watcher, Kaspersky Endpoint Security può eseguire il **rollback delle azioni eseguite dal malware nel sistema operativo** durante l'esecuzione della disinfezione.

Durante il rollback dell'attività del malware nel sistema operativo, Kaspersky Endpoint Security esegue azioni sui seguenti tipi di attività del malware:

- Attività sui file.

  Kaspersky Endpoint Security elimina i file eseguibili creati da un programma dannoso e contenuti in qualsiasi supporto, tranne quelli di rete.

  Kaspersky Endpoint Security elimina i file eseguibili creati da un programma in cui è penetrato un programma dannoso.

  Kaspersky Endpoint Security non ripristina i file modificati o eliminati.

- Attività sul registro di sistema.

  Kaspersky Endpoint Security elimina le partizioni e le chiavi del Registro di sistema create dal malware.

  Kaspersky Endpoint Security non ripristina le partizioni e le chiavi del Registro di sistema modificate o eliminate.

- Attività sul sistema.

  Kaspersky Endpoint Security termina i processi avviati da un programma dannoso.

  Kaspersky Endpoint Security termina i processi in cui è penetrato un programma dannoso.

  Kaspersky Endpoint Security non riprende i processi che sono stati arrestati da un programma dannoso.

- Attività di rete.

  Kaspersky Endpoint Security blocca l'attività di rete dei programmi dannosi.

  Kaspersky Endpoint Security blocca l'attività di rete dei processi in cui è penetrato un programma dannoso.

Il rollback delle azioni del malware può essere avviato da Anti-Virus File 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.

## Abilitazione e disabilitazione di System Watcher

System Watcher è abilitato per impostazione predefinita e viene eseguito nella modalità consigliata da Kaspersky. Se necessario, è possibile disabilitare System Watcher.

Non è consigliabile disabilitare System Watcher a meno che non sia assolutamente necessario, dal momento che questa operazione influisce sulle prestazioni dei componenti della protezione. I componenti di protezione possono richiedere i dati raccolti da System Watcher per identificare con maggiore precisione una minaccia rilevata.

È possibile abilitare o disabilitare System Watcher in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare System Watcher nella scheda **Protezione e controllo** della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Protezione**.

   Verrà aperta la sezione **Protezione**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente System Watcher.

   Verrà visualizzato un menu per la selezione delle azioni sul componente.
5. Eseguire una delle seguenti operazioni:

   - Per abilitare System Watcher, selezionare **Avvia**.

     L'icona di stato del componente , visualizzata a sinistra nella riga **System Watcher**, diventa .
   - Per disabilitare System Watcher, selezionare **Interrompi**.

     L'icona di stato del componente , visualizzata a sinistra nella riga **System Watcher**, diventa .

*Per abilitare o disabilitare System Watcher dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **System Watcher**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente **System Watcher**.
3. Eseguire una delle seguenti operazioni:

   - Per abilitare System Watcher, selezionare la casella di controllo **Abilita System Watcher**.
   - Per disabilitare System Watcher, deselezionare la casella di controllo **Abilita System Watcher**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione di System Watcher

È possibile eseguire le azioni seguenti per configurare System Watcher:

- Abilitare o disabilitare la protezione dagli exploit.
- Scegliere l'azione da eseguire in caso di rilevamento di attività dannose in un programma.
- Abilitare e disabilitare il rollback delle azioni del malware durante la disinfezione.

## Abilitazione e disabilitazione della protezione dagli exploit

*Per abilitare o disabilitare la protezione dagli exploit:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **System Watcher**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente **System Watcher**.
3. Eseguire una delle seguenti operazioni:

   - Selezionare la casella di controllo **Abilita Prevenzione exploit** se si desidera che Kaspersky Endpoint Security monitori i file utilizzati dai programmi vulnerabili in fase di avvio.

     Se Kaspersky Endpoint Security rileva che un file in uso da parte di un programma vulnerabile non è stato avviato dall'utente, procederà in base all'opzione selezionata dall'utente nell'elenco pop-up **Azione se viene rilevata una minaccia**.

   - Selezionare la casella di controllo **Abilita Prevenzione exploit** se si desidera che Kaspersky Endpoint Security monitori i file utilizzati dai programmi vulnerabili in fase di avvio.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Scelta dell'azione da eseguire in caso di rilevamento di attività dannose in un programma

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

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **System Watcher**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente **System Watcher**.
3. Nella sezione **Azione se viene rilevata una minaccia**, nell'elenco a comparsa **Se viene rilevata un'attività malware**, selezionare la seguente azione:

   - **Seleziona azione automaticamente**.
   - **Sposta il file in Quarantena**.
   - **Termina il programma dannoso**.
   - **Ignora**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Abilitazione e disabilitazione del rollback delle azioni del malware durante la disinfezione

*Per abilitare o disabilitare il rollback delle azioni del malware durante la disinfezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **System Watcher**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente **System Watcher**.

3. Eseguire una delle seguenti operazioni:

   - Se si desidera che Kaspersky Endpoint Security esegua il rollback delle azioni eseguite dal malware nel sistema operativo durante l'esecuzione della disinfezione, selezionare la casella di controllo **Esegui il rollback delle azioni del malware durante la disinfezione**.

   - Se si desidera che Kaspersky Endpoint Security ignori le azioni eseguite dal malware nel sistema operativo durante l'esecuzione della disinfezione, deselezionare la casella di controllo **Esegui il rollback delle azioni del malware durante la disinfezione**.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Firewall

Questa sezione contiene informazioni su Firewall e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Firewall

Durante l'utilizzo di reti LAN e di Internet, un computer è esposto a virus, malware e un'ampia varietà di attacchi che sfruttano le vulnerabilità dei sistemi operativi e del software.

Il firewall protegge i dati personali memorizzati nel computer dell'utente, bloccando la maggior parte delle minacce per il sistema operativo mentre il computer è connesso a Internet o a una rete LAN. Firewall rileva tutte le connessioni di rete del computer dell'utente e fornisce un elenco di indirizzi IP, con un'indicazione dello stato della connessione di rete predefinita.

Il componente Firewall filtra tutte le attività di rete in base alle regole di rete. La configurazione delle regole di rete consente di specificare il livello desiderato di protezione del computer, dal blocco dell'accesso a Internet per tutte le applicazioni alla concessione di un accesso senza alcuna limitazione.

## Abilitazione o disabilitazione di Firewall

Per impostazione predefinita, Firewall è abilitato e funziona in modalità ottimale. Se necessario, è possibile disabilitare Firewall.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Firewall nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Protezione**.

   Verrà aperta la sezione **Protezione**.
4. Fare clic con il pulsante destro del mouse sulla riga **Firewall** per aprire il menu di scelta rapida delle azioni di Firewall.
5. Eseguire una delle seguenti operazioni:

   - Per abilitare Firewall, selezionare **Avvia** dal menu di scelta rapida.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Firewall**, diventa .
   - Per disabilitare Firewall, selezionare **Interrompi** nel menu di scelta rapida.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Firewall**, diventa .

*Per abilitare o disabilitare Firewall nella finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare **Firewall**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Firewall.
3. Eseguire una delle seguenti operazioni:
   - Per abilitare Firewall, selezionare la casella di controllo **Abilita Firewall**.
   - Per disabilitare Firewall, selezionare la casella di controllo **Disabilita Firewall**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Informazioni sulle regole di rete

Le *Regole di rete* sono azioni consentite o bloccate eseguite da Firewall se viene rilevato un tentativo di stabilire una connessione di rete.

Firewall fornisce protezione dagli attacchi di rete di diverso tipo a due livelli: a livello di rete e a livello di programma. La protezione a livello di rete viene garantita applicando le regole per i pacchetti di rete. La protezione a livello di programma viene garantita applicando le regole tramite le quali le applicazioni installate possono accedere alle risorse di rete.

In base ai due livelli di protezione di Firewall, è possibile creare:

- *Regole per i pacchetti di rete*. Le regole per i pacchetti di rete applicano restrizioni ai pacchetti di rete, indipendentemente dal programma. Le regole di questo tipo limitano il traffico di rete in entrata e in uscita tramite specifiche porte del protocollo dati selezionato. Firewall specifica determinate regole per i pacchetti rete per impostazione predefinita.
- *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. Questo tipo di regole rende possibile ottimizzare il filtro delle attività di rete, ad esempio quando un determinato tipo di connessione di rete è bloccata per alcune applicazioni ma consentita per altre.

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.

È possibile specificare una priorità di esecuzione per ogni regola per i pacchetti di rete e per ogni regola di rete per le applicazioni.

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.

## Informazioni sulla categoria della connessione di rete

Firewall controlla tutte le connessioni di rete nel computer dell'utente e assegna automaticamente una categoria a ogni connessione di rete rilevata.

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

- **Rete pubblica**. Questa categoria viene assegnata alle reti che non sono protette da alcun programma anti-virus, firewall o filtro, ad esempio le reti degli Internet café. 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**. Questa categoria viene assegnata alle reti in cui gli utenti possono accedere ai file e alle stampanti sul computer in uso, ad esempio in una rete LAN o domestica.

- **Rete attendibile**. Questa categoria viene assegnata alle reti sicure, 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.

## Modifica della categoria della connessione di rete

*Per modificare la categoria della connessione di rete:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Firewall**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Firewall.
3. Fare clic sul pulsante **Reti disponibili**.

   Verrà visualizzata la finestra **Firewall**.
4. Selezionare la connessione di rete di cui si desidera modificare lo stato.
5. Dal menu di scelta rapida selezionare categoria della connessione di rete:
   - **Rete pubblica**.
   - **Rete locale**.
   - **Rete attendibile**.
6. Nella finestra **Firewall** fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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 e modifica di una regola per i pacchetti 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.

*Per creare o modificare una regola per i pacchetti di rete:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare **Firewall**.

3. Fare clic sul pulsante **Regole per i pacchetti di rete**.

4. Verrà visualizzata la finestra **Firewall** nella scheda **Regole per i pacchetti di rete**.

   La scheda mostra un elenco delle regole predefinite per i pacchetti di rete configurate da Firewall.

5. Eseguire una delle seguenti operazioni:

   - Per creare una nuova regola per i pacchetti di rete, fare clic sul pulsante **Aggiungi**.
   - Per modificare una regola per i pacchetti di rete, selezionarla nell'elenco delle regole per i pacchetti di rete, quindi fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Regola di rete**.

6. 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**.

7. Nel campo **Nome** specificare il nome del servizio di rete in uno dei seguenti modi:

   - Fare clic sull'icona a destra del campo **Nome**, quindi selezionare il nome del servizio di rete nell'elenco a discesa.

     L'elenco a discesa include i servizi di rete che definiscono le connessioni di rete utilizzate più di frequente.

   - Immettere manualmente il nome del servizio di rete nel campo **Nome**.

8. Specificare il protocollo di trasferimento dei dati:

   a. Selezionare la casella di controllo **Protocollo**.

   b. Nell'elenco a discesa selezionare il tipo di protocollo per cui monitorare l'attività di rete.

      Firewall consente di monitorare le connessioni di rete che utilizzano i protocolli TCP, UDP, ICMP, ICMPv6, IGMP e GRE.

      Se si seleziona un servizio di rete dall'elenco a discesa **Nome**, la casella di controllo **Protocollo** viene selezionata automaticamente e l'elenco a discesa accanto alla casella di controllo contiene il tipo di protocollo che corrisponde al servizio di rete selezionato. Per impostazione predefinita, la casella di controllo **Protocollo** è deselezionata.

9. Nell'elenco a discesa **Direzione** selezionare la direzione dell'attività di rete monitorata.

   Firewall consente di monitorare le connessioni di rete con le seguenti direzioni:

   - **In entrata (pacchetto)**.
   - **In entrata**.
   - **In entrata / In uscita**
   - **In uscita (pacchetto)**.
   - **In uscita**.

10. Se come protocollo è selezionato ICMP o ICMPv6, è possibile specificare il tipo di pacchetto e il codice ICMP:

    a. Selezionare la casella di controllo **Tipo ICMP**, quindi selezionare il tipo di pacchetto ICMP nell'elenco a discesa.

    b. Selezionare la casella di controllo **Codice ICMP**, quindi selezionare il codice ICMP nell'elenco a discesa.

11. 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:

    a. Digitare le porte del computer remoto nel campo **Porte remote**.

    b. Digitare le porte del computer locale nel campo **Porte locali**.

12. Nella tabella **Schede di rete** specificare le impostazioni delle schede di rete che possono essere utilizzate per inviare o ricevere i pacchetti di rete. A tale scopo, utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina**.

13. Se si desidera limitare il controllo dei pacchetti di rete in base alla relativa durata (TTL), selezionare la casella di controllo **TTL** e nel campo adiacente specificare l'intervallo di valori per la durata dei pacchetti di rete in entrata e/o in uscita.

    Una regola di rete controllerà la trasmissione dei pacchetti di rete la cui durata è inferiore al valore specificato.

    In caso contrario, deselezionare la casella di controllo **TTL**.

14. Specificare gli indirizzi di rete dei computer remoti che possono inviare e/o ricevere i pacchetti di rete. A tale scopo, selezionare uno dei valori seguenti nell'elenco a discesa **Indirizzi remoti**:

    - **Qualsiasi indirizzo**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer remoti con qualsiasi indirizzo IP.
    - **Indirizzi subnet**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer remoti con indirizzi IP associati al tipo di rete selezionato: **Reti attendibili**, **Reti locali** o **Reti pubbliche**.
    - **Indirizzi dall'elenco**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer remoti con indirizzi IP che possono essere specificati nell'elenco sottostante utilizzando i pulsanti **Aggiungi**, **Modifica** ed **Elimina**.

15. Specificare gli indirizzi di rete dei computer in cui è installato Kaspersky Endpoint Security e che possono inviare e/o ricevere i pacchetti di rete. A tale scopo, selezionare uno dei valori seguenti nell'elenco a discesa **Indirizzi locali**:

    - **Qualsiasi indirizzo**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer in cui è installato Kaspersky Endpoint Security e con qualsiasi indirizzo IP.
    - **Indirizzi dall'elenco**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer in cui è installato Kaspersky Endpoint Security e con indirizzi IP che possono essere specificati nell'elenco sottostante utilizzando i pulsanti **Aggiungi**, **Modifica** ed **Elimina**.

    Talvolta non è possibile ottenere un indirizzo locale per le applicazioni che utilizzano i pacchetti di rete. In questo caso, il valore dell'impostazione **Indirizzi locali** viene ignorato.

16. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.

17. Nella finestra **Regola di rete** fare clic su **OK**.

Se si crea una nuova regola di rete per un'applicazione, la regola viene visualizzata nella scheda **Regole per i pacchetti di rete** della finestra **Firewall**. Per impostazione predefinita, la regola per i pacchetti di rete viene posizionata in fondo all'elenco delle regole per i pacchetti di rete.

18. Nella finestra **Firewall** fare clic su **OK**.

19. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Abilitazione o disabilitazione di una regola per i pacchetti di rete

*Per abilitare o disabilitare una regola per i pacchetti di rete:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Firewall**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Firewall.

3. Fare clic sul pulsante **Regole per i pacchetti di rete**.

   Verrà visualizzata la finestra **Firewall** nella scheda **Regole per i pacchetti di rete**.

4. Selezionare la regola per i pacchetti di rete desiderata nell'elenco.

5. Eseguire una delle seguenti operazioni:

   - Per abilitare una regola, selezionare la casella di controllo accanto al nome della regola per i pacchetti di rete.
   - Per disabilitare una regola, deselezionare la casella di controllo accanto al nome della regola per i pacchetti di rete.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Firewall**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Firewall.

3. Fare clic sul pulsante **Regole per i pacchetti di rete**.

   Verrà visualizzata la finestra **Firewall** nella scheda **Regole per i pacchetti di rete**.

4. Nell'elenco selezionare la regola per i pacchetti di rete di cui si desidera modificare l'azione.

5. Nella colonna **Autorizzazione** fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare l'azione da assegnare:

- **Consenti**
- **Blocca**
- **Secondo la regola dell'applicazione**
- **Registra eventi**

6. Nella finestra **Firewall** fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Firewall**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Firewall.
3. Fare clic sul pulsante **Regole per i pacchetti di rete**.

   Verrà visualizzata la finestra **Firewall** nella scheda **Regole per i pacchetti di rete**.
4. Nell'elenco selezionare la regola per i pacchetti di rete di cui si desidera modificare la priorità.
5. Utilizzare i pulsanti **Sposta su** e **Sposta giù** per spostare la regola per i pacchetti di rete nella posizione desiderata nell'elenco delle regole per i pacchetti di rete.
6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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.

Per impostazione predefinita, il componente Firewall applica le regole di rete per un gruppo di applicazioni durante il filtro delle attività di rete di tutte le applicazioni all'interno del gruppo, in modo simile al componente Controllo privilegi applicazioni. 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.

Durante la gestione delle regole di rete delle applicazioni è possibile eseguire le seguenti azioni:

- Creare una nuova regola di rete.

  È possibile creare una nuova regola di rete utilizzata dal componente Firewall per gestire l'attività di rete dell'applicazione o delle applicazioni che appartengono al gruppo di applicazioni selezionato.

- Abilitare o disabilitare una regola di rete.

  Tutte le regole di rete vengono aggiunte all'elenco delle regole di rete per le applicazioni con lo stato *Abilitato*. Se una regola di rete è abilitata, Firewall applica la regola.

  È possibile disabilitare una regola di rete creata manualmente. Se una regola di rete è disabilitata, Firewall non applica temporaneamente la regola.

- Modificare le impostazioni di una regola di rete.

  Dopo avere creato una nuova regola di rete, è possibile modificarne le impostazioni in qualsiasi momento.

- Modificare l'azione eseguita da Firewall per una regola di rete.

  Nell'elenco delle regole di rete è possibile modificare l'azione applicata da Firewall per la regola di rete in caso di rilevamento di un'attività di rete nell'applicazione o nel gruppo di applicazioni.

- Modificare la priorità di una regola di rete.

  È possibile aumentare o ridurre la priorità di una regola di rete personalizzata.

- Eliminare una regola di rete.

  È possibile eliminare una regola di rete personalizzata, in modo da interrompere l'applicazione della regola di rete all'applicazione o al gruppo di applicazioni quando viene rilevata attività di rete e per rimuovere la regola dall'elenco delle regole di rete per le applicazioni.

## Creazione e modifica di una regola di rete per un'applicazione

*Per creare o modificare una regola di rete per un gruppo di applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Firewall**.
3. Fare clic sul pulsante **Regole di rete dell'applicazione**.

   Verrà visualizzata la finestra **Firewall** nella scheda **Regole di controllo 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 visualizzare il menu di scelta rapida, quindi selezionare **Regole applicazione** o **Regole gruppo** a seconda dell'operazione da eseguire.

   Verrà visualizzata la finestra **Regole di controllo applicazioni** o **Regole di controllo gruppo applicazioni**.
6. Nella finestra visualizzata selezionare la scheda **Regole di rete**.
7. Eseguire una delle seguenti operazioni:

   - Per creare una nuova regola di rete, fare clic sul pulsante **Aggiungi**.
   - Per modificare una regola di rete, selezionarla nell'elenco delle regole di rete, quindi fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Regola di rete**.
8. 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**
9. Nel campo **Nome** specificare il nome del servizio di rete in uno dei seguenti modi:

   - Fare clic sull'icona a destra del campo **Nome**, quindi selezionare il nome del servizio di rete nell'elenco a discesa.

     L'elenco a discesa include i servizi di rete che definiscono le connessioni di rete utilizzate più di frequente.
   - Immettere manualmente il nome del servizio di rete nel campo **Nome**.
10. Specificare il protocollo di trasferimento dei dati:

    a. Selezionare la casella di controllo **Protocollo**.

    b. Nell'elenco a discesa selezionare il tipo di protocollo per cui monitorare l'attività di rete.

    Firewall consente di monitorare le connessioni di rete che utilizzano i protocolli TCP, UDP, ICMP, ICMPv6, IGMP e GRE.

    Se si seleziona un servizio di rete dall'elenco a discesa **Nome**, la casella di controllo **Protocollo** viene selezionata automaticamente e l'elenco a discesa accanto alla casella di controllo contiene il tipo di protocollo che corrisponde al servizio di rete selezionato. Per impostazione predefinita, la casella di controllo **Protocollo** è deselezionata.
11. Nell'elenco a discesa **Direzione** selezionare la direzione dell'attività di rete monitorata.

Firewall consente di monitorare le connessioni di rete con le seguenti direzioni:

- **In entrata**.
- **In entrata/In uscita**.
- **In uscita**.

12. Se come protocollo è selezionato ICMP o ICMPv6, è possibile specificare il tipo di pacchetto e il codice ICMP:
    a. Selezionare la casella di controllo **Tipo ICMP**, quindi selezionare il tipo di pacchetto ICMP nell'elenco a discesa.
    b. Selezionare la casella di controllo **Codice ICMP**, quindi selezionare il codice ICMP nell'elenco a discesa.
13. 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:
    a. Digitare le porte del computer remoto nel campo **Porte remote**.
    b. Digitare le porte del computer locale nel campo **Porte locali**.
14. Specificare gli indirizzi di rete dei computer remoti che possono inviare e/o ricevere i pacchetti di rete. A tale scopo, selezionare uno dei valori seguenti nell'elenco a discesa **Indirizzi remoti**:
    - **Qualsiasi indirizzo**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer remoti con qualsiasi indirizzo IP.
    - **Indirizzi subnet**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer remoti con indirizzi IP associati al tipo di rete selezionato: **Reti attendibili**, **Reti locali** o **Reti pubbliche**.
    - **Indirizzi dall'elenco**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer remoti con indirizzi IP che possono essere specificati nell'elenco sottostante utilizzando i pulsanti **Aggiungi**, **Modifica** ed **Elimina**.
15. Specificare gli indirizzi di rete dei computer in cui è installato Kaspersky Endpoint Security e che possono inviare e/o ricevere i pacchetti di rete. A tale scopo, selezionare uno dei valori seguenti nell'elenco a discesa **Indirizzi locali**:
    - **Qualsiasi indirizzo**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer in cui è installato Kaspersky Endpoint Security e con qualsiasi indirizzo IP.
    - **Indirizzi dall'elenco**. La regola di rete controlla i pacchetti di rete inviati e/o ricevuti dai computer in cui è installato Kaspersky Endpoint Security e con indirizzi IP che possono essere specificati nell'elenco sottostante utilizzando i pulsanti **Aggiungi**, **Modifica** ed **Elimina**.

    Talvolta non è possibile ottenere un indirizzo locale per le applicazioni che utilizzano i pacchetti di rete. In questo caso, il valore dell'impostazione **Indirizzi locali** viene ignorato.
16. Se si desidera che le azioni della regola di rete vengano registrate nel rapporto, selezionare la casella di controllo **Registra eventi**.
17. Nella finestra **Regola di rete** fare clic su **OK**.

    Se è stata creata una nuova regola di rete, la regola viene visualizzata nella scheda **Regole di rete**.

18. Fare clic su **OK** nella finestra **Regole di controllo gruppo applicazioni** se la regola è destinata a un gruppo di applicazioni o nella finestra **Regole di controllo applicazioni** se la regola è destinata a un'applicazione.
19. Nella finestra **Firewall** fare clic su **OK**.
20. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Abilitazione e disabilitazione di una regola di rete per un'applicazione

*Per abilitare o disabilitare una regola di rete per un'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Firewall**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Firewall.
3. Fare clic sul pulsante **Regole di rete dell'applicazione**.

   Verrà visualizzata la finestra **Firewall** nella scheda **Regole di controllo applicazioni**.
4. Nell'elenco selezionare l'applicazione o il gruppo di applicazioni per cui si desidera abilitare o disabilitare una regola di rete.
5. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Regole applicazione** o **Regole gruppo** a seconda dell'operazione da eseguire.

   Verrà visualizzata la finestra **Regole di controllo applicazioni** o **Regole di controllo gruppo applicazioni**.
6. Nella finestra visualizzata selezionare la scheda **Regole di rete**.
7. Nell'elenco delle regole di rete per un gruppo di applicazioni selezionare la regola di rete desiderata.
8. Eseguire una delle seguenti operazioni:
   - Per abilitare la regola, selezionare la casella di controllo accanto al nome della regola di rete.
   - Per disabilitare la regola, deselezionare la casella di controllo accanto al nome della regola di rete.

   > Non è possibile disabilitare una regola di rete per un gruppo di applicazioni creata da Firewall per impostazione predefinita.
9. Fare clic su **OK** nella finestra **Regole di controllo gruppo applicazioni** se la regola è destinata a un gruppo di applicazioni o nella finestra **Regole di controllo applicazioni** se la regola è destinata a un'applicazione.
10. Nella finestra **Firewall** fare clic su **OK**.
11. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Firewall**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Firewall.
3. Fare clic sul pulsante **Regole di rete dell'applicazione**.

   Verrà visualizzata la finestra **Firewall** nella scheda **Regole di controllo 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. Nella colonna **Rete** fare clic per visualizzare il menu di scelta rapida, quindi selezionare l'azione da assegnare:
   - **Eredita**
   - **Consenti**
   - **Blocca**
6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

*Per modificare la risposta di Firewall per una regola di rete per un'applicazione o un gruppo di applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare **Firewall**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Firewall.
3. Fare clic sul pulsante **Regole di rete dell'applicazione**.

   Verrà visualizzata la finestra **Firewall** nella scheda **Regole di controllo 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 visualizzare il menu di scelta rapida, quindi selezionare **Regole applicazione** o **Regole gruppo** a seconda dell'operazione da eseguire.

   Verrà visualizzata la finestra **Regole di controllo applicazioni** o **Regole di controllo gruppo applicazioni**.
6. Nella finestra visualizzata 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:
   - **Consenti**

- **Blocca**
- **Registra eventi**

9. Fare clic su **OK** nella finestra **Regole di controllo gruppo applicazioni** se la regola è destinata a un gruppo di applicazioni o nella finestra **Regole di controllo applicazioni** se la regola è destinata a un'applicazione.
10. Nella finestra **Firewall** fare clic su **OK**.
11. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Firewall**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Firewall.
3. Fare clic sul pulsante **Regole di rete dell'applicazione**.

   Verrà visualizzata la finestra **Firewall** nella scheda **Regole di controllo 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 visualizzare il menu di scelta rapida, quindi selezionare **Regole applicazione** o **Regole gruppo** a seconda dell'operazione da eseguire.

   Verrà visualizzata la finestra **Regole di controllo applicazioni** o **Regole di controllo gruppo applicazioni**.
6. Nella finestra visualizzata selezionare la scheda **Regole di rete**.
7. Selezionare la regola di rete di cui si desidera modificare la priorità.
8. Utilizzare i pulsanti **Sposta su** e **Sposta giù** per spostare la regola di rete nella posizione desiderata nell'elenco delle regole di rete.
9. Fare clic su **OK** nella finestra **Regole di controllo gruppo applicazioni** se la regola è destinata a un gruppo di applicazioni o nella finestra **Regole di controllo applicazioni** se la regola è destinata a un'applicazione.
10. Nella finestra **Firewall** fare clic su **OK**.

11. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Monitor di Rete

Questa sezione contiene informazioni su Monitor di Rete e istruzioni per l'avvio di Monitor di Rete.

## Informazioni su 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.

## Avvio di Monitor di Rete

*Per avviare Monitor di Rete:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Protezione**.

   Verrà aperta la sezione **Protezione**.
4. Fare clic con il pulsante destro del mouse sulla riga **Firewall** per aprire il menu di scelta rapida delle operazioni di Firewall.
5. Dal menu di scelta rapida selezionare **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.
   - La scheda **Porte aperte** elenca tutte le porte di rete aperte del computer.
   - 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 Prevenzione attacchi di rete dopo il rilevamento di un tentativo di attacco di rete da parte di tali indirizzi IP.

# Prevenzione attacchi di rete

Questa sezione contiene informazioni su Prevenzione attacchi di rete e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Prevenzione attacchi di rete

Prevenzione attacchi di rete esamina il traffico di rete in entrata alla ricerca di attività tipiche degli attacchi di rete. Quando viene rilevato un tentativo di attacco di rete contro il computer in uso, Kaspersky Endpoint Security blocca l'attività di rete dal computer che ha originato l'attacco. Viene quindi visualizzato un avviso che indica è stato tentato un attacco di rete e mostra informazioni sul computer che ha originato l'attacco.

Il traffico di rete dal computer che ha originato l'attacco viene bloccato per un'ora. È possibile modificare le impostazioni per il blocco di un computer che origina un attacco.

Nei database di Kaspersky Endpoint Security è inclusa una descrizione degli attacchi di rete attualmente conosciuti, nonché dei metodi utilizzati per combatterli. L'elenco degli attacchi di rete che il componente Prevenzione attacchi di rete è in grado di rilevare viene aggiornato durante gli aggiornamenti dei database e dei moduli dell'applicazione.

## Abilitazione e disabilitazione di Prevenzione attacchi di rete

Per impostazione predefinita, Prevenzione attacchi di rete è abilitato e opera in modalità normale. Se necessario, è possibile disabilitare Prevenzione attacchi di rete.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Prevenzione attacchi di rete nella scheda Protezione e controllo della finestra principale dell'applicazione, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Protezione**.

   Verrà aperta la sezione **Protezione**.
4. Fare clic con il pulsante destro del mouse sulla riga **Prevenzione attacchi di rete** per visualizzare il menu di scelta rapida delle azioni di Prevenzione attacchi di rete.
5. Eseguire una delle seguenti operazioni:
   - Per abilitare Prevenzione attacchi di rete, selezionare **Avvia** dal menu di scelta rapida.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Prevenzione attacchi di rete**, diventa .
   - Per disabilitare Prevenzione attacchi di rete, selezionare **Interrompi** dal menu di scelta rapida.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Prevenzione attacchi di rete**, diventa .

*Per abilitare o disabilitare Prevenzione attacchi di rete nella finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Prevenzione attacchi di rete**.

   Le impostazioni di Prevenzione attacchi di rete sono visualizzate nella parte destra della finestra.
3. Eseguire le seguenti operazioni:

   - Per abilitare Prevenzione attacchi di rete, selezionare la casella di controllo **Attiva Prevenzione attacchi di rete**.
   - Per disabilitare Prevenzione attacchi di rete, deselezionare la casella di controllo **Attiva Prevenzione attacchi di rete**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Impostazioni Prevenzione attacchi di rete

È possibile eseguire le seguenti azioni per configurare le impostazioni di Prevenzione attacchi di rete:

- Configurare le impostazioni utilizzate per il blocco di un computer che origina un attacco.
- Generare un elenco di indirizzi per le esclusioni dal blocco.

## Modifica delle impostazioni utilizzate per il blocco di un computer che origina un attacco

*Per modificare le impostazioni per il blocco di un computer che origina un attacco:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Prevenzione attacchi di rete**.

   Le impostazioni di Prevenzione attacchi di rete sono visualizzate nella parte destra della finestra.
3. Selezionare la casella di controllo **Aggiungi il computer che ha originato l'attacco all'elenco di computer bloccati per**.

   Se la casella di controllo è selezionata, quando viene rilevato un tentativo di attacco di rete, Prevenzione attacchi di rete blocca il traffico di rete dal computer che ha originato l'attacco per il periodo di tempo specificato. In questo modo è possibile proteggere automaticamente il computer da ulteriori possibili attacchi di rete dallo stesso indirizzo.

   Se la casella di controllo è deselezionata, quando viene rilevato un tentativo di attacco di rete, Prevenzione attacchi di rete non abilita la protezione automatica da ulteriori possibili attacchi di rete dallo stesso indirizzo.
4. Modificare il periodo di tempo per cui il computer che originato l'attacco viene bloccato nel campo accanto alla casella di controllo **Aggiungi il computer che ha originato l'attacco all'elenco di computer bloccati per**.

5. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione degli indirizzi delle esclusioni dal blocco

*Per configurare gli indirizzi delle esclusioni dal blocco:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Prevenzione attacchi di rete**.

   Le impostazioni di Prevenzione attacchi di rete sono visualizzate nella parte destra della finestra.
3. Fare clic sul pulsante **Esclusioni**.

   Verrà visualizzata la finestra **Esclusioni**.
4. Eseguire una delle seguenti operazioni:

   - Per aggiungere un nuovo indirizzo IP, fare clic sul pulsante **Aggiungi**.
   - Per modificare un indirizzo IP aggiunto in precedenza, selezionarlo nell'elenco di indirizzi e fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Indirizzo IP**.
5. Immettere l'Indirizzo IP del computer da cui non devono essere bloccati gli attacchi di rete.
6. Nella finestra **Indirizzo IP** fare clic su **OK**.
7. Nella finestra **Esclusioni** fare clic su **OK**.
8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Prevenzione Attacchi BadUSB

Questa sezione contiene informazioni sul componente Prevenzione unità USB dannose.

## Informazioni su Prevenzione unità USB dannose

Alcuni virus modificano il firmware dei dispositivi USB per indurre il sistema operativo a rilevare il dispositivo USB come una tastiera.

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 dall'applicazione come una tastiera, l'applicazione richiede all'utente di immettere un codice numerico generato dall'applicazione da questa tastiera o utilizzando Tastiera sullo schermo (se disponibile). Questa procedura è denominata autorizzazione della tastiera. L'applicazione consente l'utilizzo di una tastiera autorizzata e blocca una tastiera che non è stata autorizzata.

Prevenzione unità USB dannose viene eseguito in background non appena il componente viene installato. Se l'applicazione non è sottoposta a un criterio di Kaspersky Security Center, è possibile abilitare o disabilitare Prevenzione unità USB dannose sospendendo e riprendendo temporaneamente la protezione e il controllo del computer.

## Installazione del componente Prevenzione Attacchi BadUSB

Se è stata selezionata l'installazione di base o standard durante l'installazione di Kaspersky Endpoint Security, il componente Prevenzione Attacchi BadUSB non sarà disponibile. Per installarlo, è necessario modificare il set di componenti dell'applicazione.

*Per installare il componente Prevenzione Attacchi BadUSB:*

1. Dal menu **Start** selezionare **Applicazioni** → **Kaspersky Endpoint Security 10 for Windows** → **Modifica, Ripristina o Rimuovi**.

   Verrà avviata l'Installazione guidata.

2. Nella finestra **Modifica, ripristino o rimozione dell'applicazione** dell'Installazione guidata dell'applicazione fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Installazione personalizzata** dell'Installazione guidata dell'applicazione.

3. Nel menu di scelta rapida dell'icona accanto al nome del componente **Prevenzione unità USB dannose** selezionare l'opzione **La funzionalità verrà installata sul disco rigido locale**.

4. Fare clic sul pulsante **Avanti**.

5. Attenersi alle istruzioni dell'Installazione guidata.

## Abilitazione e disabilitazione di Prevenzione Attacchi BadUSB

*Per abilitare o disabilitare Prevenzione unità USB dannose:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Prevenzione unità USB dannose**.

   Le impostazioni di Prevenzione unità USB dannose sono visualizzate nella parte destra della finestra.
3. Eseguire una delle seguenti operazioni:

   - Per abilitare Prevenzione unità USB dannose, selezionare la casella di controllo **Abilita Prevenzione unità USB dannose**.
   - Per disabilitare Prevenzione unità USB dannose, deselezionare la casella di controllo **Abilita Prevenzione unità USB dannose**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Autorizzazione o divieto dell'utilizzo di Tastiera sullo schermo per l'autorizzazione

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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Protezione anti-virus**, selezionare la sottosezione **Prevenzione unità USB dannose**.

   Le impostazioni del componente vengono visualizzate nella parte destra della finestra.
3. Eseguire una delle seguenti operazioni:

   - Selezionare la casella di controllo **Impedisci di utilizzare Tastiera sullo schermo per l'autorizzazione** per impedire l'utilizzo di Tastiera sullo schermo per l'autorizzazione.
   - Deselezionare la casella di controllo **Impedisci di utilizzare Tastiera sullo schermo per l'autorizzazione** per consentire l'utilizzo di Tastiera sullo schermo per l'autorizzazione.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Autorizzazione tastiera

I dispositivi USB identificati dal sistema operativo come tastiere e connessi al computer prima dell'installazione del componente Prevenzione unità USB dannose sono considerati autorizzati dopo l'installazione del componente.

L'applicazione richiede l'autorizzazione del dispositivo USB connesso che è stato identificato dal sistema operativo come una tastiera solo se la richiesta dell'autorizzazione della tastiera USB è abilitata. L'utente non può utilizzare una tastiera non autorizzata finché non viene autorizzata.

Se la richiesta dell'autorizzazione della tastiera USB è disabilitata, l'utente può utilizzare tutte le tastiere connesse. Subito dopo l'abilitazione della richiesta dell'autorizzazione della tastiera USB, l'applicazione visualizza una richiesta di autorizzazione per ogni tastiera non autorizzata connessa.

*Per autorizzare una tastiera:*

1. Con l'autorizzazione della tastiera USB abilitata, collegare la tastiera a una porta USB.

   Verrà visualizzata la finestra **Autorizzazione tastiera <nome della tastiera>**, con i dettagli della tastiera connessa e un codice numerico per la relativa autorizzazione.

2. Immettere il codice numerico generato in modo casuale nella finestra di autorizzazione dalla tastiera connessa o da Tastiera sullo schermo (se disponibile).

3. Fare clic su **OK**.

   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 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. Sono disponibili tre tentativi per l'immissione del codice numerico. Se il codice numerico viene immesso in modo errato per tre volte consecutive o la finestra **Autorizzazione tastiera <nome della tastiera>** viene chiusa, l'applicazione blocca l'input da questa tastiera. Quando la tastiera viene connessa di nuovo o il sistema operativo viene riavviato, l'applicazione richiede all'utente di eseguire nuovamente l'autorizzazione della tastiera.

# Controllo avvio applicazioni

Questa sezione contiene informazioni su Controllo avvio applicazioni e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Controllo avvio applicazioni

Il componente Controllo avvio applicazioni monitora i tentativi dell'utente di avviare le applicazioni e gestisce l'avvio delle applicazioni tramite le *regole di Controllo avvio applicazioni*.

L'avvio delle applicazioni le cui impostazioni non corrispondono ad alcuna regola di Controllo avvio applicazioni è gestito dalla modalità operativa selezionata del componente. La *modalità Blacklist* è selezionata per impostazione predefinita. Questa modalità consente l'avvio di tutte le applicazioni da parte di qualsiasi utente.

Tutti i tentativi dell'utente di avviare applicazioni vengono registrati nei rapporti.

## Abilitazione e disabilitazione di Controllo avvio applicazioni

Nonostante Controllo avvio applicazioni sia disabilitato per impostazione predefinita, è possibile abilitarlo se necessario.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Controllo avvio applicazioni nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Controllo endpoint**.

   Verrà aperta la sezione **Controllo endpoint**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente Controllo avvio applicazioni.

   Verrà visualizzato un menu per la selezione delle azioni sul componente.
5. Eseguire una delle seguenti operazioni:

   - Per abilitare il componente Controllo avvio applicazioni, selezionare **Avvia** dal menu.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Controllo avvio applicazioni**, diventa .
   - Per disabilitare il componente Controllo avvio applicazioni, selezionare **Interrompi** dal menu.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Controllo avvio applicazioni**, diventa .

*Per abilitare o disabilitare Controllo avvio applicazioni dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo avvio applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo avvio applicazioni.
3. Eseguire una delle seguenti operazioni:

   - Per abilitare Controllo avvio applicazioni, selezionare la casella di controllo **Abilita Controllo avvio applicazioni**.
   - Per disabilitare Controllo avvio applicazioni, deselezionare la casella di controllo **Abilita Controllo avvio applicazioni**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Limitazioni delle funzionalità di Controllo avvio applicazioni

L'esecuzione del componente Controllo avvio applicazioni è limitata nei seguenti casi:

- Quando si esegue l'upgrade della versione dell'applicazione, l'importazione delle impostazioni del componente Controllo avvio applicazioni non è supportata.

  Per ripristinare le funzionalità di Controllo avvio applicazione, è necessario riconfigurare le impostazioni del componente.
- 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. Se i database locali non contengono informazioni sull'applicazione, l'applicazione non verrà categorizzata in un gruppo di attendibilità.

  La categorizzazione delle applicazioni può variare a seconda del fatto che sia disponibile o meno la connessione con i server 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 avvio applicazioni, il componente non bloccherà uno script avviato da questo 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:

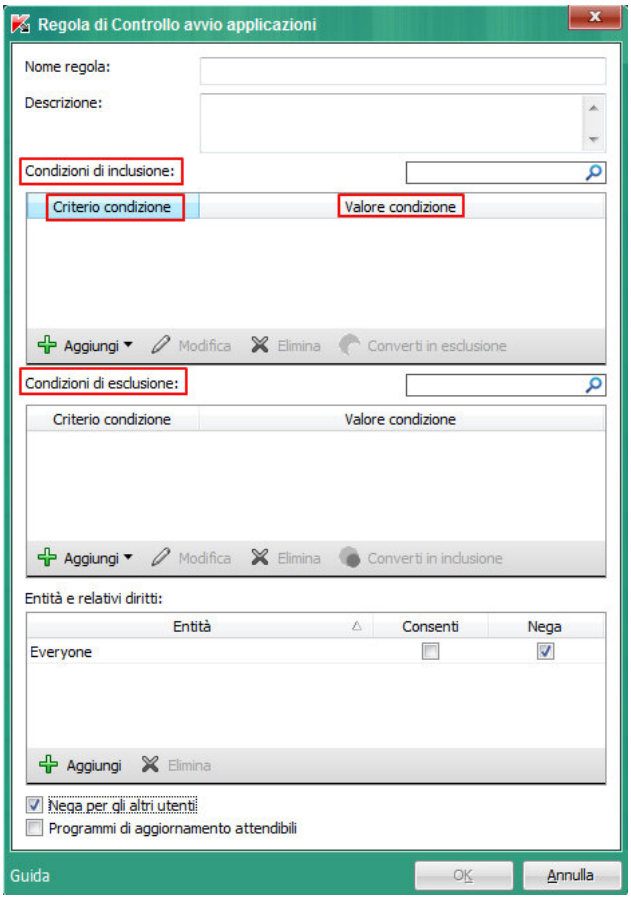
- { cCmdLineParser::itCmd, _T("%ComSpec%") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
- { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

## Informazioni sulle regole di Controllo avvio applicazioni

Kaspersky Endpoint Security controlla l'avvio delle applicazioni da parte degli utenti tramite regole. Una regola di Controllo avvio applicazioni specifica le condizioni di attivazione e l'azione eseguita da Controllo avvio applicazioni quando viene avviata la regola (autorizzazione o blocco dell'avvio delle applicazioni da parte degli utenti).

## Condizioni di attivazione della regola

Una condizione di attivazione della regola presenta la seguente corrispondenza: "tipo di condizione - criterio della condizione - valore della condizione" (vedere la figura seguente). In base alle condizioni di attivazione della regola, Kaspersky Endpoint Security applica (o non applica) una regola a un'applicazione.




Regola di Controllo avvio applicazioni. Parametri della condizione di attivazione della regola

Le regole utilizzano condizioni di inclusione ed esclusione:

- *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, entità 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 avvio applicazioni esegue l'azione specificata nella regola. Se i parametri dell'applicazione corrispondono ai valori dei criteri specificati nella condizione di esclusione, Controllo avvio applicazioni non controlla l'avvio dell'applicazione.

### Decisioni prese dal componente Controllo avvio applicazioni all'attivazione di una regola

Quando viene attivata una regola, Controllo avvio 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 specificate una regola di autorizzazione di Controllo avvio applicazioni per un gruppo di utenti e una regola di blocco di Controllo avvio 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 avvio applicazioni possono disporre di tre valori per lo stato operativo:

- **Attivato.**

  Questo stato indica che la regola è abilitata.

- **Disattivato.**

  Questo stato indica che la regola è disabilitata.

### Regole predefinite di Controllo avvio applicazioni

Per impostazione predefinita, Controllo avvio applicazioni opera in modalità Blacklist. Questo componente consente l'avvio di tutte le applicazioni da parte di tutti gli utenti. Quando un utente tenta di avviare un'applicazione che è bloccata dalle regole di Controllo avvio applicazioni, Kaspersky Endpoint Security blocca l'avvio dell'applicazione (se è selezionata l'azione **Blocca**) o salva le informazioni sull'avvio dell'applicazione in un rapporto (se è selezionata l'azione **Notifica**).

## Gestione delle regole di Controllo avvio applicazioni

Per le regole di Controllo avvio applicazioni è possibile eseguire le seguenti azioni:

- Aggiungere una nuova regola
- Creare o modificare le condizioni di attivazione di una regola
- Modificare lo stato di una regola

  Una regola di Controllo avvio applicazioni può essere abilitata (la casella di controllo accanto alla regola è selezionata) o disabilitata (la casella di controllo accanto alla regola è deselezionata). Una regola di Controllo avvio applicazioni è abilitata per impostazione predefinita dopo la creazione.
- Elimina la regola

## Aggiunta e modifica di una regola di Controllo avvio applicazioni

*Per aggiungere o modificare una regola di Controllo avvio applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo avvio applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo avvio applicazioni.
3. Selezionare **Abilita Controllo avvio applicazioni** per rendere le impostazioni dei componenti disponibili alla modifica.
4. 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 avvio applicazioni**.
5. Specificare o modificare le impostazioni della regola:
   a. Nel campo **Nome regola** immettere o modificare il nome della regola.
   b. Nella tabella **Condizioni di inclusione** creare o modificare l'elenco delle condizioni di inclusione per l'attivazione di una regola facendo clic sui pulsanti **Aggiungi**, **Modifica**, **Elimina** e **Converti in esclusione**.
   c. Nella tabella **Condizioni di esclusione** creare o modificare l'elenco delle condizioni di esclusione per l'attivazione di una regola facendo clic sui pulsanti **Aggiungi**, **Modifica**, **Elimina** e **Converti in inclusione**.
   d. Se necessario, modificare il tipo di condizione di attivazione della regola:
      - Per modificare il tipo di condizione da una condizione di inclusione a una condizione di esclusione, selezionare una condizione nella tabella **Condizioni di inclusione**, quindi fare clic sul pulsante **Converti in esclusione**.
      - Per modificare il tipo di condizione da una condizione di esclusione a una condizione di inclusione, selezionare una condizione nella tabella **Condizioni di esclusione**, quindi fare clic sul pulsante **Converti in inclusione**.

e. 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 **Entità e relativi diritti**.

Verrà visualizzata la finestra **Seleziona utenti e gruppi** di Microsoft Windows. In questa finestra è possibile selezionare utenti e/o gruppi di utenti.

Per impostazione predefinita, il valore **Everyone** 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.

f. Nella tabella **Entità e relativi diritti** selezionare le caselle di controllo **Consenti** o **Blocca** accanto agli utenti e/o ai gruppi di utenti per specificare i diritti per l'avvio delle applicazioni.

La casella di controllo selezionata per impostazione predefinita dipende dalla modalità operativa di Controllo avvio applicazioni.

g. Selezionare la casella di controllo **Nega per gli altri utenti** se si desidera impedire a tutti gli utenti che non compaiono nella colonna **Entità** e che non fanno parte del gruppo di utenti specificati nella colonna **Entità** di avviare le applicazioni che corrispondono alle condizioni di attivazione della regola.

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 **Entità e relativi diritti** e che non appartengono ai gruppi di utenti specificati nella tabella **Entità e relativi diritti**.

h. Se si desidera che Kaspersky Endpoint Security consideri le applicazioni che corrispondono alle condizioni di attivazione della regola come programmi di aggiornamento attendibili e consenta loro di avviare altre applicazioni per cui non sono definite regole di Controllo avvio applicazioni, selezionare la casella di controllo **Programmi di aggiornamento attendibili**.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Aggiunta di una condizione di attivazione a una regola di Controllo avvio applicazioni

*Per aggiungere una nuova condizione di attivazione a una regola di Controllo avvio applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo avvio applicazioni**.

Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo avvio applicazioni.

3. Selezionare **Abilita Controllo avvio applicazioni** per rendere le impostazioni dei componenti disponibili alla modifica.

4. Eseguire una delle seguenti operazioni:

- Se si desidera creare una nuova regola e aggiungervi una condizione di attivazione, fare clic sul pulsante **Aggiungi**.

- Se si desidera aggiungere una condizione di attivazione a una regola esistente, selezionare la regola dell'elenco di regole e fare clic sul pulsante **Modifica**.

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

5. Nella tabella **Condizioni di inclusione** o **Condizioni di esclusione** fare clic sul pulsante **Aggiungi**.

È possibile utilizzare l'elenco a discesa del pulsante **Aggiungi** per aggiungere varie condizioni di attivazione alla regola (vedere le istruzioni seguenti).

*Per aggiungere una condizione di attivazione di una regola in base alle proprietà dei file nella cartella specificata:*

1. Nell'elenco a discesa del pulsante **Aggiungi** selezionare **Condizioni dalle proprietà dei file nella cartella specificata**.

   Verrà visualizzata la finestra standard di Microsoft Windows **Seleziona la cartella**.

2. Nella finestra **Seleziona la cartella** selezionare una cartella che contiene i file eseguibili delle applicazioni di cui si desidera utilizzare le proprietà come base per una o più condizioni di attivazione di una regola.

3. Fare clic su **OK**.

   Verrà visualizzata la finestra **Aggiungi condizione**.

4. Nell'elenco a discesa **Mostra criterio** selezionare il criterio in base al quale creare una o più condizioni di attivazione della regola: **Codice hash file**, **Certificato**, **Categoria KL**, **Metadati** o **Percorso cartella**.

   Kaspersky Endpoint Security non supporta un codice 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.

5. Se è stato selezionato **Metadati** nell'elenco a discesa **Mostra criterio**, selezionare le caselle di controllo accanto alle proprietà del file eseguibile che si desidera utilizzare nella condizione per l'attivazione della regola: **Nome del file**, **Versione file**, **Nome applicazione**, **Versione dell'applicazione** e **Produttore**.

   Se non è selezionata alcuna delle proprietà specificate, la regola non può essere salvata.

6. Se è stato selezionato **Certificato** nell'elenco a discesa **Mostra criterio**, selezionare le caselle di controllo accanto alle impostazioni che si desidera utilizzare nella condizione di attivazione della regola: **Autorità di emissione**, **Entità** e **Identificazione personale**.

   Se non è selezionata alcuna delle impostazioni specificate, la regola non può essere salvata.

   Non è consigliabile utilizzare solo i criteri **Autorità di emissione** ed **Entità** come condizioni di attivazione della regola. L'utilizzo di questi criteri non è affidabile.

7. Selezionare le caselle di controllo accanto ai nomi dei file eseguibili delle applicazioni di cui si desidera includere le proprietà nelle condizioni di attivazione della regola.

8. Fare clic sul pulsante **Avanti**.

   Verrà visualizzato un elenco di condizioni formulate di attivazione della regola.

9. Nell'elenco delle condizioni di attivazione della regola create selezionare le caselle di controllo accanto alle condizioni di attivazione della regola che si desidera aggiungere alla regola di Controllo avvio applicazioni.

10. Fare clic sul pulsante **Termina**.

*Per aggiungere una condizione di attivazione di una regola in base alle proprietà delle applicazioni avviate nel computer:*

1. Nell'elenco a discesa del pulsante **Aggiungi** selezionare **Condizioni dalle proprietà delle applicazioni avviate**.
2. Nella finestra **Aggiungi condizione**, nell'elenco a discesa **Mostra criterio**, selezionare il criterio in base al quale creare una o più condizioni di attivazione della regola: **Codice hash file**, **Certificato**, **Categoria KL**, **Metadati** o **Percorso cartella**.
3. Se è stato selezionato **Metadati** nell'elenco a discesa **Mostra criterio**, selezionare le caselle di controllo accanto alle proprietà del file eseguibile che si desidera utilizzare nella condizione per l'attivazione della regola: **Nome del file**, **Versione file**, **Nome applicazione**, **Versione dell'applicazione** e **Produttore**.

   Se non è selezionata alcuna delle proprietà specificate, la regola non può essere salvata.
4. Se è stato selezionato **Certificato** nell'elenco a discesa **Mostra criterio**, selezionare le caselle di controllo accanto alle impostazioni che si desidera utilizzare nella condizione di attivazione della regola: **Autorità di emissione**, **Entità** e **Identificazione personale**.

   Se non è selezionata alcuna delle impostazioni specificate, la regola non può essere salvata.

   > Non è consigliabile utilizzare solo i criteri **Autorità di emissione** ed **Entità** come condizioni di attivazione della regola. L'utilizzo di questi criteri non è affidabile.
5. Selezionare le caselle di controllo accanto ai nomi dei file eseguibili delle applicazioni di cui si desidera includere le proprietà nelle condizioni di attivazione della regola.
6. Fare clic sul pulsante **Avanti**.

   Verrà visualizzato un elenco di condizioni formulate di attivazione della regola.
7. Nell'elenco delle condizioni di attivazione della regola create selezionare le caselle di controllo accanto alle condizioni di attivazione della regola che si desidera aggiungere alla regola di Controllo avvio applicazioni.
8. Fare clic sul pulsante **Termina**.

*Per aggiungere una condizione di attivazione di una regola in base a una categoria KL:*

1. Nell'elenco a discesa sotto il pulsante **Aggiungi** selezionare **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 "Applicazioni Office" include le applicazioni della suite Microsoft Office, Adobe® Acrobat® e altre ancora.
2. Nella finestra **Condizioni "Categoria KL"** selezionare le caselle di controllo accanto ai nomi delle categorie KL da utilizzare per creare le condizioni di attivazione della regola.
3. Fare clic su **OK**.

*Per aggiungere una condizione personalizzata di attivazione di una regola:*

1. Nell'elenco a discesa del pulsante **Aggiungi** selezionare **Condizione personalizzata**.
2. Nella finestra **Condizione personalizzata** fare clic sul pulsante **Seleziona** e specificare il percorso del file eseguibile dell'applicazione.
3. Selezionare il criterio in base al quale creare una condizione di attivazione della regola: **Codice hash file**, **Certificato**, **Metadati** o **Percorso del file o della cartella**.

Se si utilizzano collegamenti simbolici nel campo **Percorso del file o della cartella**, è consigliabile risolvere i collegamenti simbolici per il corretto funzionamento della regola di Controllo avvio applicazioni. A tale scopo, fare clic sul pulsante **Risolvi collegamento simbolico**.

4. Se necessario, configurare le impostazioni del criterio selezionato.
5. Fare clic su **OK**.

*Per aggiungere una condizione di attivazione di una regola in base alle informazioni sull'unità che contiene il file eseguibile di un'applicazione:*

1. Nell'elenco a discesa del pulsante **Aggiungi** selezionare **Condizione dall'unità del file**.
2. Nella finestra **Condizione dall'unità del file**, nell'elenco a discesa **Unità**, selezionare il tipo di unità da cui l'avvio delle applicazioni sarà utilizzato come condizione di attivazione della regola.
3. Fare clic su **OK**.

## Modifica dello stato di una regola di Controllo avvio applicazioni

*Per modificare lo stato di una regola di Controllo avvio applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo avvio applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo avvio applicazioni.
3. Selezionare **Abilita Controllo avvio applicazioni** per rendere le impostazioni dei componenti disponibili alla modifica.
4. Selezionare la regola di cui si desidera modificare lo stato.
5. Nella colonna **Stato** eseguire le seguenti operazioni:
   - Se si desidera abilitare l'utilizzo di una regola, selezionare la casella di controllo accanto alla regola.
   - Se si desidera disabilitare l'utilizzo di una regola, deselezionare la casella di controllo accanto alla regola.
6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Verifica delle regole di Controllo avvio applicazioni

Per garantire che le regole di Controllo avvio applicazioni non blocchino le applicazioni necessarie per le attività lavorative, è consigliabile impostare le nuove regole create in modalità di test e analizzarne l'esecuzione.

L'analisi dell'esecuzione delle regole di Controllo avvio applicazioni richiede la verifica degli eventi di Controllo avvio applicazioni segnalati a Kaspersky Security Center. Se viene consentito l'avvio di tutte le applicazioni necessarie per il lavoro nel computer dell'utente, le regole sono state create correttamente. In caso contrario, è consigliabile controllare le impostazioni delle regole create.

La modalità di test per le regole di Controllo avvio applicazioni è disabilitata per impostazione predefinita.

*Per verificare le regole di Controllo avvio applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo avvio applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo avvio applicazioni.
3. Selezionare **Abilita Controllo avvio applicazioni** per rendere le impostazioni dei componenti disponibili alla modifica.
4. Nell'elenco a discesa **Modalità Controllo avvio applicazioni** selezionare uno dei seguenti elementi:

   - **Blacklist**, se si desidera consentire l'avvio di tutte le applicazioni tranne quelle specificate nelle regole di blocco.
   - **Whitelist**, se si desidera bloccare l'avvio di tutte le applicazioni tranne quelle specificate nelle regole di autorizzazione.
5. Nell'elenco a discesa **Azione** selezionare **Notifica**.
6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

Kaspersky Endpoint Security non bloccherà le applicazioni il cui avvio non è consentito dalle regole di Controllo avvio applicazioni, ma invierà notifiche sul relativo avvio all'Administration Server.

## Modifica dei modelli dei messaggi di Controllo avvio applicazioni

Quando un utente tenta di avviare un'applicazione bloccata da una regola di Controllo avvio 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo avvio applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo avvio applicazioni.
3. Selezionare **Abilita Controllo avvio applicazioni** per rendere le impostazioni dei componenti disponibili alla modifica.
4. Fare clic sul pulsante **Modelli**.

Verrà visualizzata la finestra **Modelli di messaggi**.

5. Eseguire una delle seguenti operazioni:

   - Per modificare il modello del messaggio visualizzato quando viene bloccato l'avvio di un'applicazione, selezionare la scheda **Blocco**.

   - Per modificare il modello del messaggio inviato all'amministratore della rete LAN, selezionare la scheda **Messaggio all'amministratore**.

6. Modificare il modello del messaggio visualizzato quando viene bloccato l'avvio di un'applicazione o del messaggio inviato all'amministratore. A tale scopo, utilizzare i pulsanti **Predefinito** e **Variabile**.

7. Fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Informazioni sulle modalità di esecuzione di Controllo avvio applicazioni

Il componente Controllo avvio applicazioni opera in due modalità:

- **Blacklist**. In questa modalità, Controllo avvio applicazioni consente a tutti gli utenti di avviare tutte le applicazioni, tranne quelle specificate nelle regole di blocco di Controllo avvio applicazioni.

  Questa modalità di Controllo avvio applicazioni è abilitata per impostazione predefinita.

- **Whitelist**. In questa modalità, Controllo avvio applicazioni impedisce a tutti gli utenti di avviare qualsiasi applicazione, tranne quelle specificate nelle regole di autorizzazione di Controllo avvio applicazioni.

  Se le regole di autorizzazione di Controllo avvio applicazioni sono completamente configurate, il componente blocca l'avvio di tutte le nuove applicazioni che non sono state verificate dall'amministratore della rete LAN, mentre consente l'utilizzo del sistema operativo e delle applicazioni attendibili utilizzate dagli utenti per il proprio lavoro.

In ogni modalità è possibile eseguire due azioni sulle applicazioni in esecuzione: Kaspersky Endpoint Security può bloccare l'avvio delle applicazioni o inviare una notifica all'utente sull'avvio di un'applicazione che corrisponde alle condizioni delle regole di Controllo avvio applicazioni.

Controllo avvio applicazioni può essere configurato per operare in queste modalità sia nell'interfaccia locale di Kaspersky Endpoint Security che utilizzando Kaspersky Security Center.

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

- Creazione delle categorie di applicazioni.

  Le regole di Controllo avvio applicazioni create in Kaspersky Security Center Administration Console sono basate su categorie di applicazioni personalizzate e non sulle condizioni di inclusione e di esclusione, come nel caso dell'interfaccia locale di Kaspersky Endpoint Security.

- Raccolta delle informazioni sulle applicazioni installate nei computer della rete LAN.

Per questo motivo è consigliabile utilizzare Kaspersky Security Center per configurare l'esecuzione del componente Controllo avvio applicazioni.

# Selezione della modalità di Controllo avvio applicazioni

*Per selezionare la modalità di Controllo avvio applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo avvio applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo avvio applicazioni.

3. Selezionare **Abilita Controllo avvio applicazioni** per rendere le impostazioni dei componenti disponibili alla modifica.

4. Nell'elenco a discesa **Modalità Controllo avvio applicazioni** selezionare una delle seguenti opzioni:

   - **Blacklist**, se si desidera consentire l'avvio di tutte le applicazioni tranne quelle specificate nelle regole di blocco.

   - **Whitelist**, se si desidera bloccare l'avvio di tutte le applicazioni tranne quelle specificate nelle regole di autorizzazione.

     Quando è selezionata questa modalità, per impostazione predefinita vengono create due regole di Controllo avvio applicazioni: **Immagine gold** e **Programmi di aggiornamento attendibili**. È impossibile eliminare queste regole. Le impostazioni di queste regole non possono essere modificate. È possibile abilitare o disabilitare queste regole selezionando o deselezionando la casella di controllo della regola corrispondente. 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 utilizzare di nuovo queste regole, è sufficiente selezionare la modalità desiderata nell'elenco a discesa **Modalità Controllo avvio applicazioni**.

5. Nell'elenco a discesa **Azione** selezionare l'azione che deve essere eseguita dal componente quando un utente tenta di avviare un'applicazione bloccata dalle regole di Controllo avvio applicazioni.

6. Selezionare la casella di controllo **Controlla DLL e moduli** 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.

   Se la casella di controllo è selezionata, i moduli DLL e i driver vengono monitorati prima dell'avvio di Kaspersky Endpoint Security. Per configurare il successivo monitoraggio di tutti i moduli DLL e i driver prima dell'avvio dell'applicazione, riavviare il computer dopo avere selezionato la casella di controllo **Controlla DLL e moduli**. Se non è possibile riavviare il computer, dopo avere selezionato la casella di controllo **Controlla DLL e moduli** è possibile caricare moduli DLL e driver durante l'esecuzione di Kaspersky Endpoint Security. In questo caso, il monitoraggio ha effetto solo per i moduli DLL e i driver caricati mentre Kaspersky Endpoint Security è in esecuzione.

Durante il monitoraggio dei moduli DLL e dei driver, non è consigliabile utilizzare le regole di Controllo avvio applicazioni che sono state create in base alle categorie KL. La determinazione delle categorie KL (incluse le regole "Sistema operativo e relativi componenti") per i moduli DLL e i driver potrebbe non funzionare correttamente. In particolare, la regola "Sistema operativo e relativi componenti" è stata creata per impostazione predefinita e non viene distribuita durante l'avvio di moduli DLL e driver. Quando si attiva questa funzione, è necessario creare regole di autorizzazione distinte per moduli DLL e driver. L'utilizzo della funzione **Controlla DLL e moduli** se tali regole di autorizzazione non sono presenti potrebbe rendere instabile il sistema.

È consigliabile attivare la protezione tramite password per configurare le impostazioni del programma, in modo che sia possibile disattivare le regole di autorizzazione che bloccano l'avvio dei moduli DLL e dei driver di importanza critica, senza modificare le impostazioni del criterio di Kaspersky Security Center.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Gestione delle regole di Controllo avvio applicazioni tramite Kaspersky Security Center

Questa sezione contiene informazioni sull'utilizzo di Kaspersky Security Center per configurare le regole di Controllo avvio applicazioni, oltre a raccomandazioni per l'utilizzo ottimale di Controllo avvio applicazioni.

## Raccolta delle informazioni sulle applicazioni installate nei computer degli utenti

Per creare regole di Controllo avvio applicazioni ottimali, è prima consigliabile raccogliere informazioni sulle applicazioni utilizzate nei computer della rete locale. 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**.

## Creazione delle categorie di applicazioni

Per maggiore praticità durante la creazione delle regole, è possibile creare categorie di applicazioni e utilizzarle per la creazione delle regole di Controllo avvio 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 Administration Console di Kaspersky Security Center.
2. Nella struttura di Administration Console selezionare la cartella **Avanzate** → **Gestione applicazioni** → **Categorie di applicazioni**.
3. Fare clic sul pulsante **Crea 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.

## Creazione delle regole di Controllo avvio applicazioni tramite Kaspersky Security Center

*Per creare una regola di Controllo avvio applicazioni tramite Kaspersky Security Center:*

1. Aprire Administration Console di Kaspersky Security Center.
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 desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Controllo endpoint** selezionare la sottosezione **Controllo avvio applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo avvio applicazioni.
7. Fare clic sul pulsante **Aggiungi**.

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

8. Nell'elenco a discesa **Categoria** selezionare la categoria di applicazioni in base alla quale creare una regola.

9. Specificare l'elenco degli utenti e/o dei gruppi di utenti per cui configurare l'autorizzazione per l'avvio delle applicazioni della categoria selezionata. A tale scopo, nella tabella **Entità e relativi diritti** fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra standard di Microsoft Windows **Seleziona utenti e gruppi**. In questa finestra è possibile selezionare utenti e/o gruppi di utenti.

10. Nella tabella **Entità e relativi diritti**:

    - Se si desidera consentire agli utenti e/o ai gruppi di utenti di avviare le applicazioni che appartengono alla categoria selezionata, selezionare le caselle di controllo **Consenti** accanto agli utenti corrispondenti.

    - Se si desidera impedire agli utenti e/o ai gruppi di utenti di avviare le applicazioni che appartengono alla categoria selezionata, selezionare le caselle di controllo **Blocca** accanto agli utenti 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 **Entità** e che non fanno parte del gruppo di utenti specificati nella colonna **Entità** di avviare le applicazioni che appartengono alla categoria selezionata.

12. Se si desidera che Kaspersky Endpoint Security consideri le applicazioni della categoria specificata nella regola come programmi di aggiornamento attendibili e consenta loro di avviare altre applicazioni per cui non sono definite regole di Controllo avvio applicazioni, selezionare la casella di controllo **Programmi di aggiornamento attendibili**.

13. Fare clic su **OK**.

14. Nella sezione **Controllo avvio applicazioni** della finestra delle proprietà del criterio fare clic sul pulsante **Applica**.

## Modifica dello stato di una regola di Controllo avvio applicazioni tramite Kaspersky Security Center

*Per modificare lo stato di una regola di Controllo avvio applicazioni:*

1. Aprire Administration Console di Kaspersky Security Center.

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 desiderato.

5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:

   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.

   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

6. Nella sezione **Controllo endpoint** selezionare la sottosezione **Controllo avvio applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo avvio applicazioni.

7. Selezionare la regola di Controllo avvio applicazioni di cui si desidera modificare lo stato.

8. Nella colonna **Stato** eseguire una delle seguenti operazioni:

   - Se si desidera abilitare l'utilizzo di una regola, selezionare la casella di controllo accanto alla regola.
   - Se si desidera disabilitare l'utilizzo di una regola, deselezionare la casella di controllo accanto alla regola.

9. Fare clic sul pulsante **Applica**.

# Controllo privilegi applicazioni

Questo componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

Questa sezione contiene informazioni su Controllo privilegi applicazioni e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Controllo privilegi applicazioni

Controllo privilegi applicazioni 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 di identità.

Questo componente controlla l'attività delle applicazioni, incluso l'accesso alle risorse protette come file, cartelle e chiavi del Registro di sistema, utilizzando le *regole di controllo delle applicazioni*. Le regole di controllo delle applicazioni sono un set di restrizioni applicate alle varie azioni delle applicazioni del sistema operativo e ai diritti di accesso alle risorse del computer.

Le attività di rete delle applicazioni sono monitorate dal componente Firewall.

Quando un'applicazione viene avviata per la prima volta, Controllo privilegi applicazioni esamina l'applicazione e la inserisce in un gruppo di attendibilità. Un gruppo di attendibilità definisce le regole di controllo delle applicazioni che vengono applicate da Kaspersky Endpoint Security durante il controllo delle attività delle applicazioni.

È consigliabile partecipare a Kaspersky Security Network per rendere più efficace il funzionamento di Controllo privilegi applicazioni. I dati ottenuti tramite Kaspersky Security Network consentono di ordinare le applicazioni in gruppi con una maggiore precisione e di applicare regole di controllo delle applicazioni ottimali.

Al successivo avvio dell'applicazione, Controllo privilegi applicazioni ne verifica l'integrità. Se l'applicazione non è stata modificata, il componente applica all'applicazione le regole di controllo delle applicazioni correnti. Se l'applicazione è stata modificata, Controllo privilegi applicazioni l'analizza nuovamente, come avviene al primo avvio.

## Limitazioni del controllo dei dispositivi audio e video

### Informazioni sulla protezione dei flussi audio

Per la protezione dei flussi audio tenere presenti le seguenti considerazioni speciali:

- Per poter utilizzare questa funzionalità, il componente Controllo privilegi applicazioni deve essere abilitato.
- Se l'applicazione ha iniziato a ricevere il flusso audio prima dell'avvio del componente di Controllo privilegi applicazioni, 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 nella finestra delle impostazioni di Controllo applicazioni), 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.

## Considerazioni speciali sull'utilizzo dei dispositivi audio e video durante l'installazione e l'upgrade di Kaspersky Endpoint Security

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.

## Informazioni sull'accesso alle webcam da parte 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.

## Webcam supportate

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.

## Abilitazione e disabilitazione di Controllo privilegi applicazioni

Per impostazione predefinita, Controllo privilegi applicazioni è abilitato e viene eseguito nella modalità consigliata dagli specialisti di Kaspersky. Se necessario, è possibile disabilitare Controllo privilegi applicazioni.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Controllo privilegi applicazioni nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Controllo endpoint**.

   Verrà aperta la sezione **Controllo endpoint**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente Controllo privilegi applicazioni.

   Verrà visualizzato un menu per la selezione delle azioni sul componente.
5. Eseguire una delle seguenti operazioni:

   - Per abilitare Controllo privilegi applicazioni, selezionare **Avvia**.

     L'icona di stato del componente , visualizzata a sinistra nella riga Controllo privilegi applicazioni, diventa .
   - Per disabilitare il componente Controllo privilegi applicazioni, selezionare **Interrompi**.

     L'icona di stato del componente , visualizzata a sinistra nella riga Controllo privilegi applicazioni, diventa .

*Per abilitare o disabilitare Controllo privilegi applicazioni dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.

3. Nella parte destra della finestra eseguire una delle seguenti operazioni:

   - Per abilitare Controllo privilegi applicazioni, selezionare la casella di controllo **Abilita Controllo privilegi applicazioni**.
   - Per disabilitare Controllo privilegi applicazioni, deselezionare la casella di controllo **Abilita Controllo privilegi applicazioni**.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Gestione dei gruppi di attendibilità delle applicazioni

Quando un'applicazione viene avviata per la prima volta, il componente Controllo privilegi applicazioni controlla la sicurezza dell'applicazione e la inserisce in un gruppo 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 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 nei database KSN è cambiata.

È possibile selezionare un gruppo di attendibilità a cui devono essere assegnate automaticamente tutte le applicazioni sconosciute. Le applicazioni che sono state avviate prima di Kaspersky Endpoint Security vengono spostate automaticamente nel gruppo di attendibilità specificato nella finestra **Seleziona gruppo di attendibilità**.

Il componente controlla solo l'attività di rete delle applicazioni avviate prima di Kaspersky Endpoint Security in base al set delle regole di rete nelle impostazioni di Firewall.

## Configurazione delle impostazioni per l'assegnazione delle applicazioni ai gruppi di attendibilità

Se la partecipazione a Kaspersky Security Network è abilitata, Kaspersky Endpoint Security invia a KSN una query sulla reputazione di un'applicazione ogni volta che l'applicazione viene avviata. In base alla risposta ricevuta da KSN, l'applicazione può essere spostata in un gruppo di attendibilità diverso da quello specificato nelle impostazioni di Controllo privilegi applicazioni.

*Per configurare le impostazioni per il posizionamento delle applicazioni nei gruppi di attendibilità:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.

3. Se si desidera inserire automaticamente le applicazioni dotate di firma digitale dei produttori attendibili nel gruppo Attendibili, selezionare la casella di controllo **Considera attendibili le applicazioni con firma digitale**.

   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.

4. Scegliere il modo in cui le applicazioni sconosciute devono essere assegnate ai gruppi di attendibilità:

   - Per utilizzare l'analisi euristica per assegnare le applicazioni sconosciute ai gruppi di attendibilità, selezionare l'opzione **Usa l'analisi euristica per definire il gruppo** e specificare nel campo **Tempo limite per definire il gruppo** il periodo di tempo allocato per la scansione dell'applicazione avviata.

   - Se si desidera assegnare tutte le applicazioni sconosciute a un gruppo di attendibilità specificato, scegliere l'opzione **Sposta automaticamente nel gruppo**, quindi selezionare il gruppo di attendibilità appropriato dall'elenco a discesa.

     Per motivi di sicurezza, il gruppo **Attendibili** non è incluso nei valori dell'impostazione **Sposta automaticamente nel gruppo**.

5. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica di un gruppo di attendibilità

Al primo avvio di un'applicazione, Kaspersky Endpoint Security la inserisce automaticamente in un gruppo di attendibilità. È possibile spostare manualmente l'applicazione in un altro gruppo di attendibilità, se necessario.

Gli specialisti di Kaspersky consigliano di non spostare le applicazioni dal gruppo di attendibilità a cui sono assegnate automaticamente. È preferibile modificare le regole per una specifica applicazione.

*Per modificare il gruppo di attendibilità a cui un'applicazione è stata assegnata automaticamente da Kaspersky Endpoint Security al primo avvio:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.

3. Fare clic sul pulsante **Applicazioni**.

   Verrà aperta la scheda **Regole di controllo applicazioni** nella finestra **Applicazioni**.

4. Selezionare l'applicazione desiderata nella scheda **Regole di controllo applicazioni**.

5. Eseguire una delle seguenti operazioni:

   - Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida dell'applicazione. Dal menu di scelta rapida dell'applicazione selezionare **Sposta nel gruppo** → <νομε γρυππο>.

- Per aprire il menu di scelta rapida, fare clic sul collegamento **Attendibili** / **Restrizione bassa** / **Restrizione alta** / **Non attendibili**. Nel menu di scelta rapida selezionare il gruppo di attendibilità desiderato.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Selezione di un gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security

Il componente controlla solo l'attività di rete delle applicazioni che sono state avviate prima di Kaspersky Endpoint Security. Il controllo viene eseguito in base alle regole di rete specificate 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.

*Per selezionare il gruppo di attendibilità per le applicazioni avviate prima di Kaspersky Endpoint Security:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.

3. Fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Seleziona gruppo di attendibilità**.

4. Selezionare il gruppo di attendibilità desiderato.

5. Fare clic su **OK**.

6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Gestione delle regole di controllo applicazioni

Per impostazione predefinita, l'attività delle applicazioni è controllata dalle regole di controllo delle applicazioni definite per il gruppo di attendibilità a cui Kaspersky Endpoint Security ha assegnato l'applicazione al primo avvio. Se necessario, è possibile modificare le regole di controllo 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.

Le regole di controllo delle applicazioni definite per singole applicazioni o gruppi di applicazioni all'interno di un gruppo di attendibilità hanno una priorità superiore rispetto alle regole di controllo delle applicazioni definite per un gruppo di attendibilità. In altre parole, se le impostazioni delle regole di controllo delle applicazioni per una singola applicazione o per un gruppo di applicazioni all'interno di un gruppo di attendibilità sono diverse dalle impostazioni delle regole di controllo delle applicazioni per il gruppo di attendibilità, il componente Controllo privilegi applicazioni controlla l'attività dell'applicazione o del gruppo di applicazioni all'interno del gruppo di attendibilità in base alle regole di controllo delle applicazioni definite per tale applicazione o gruppo di applicazioni.

# Modifica delle regole di controllo applicazioni per gruppi di attendibilità e gruppi di applicazioni

Le regole ottimali di controllo delle applicazioni per i differenti gruppi di attendibilità vengono create per impostazione predefinita. Le impostazioni delle regole per il controllo dei gruppi di applicazioni ereditano i valori dalle impostazioni delle regole di controllo dei gruppi di attendibilità. È possibile modificare le regole preimpostate di controllo dei gruppi di attendibilità e di controllo dei gruppi di applicazioni.

*Per modificare le regole di controllo dei gruppi di attendibilità o di controllo dei gruppi di applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.
3. Fare clic sul pulsante **Applicazioni**.

   Verrà aperta la scheda **Regole di controllo applicazioni** nella finestra **Controllo privilegi applicazioni**.
4. Selezionare il gruppo di attendibilità o il gruppo di applicazioni desiderato.
5. Dal menu di scelta rapida di un gruppo di attendibilità o di un gruppo di applicazioni selezionare **Regole gruppo**.

   Verrà visualizzata la finestra **Regole di controllo gruppo applicazioni**.
6. Nella finestra **Regole di controllo gruppo applicazioni** eseguire una delle seguenti operazioni:

   - Per modificare le regole di controllo dei gruppi di attendibilità o dei gruppi di applicazioni che determinano i diritti del gruppo di attendibilità o del gruppo di applicazioni di accedere al Registro di sistema del sistema operativo, ai file dell'utente e alle impostazioni delle applicazioni, selezionare la scheda **File e registro di sistema**.
   - Per modificare le regole di controllo dei gruppi di attendibilità o dei gruppi di applicazioni che determinano i diritti del gruppo di attendibilità o del gruppo di applicazioni di accedere ai processi e agli oggetti del sistema operativo, selezionare la scheda **Diritti**.
7. Per la risorsa desiderata, nella colonna dell'azione corrispondente, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
8. Dal menu di scelta rapida selezionare l'elemento desiderato.

   - **Eredita**
   - **Consenti**
   - **Blocca**
   - **Registra eventi**

   Se si stanno modificando regole di controllo di un gruppo di attendibilità, il comando **Eredita** non è disponibile.

9. Fare clic su **OK**.
10. Nella finestra **Applicazioni** fare clic su **OK**.
11. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica di una regola di controllo delle applicazioni

Per impostazione predefinita, le impostazioni delle regole di controllo delle applicazioni per le applicazioni che appartengono a un gruppo di applicazioni o a un gruppo di attendibilità ereditano i valori delle impostazioni delle regole di controllo dei gruppi di attendibilità. È possibile modificare le impostazioni delle regole di controllo delle applicazioni.

*Per modificare una regola di controllo per le applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.
3. Fare clic sul pulsante **Applicazioni**.

   Verrà aperta la scheda **Regole di controllo applicazioni** nella finestra **Controllo privilegi applicazioni**.
4. Selezionare l'applicazione desiderata.
5. Eseguire una delle seguenti operazioni:

   - Dal menu di scelta rapida dell'applicazione selezionare **Regole applicazione**.
   - Fare clic sul pulsante **Avanzate** nell'angolo inferiore destro della scheda **Regole di controllo applicazioni**.

   Verrà visualizzata la finestra **Regole di controllo applicazioni**.
6. Nella finestra **Regole di controllo applicazioni** eseguire una delle seguenti operazioni:

   - Per modificare le regole di controllo delle applicazioni che determinano i diritti dell'applicazione di accedere al Registro di sistema del sistema operativo, ai file dell'utente e alle impostazioni delle applicazioni, selezionare la scheda **File e registro di sistema**.
   - Per modificare le regole di controllo delle applicazioni che determinano i diritti dell'applicazione di accedere ai processi e agli oggetti del sistema operativo, selezionare la scheda **Diritti**.
7. Per la risorsa desiderata, nella colonna dell'azione corrispondente, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
8. Dal menu di scelta rapida selezionare l'elemento desiderato.

   - **Eredita**
   - **Consenti**

- **Blocca**
- **Registra eventi**

9. Fare clic su **OK**.
10. Nella finestra **Applicazioni** fare clic su **OK**.
11. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Disabilitazione dei download e degli aggiornamenti delle regole di controllo delle applicazioni dal database di Kaspersky Security Network

Per impostazione predefinita, quando vengono rilevate nuove informazioni su un'applicazione nel database di Kaspersky Security Network, Kaspersky Endpoint Security applica le regole di controllo scaricate dal database KSN per questa applicazione. È possibile quindi modificare manualmente le regole di controllo per l'applicazione.

Se un'applicazione non era presente nel database di Kaspersky Security Network al primo avvio ma le informazioni sono state aggiunte al database successivamente, per impostazione predefinita Kaspersky Endpoint Security aggiorna automaticamente le regole di controllo per l'applicazione.

È possibile disabilitare i download delle regole di controllo delle applicazioni dal database di Kaspersky Security Network e l'aggiornamento automatico delle regole di controllo per le applicazioni precedentemente sconosciute.

*Per disabilitare i download e gli aggiornamenti delle regole di controllo delle applicazioni dal database di Kaspersky Security Network:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.
3. Deselezionare la casella di controllo **Aggiorna le regole di controllo per le applicazioni precedentemente sconosciute dai database KSN**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Disabilitazione dell'ereditarietà delle restrizioni dal processo principale

L'avvio dell'applicazione può essere effettuato dall'utente o da un'altra applicazione in esecuzione. Quando l'avvio dell'applicazione viene effettuato da un'altra applicazione, viene creata una sequenza di avvio che include processi principali e secondari.

Quando un'applicazione tenta di ottenere l'accesso a una risorsa protetta, Controllo privilegi applicazioni analizza tutti i processi principali dell'applicazione per determinare se dispongono dei diritti per l'accesso alla risorsa protetta. Viene quindi osservata la regola della priorità minima: durante il confronto tra i diritti di accesso dell'applicazione e quelli del processo principale, vengono applicati all'attività dell'applicazione i diritti di accesso con una priorità minima.

La priorità dei diritti di accesso è la seguente:

1. **Consenti** Questo diritto di accesso ha la priorità più elevata.
2. **Blocca** Questo diritto di accesso ha la priorità più bassa.

Questo meccanismo impedisce l'utilizzo delle applicazioni attendibili da parte di un'applicazione non attendibile o di un'applicazione con diritti limitati per eseguire azioni che richiedono determinati privilegi.

Se le attività di un'applicazione vengono bloccate perché un processo principale dispone di diritti insufficienti, è possibile modificare tali diritti o disabilitare l'ereditarietà delle restrizioni dal processo principale.

*Per disabilitare l'ereditarietà delle restrizioni dal processo principale:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.
3. Fare clic sul pulsante **Applicazioni**.

   Verrà aperta la scheda **Regole di controllo applicazioni** nella finestra **Controllo privilegi applicazioni**.
4. Selezionare l'applicazione desiderata.
5. Dal menu di scelta rapida dell'applicazione selezionare **Regole applicazione**.

   Verrà visualizzata la finestra **Regole di controllo applicazioni**.
6. Nella finestra **Regole di controllo applicazioni** selezionare la scheda **Esclusioni**.
7. Selezionare la casella di controllo **Non ereditare restrizioni del processo principale (applicazione)**.
8. Fare clic su **OK**.
9. Nella finestra **Applicazioni** fare clic su **OK**.
10. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Esclusione di specifiche azioni delle applicazioni dalle regole di controllo delle applicazioni

*Per escludere specifiche azioni delle applicazioni dalle regole di controllo delle applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.
3. Fare clic sul pulsante **Applicazioni**.

Verrà aperta la scheda **Regole di controllo applicazioni** nella finestra **Controllo privilegi applicazioni**.

4. Selezionare l'applicazione desiderata.
5. Dal menu di scelta rapida dell'applicazione selezionare **Regole applicazione**.

   Verrà visualizzata la finestra **Regole di controllo applicazioni**.
6. Selezionare la scheda **Esclusioni**.
7. Selezionare le caselle di controllo accanto alle azioni dell'applicazione che non è necessario monitorare.
8. Fare clic su **OK**.
9. Nella finestra **Applicazioni** fare clic su **OK**.
10. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Rimozione delle regole di Controllo Applicazioni obsolete

Per impostazione predefinita, le regole di controllo per le applicazioni non avviate per 60 giorni vengono eliminate. È possibile modificare la durata di archiviazione per le regole di controllo delle applicazioni inutilizzate o disabilitare l'eliminazione automatica delle regole.

*Per eliminare le regole di Controllo Applicazioni obsolete:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.
3. Eseguire una delle seguenti operazioni:

   - Se si desidera eliminare le regole di controllo delle applicazioni inutilizzate, selezionare la casella di controllo **Elimina le regole per le applicazioni che non vengono avviate per più di**, quindi selezionare il numero di giorni desiderato.
   - Per disabilitare l'eliminazione automatica delle regole di controllo delle applicazioni utilizzate, deselezionare la casella di controllo **Elimina le regole per le applicazioni che non vengono avviate per più di**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Protezione delle risorse del sistema operativo e dei dati di identità

Controllo privilegi applicazioni gestisce i diritti delle applicazioni per l'esecuzione di azioni sulle varie categorie di risorse del sistema operativo e di dati di identità.

Le categorie preimpostate di risorse protette sono state definite dagli specialisti di Kaspersky. Non è possibile modificare o eliminare le categorie preimpostate di risorse protette o le risorse protette in queste categorie.

È possibile eseguire le seguenti azioni:

- Aggiungere una nuova categoria di risorse protette.
- Aggiungere una nuova risorsa protetta.
- Disabilitare la protezione di una risorsa.

## Aggiunta di una categoria di risorse protette

*Per aggiungere una nuova categoria di risorse protette:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.
3. Fare clic sul pulsante **Risorse**.

   Verrà aperta la scheda **Risorse protette** nella finestra **Controllo privilegi applicazioni**.
4. Nella parte sinistra della scheda **Risorse protette** selezionare una sezione o una categoria di risorse protette a cui aggiungere una nuova categoria di risorse protette.
5. Fare clic sul pulsante **Aggiungi** e selezionare **Categoria** nell'elenco a discesa.

   Verrà visualizzata la finestra **Categoria di risorse protette**.
6. Nella finestra **Categoria di risorse protette** visualizzata immettere un nome per la nuova categoria di risorse protette.
7. Fare clic su **OK**.

   Viene visualizzato un nuovo elemento nell'elenco delle categorie di risorse protette.
8. Nella finestra **Controllo privilegi applicazioni** fare clic su **OK**.
9. Per salvare le modifiche, fare clic sul pulsante **Salva**.

Dopo avere aggiunto una categoria di risorse protette, è possibile modificarla o rimuoverla facendo clic sui pulsanti **Modifica** o **Rimuovi** nell'angolo superiore sinistro della scheda **Risorse protette**.

## Aggiunta di una risorsa protetta

*Per aggiungere una risorsa protetta:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.
3. Fare clic sul pulsante **Risorse**.

   Verrà aperta la scheda **Risorse protette** nella finestra **Controllo privilegi applicazioni**.
4. Nella parte sinistra della scheda **Risorse protette** selezionare una categoria di risorse protette a cui aggiungere una nuova risorsa protetta.
5. Fare clic sul pulsante **Aggiungi** e selezionare nell'elenco a discesa il tipo di risorsa da aggiungere:

   - **File o cartella**.
   - **Chiave di registro**.

   Verrà visualizzata la finestra **Risorsa protetta**.
6. Nella finestra **Risorsa protetta** immettere il nome della risorsa protetta nel campo **Nome**.
7. Fare clic sul pulsante **Sfoglia**.
8. Nella finestra visualizzata specificare le impostazioni necessarie a seconda del tipo di risorsa protetta da aggiungere. Fare clic su **OK**.
9. Nella finestra **Risorsa protetta** fare clic su **OK**.

   Viene visualizzato un nuovo elemento nell'elenco delle risorse protette della categoria selezionata nella scheda **Risorse protette**.
10. Nella finestra **Controllo privilegi applicazioni** fare clic su **OK**.
11. Per salvare le modifiche, fare clic sul pulsante **Salva**.

Dopo avere aggiunto una risorsa protetta, è possibile modificarla o rimuoverla facendo clic sui pulsanti **Modifica** o **Rimuovi** nell'angolo superiore sinistro della scheda **Risorse protette**.

## Disabilitazione della protezione di una risorsa

*Per disabilitare la protezione di una risorsa:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo privilegi applicazioni**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo privilegi applicazioni.
3. Nella parte destra della finestra fare clic sul pulsante **Risorse**.

Verrà aperta la scheda **Risorse protette** nella finestra **Controllo privilegi applicazioni**.

4. Eseguire una delle seguenti operazioni:

   - Nella parte sinistra della scheda, nell'elenco delle risorse protette, selezionare la risorsa per cui si desidera disabilitare la protezione e deselezionare la casella di controllo accanto al relativo nome.

   - Fare clic su **Esclusioni**, quindi eseguire le seguenti operazioni:

     a. Nella finestra **Esclusioni** fare clic sul pulsante **Aggiungi**. Selezionare dall'elenco a discesa il tipo di risorsa che si desidera aggiungere all'elenco delle esclusioni dalla protezione del componente Controllo privilegi applicazioni: **File o cartella** o **Chiave di registro**.

     Verrà visualizzata la finestra **Risorsa protetta**.

     b. Nella finestra **Risorsa protetta** immettere il nome della risorsa protetta nel campo **Nome**.

     c. Fare clic sul pulsante **Sfoglia**.

     d. Nella finestra visualizzata specificare le impostazioni desiderate a seconda del tipo di risorsa protetta che si desidera aggiungere all'elenco delle esclusioni dalla protezione del componente Controllo privilegi applicazioni.

     e. Fare clic su **OK**.

     f. Nella finestra **Risorsa protetta** fare clic su **OK**.

     Viene visualizzato un nuovo elemento nell'elenco delle risorse escluse dalla protezione del componente Controllo privilegi applicazioni.

     > Dopo avere aggiunto una risorsa all'elenco delle esclusioni dalla protezione del componente Controllo privilegi applicazioni, è possibile modificarla o rimuoverla facendo clic sui pulsanti **Modifica** o **Rimuovi** nella parte superiore della finestra **Esclusioni**.

     g. Nella finestra **Esclusioni** fare clic su **OK**.

5. Nella finestra **Controllo privilegi applicazioni** fare clic su **OK**.

6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Monitor vulnerabilità

Questo componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

Questa sezione contiene informazioni su Monitor vulnerabilità e istruzioni su come abilitare o disabilitare il componente.

## Informazioni su Monitor vulnerabilità

Il componente Monitor vulnerabilità esegue una scansione in tempo reale delle vulnerabilità nelle applicazioni in esecuzione nel computer dell'utente o avviate da quest'ultimo. Quando il componente Monitor vulnerabilità è abilitato, non è necessario avviare l'attività Scansione Vulnerabilità. Questa scansione è importante quando un'attività Scansione Vulnerabilità per le applicazioni installate nel computer dell'utente non è mai stata eseguita o non viene eseguita da molto tempo.

## Abilitazione e disabilitazione di Monitor vulnerabilità

Il componente Monitor vulnerabilità è disabilitato per impostazione predefinita. Se necessario, è possibile abilitare Monitor vulnerabilità.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Monitor vulnerabilità nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Controllo endpoint**.

   Verrà aperta la sezione **Controllo endpoint**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente Monitor vulnerabilità.

   Verrà visualizzato un menu per la selezione delle azioni sul componente.
5. Eseguire una delle seguenti operazioni:

   - Per abilitare Monitor vulnerabilità, selezionare **Avvia**.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Monitor vulnerabilità**, diventa .
   - Per disabilitare Monitor vulnerabilità, selezionare **Interrompi**.

     L'icona di stato del componente , visualizzata a sinistra nella riga **Monitor vulnerabilità**, diventa .

*Per abilitare o disabilitare Monitor vulnerabilità dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare **Monitor vulnerabilità**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Monitor vulnerabilità.
3. Nella parte destra della finestra eseguire una delle seguenti operazioni:

   - Se si desidera che Kaspersky Endpoint Security esegua una scansione delle vulnerabilità delle applicazioni in esecuzione nel computer dell'utente o avviate da quest'ultimo, selezionare la casella di controllo **Abilita Monitor vulnerabilità**.
   - Se non si desidera che Kaspersky Endpoint Security esegua una scansione delle vulnerabilità delle applicazioni in esecuzione nel computer dell'utente o avviate da quest'ultimo, deselezionare la casella di controllo **Abilita Monitor vulnerabilità**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Controllo dispositivi

Questo componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

Questa sezione contiene informazioni su Controllo dispositivi e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Controllo dispositivi

Controllo dispositivi garantisce la protezione dei dati riservati limitando l'accesso dell'utente ai dispositivi installati nel computer o ad esso connessi, inclusi:

- Dispositivi di memorizzazione dei dati (dischi rigidi, unità rimovibili, unità a nastro e unità CD/DVD)
- Dispositivi di trasferimento dei dati (modem, schede di rete esterne)
- Dispositivi progettati per la conversione dei dati in copie cartacee (stampanti)
- Bus di connessione (anche denominati semplicemente "bus"), ovvero interfacce per la connessione di dispositivi ai computer (come ad esempio USB, FireWire e infrarossi)

Controllo dispositivi gestisce l'accesso degli utenti ai dispositivi applicando *regole di accesso ai dispositivi* (anche denominate "regole di accesso") e *regole di accesso ai bus di connessione* (anche denominate "regole di accesso ai bus").

## Abilitazione e disabilitazione di Controllo dispositivi

Controllo dispositivi è abilitato per impostazione predefinita. Se necessario, è possibile disabilitare Controllo dispositivi.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Controllo dispositivi nella scheda **Protezione e controllo** della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Controllo endpoint**.

   Verrà aperta la sezione **Controllo endpoint**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente Controllo dispositivi.

Verrà visualizzato un menu per la selezione delle azioni sul componente.

5. Eseguire una delle seguenti operazioni:

   - Per abilitare il componente Controllo dispositivi, selezionare **Avvia** dal menu.
   - Per disabilitare il componente Controllo dispositivi, selezionare **Interrompi** dal menu.

*Per abilitare o disabilitare Controllo dispositivi dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo dispositivi**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo dispositivi.
3. Eseguire una delle seguenti operazioni:

   - Per abilitare Controllo dispositivi, selezionare la casella di controllo **Abilita Controllo dispositivi**.
   - Per disabilitare Controllo dispositivi, deselezionare la casella di controllo **Abilita Controllo dispositivi**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Informazioni sulle regole di accesso a dispositivi e bus di connessione

Una regola di accesso ai dispositivi è una combinazione di parametri che definisce le seguenti funzioni del componente Controllo dispositivi:

- Consentire a utenti e/o gruppi di utenti selezionati di accedere a specifici tipi di dispositivi durante specifici periodi di tempo.

  È possibile selezionare un utente e/o un gruppo di utenti e creare una pianificazione di accesso ai dispositivi per tale utente o gruppo.
- Impostare il diritto per la lettura del contenuto dei dispositivi di memoria.
- Impostare il diritto per la modifica del contenuto dei dispositivi di memoria.

Per impostazione predefinita, vengono create regole di accesso per tutti i tipi di dispositivi nella classificazione del componente Controllo dispositivi. Tali regole consentono a tutti gli utenti di accedere in modo completo ai dispositivi in qualsiasi momento, se è consentito l'accesso ai bus di connessione dei tipi di dispositivi corrispondenti.

La regola di accesso al bus di connessione consente o blocca l'accesso al bus di connessione.

Per impostazione predefinita, vengono create regole che consentono l'accesso a tutti i bus di connessione presenti nella classificazione del componente Controllo dispositivi.

Non è possibile creare o eliminare regole di accesso ai dispositivi o regole di accesso ai bus di connessione; è solo possibile modificarle.

## Informazioni sui dispositivi attendibili

I *dispositivi attendibili* sono dispositivi a cui hanno accesso completo gli utenti specificati nelle impostazioni del dispositivo attendibile.

Per l'utilizzo dei dispositivi attendibili sono disponibili le seguenti azioni:

- Aggiungere il dispositivo all'elenco dei dispositivi attendibili.
- Modificare l'utente e/o il gruppo di utenti a cui è consentito accedere al dispositivo attendibile.
- Eliminare il dispositivo dall'elenco dei dispositivi attendibili.

Se è stato aggiunto un dispositivo all'elenco dei dispositivi attendibili ed è stata creata una regola di accesso per questo tipo di dispositivo che blocca o limita l'accesso, Kaspersky Endpoint Security stabilisce se concedere o meno l'accesso al dispositivo in base alla sua presenza nell'elenco dei dispositivi attendibili. La presenza nell'elenco dei dispositivi attendibili ha una priorità più alta rispetto a una regola di accesso.

## Decisioni standard sull'accesso ai dispositivi

Kaspersky Endpoint Security stabilisce se consentire l'accesso a un dispositivo dopo che l'utente connette il dispositivo al computer.

Decisioni standard sull'accesso ai dispositivi

| N. | Condizioni iniziali | Passaggi intermedi da intraprendere finché non viene presa una decisione in merito all'accesso | | | Decisione in merito all'accesso al dispositivo |
|---|---|---|---|---|---|
| | | Verifica della presenza del dispositivo nell'elenco dei dispositivi attendibili | Verifica dell'accesso al dispositivo in base alla regola di accesso | Verifica dell'accesso al bus in base alla regola di accesso al bus | |
| 1 | Il dispositivo non è presente nella classificazione dei dispositivi del componente Controllo dispositivi. | Non incluso nell'elenco dei dispositivi attendibili. | Nessuna regola di accesso. | Non soggetto a scansione. | Accesso consentito. |
| 2 | Il dispositivo è attendibile. | Incluso nell'elenco dei dispositivi attendibili. | Non soggetto a scansione. | Non soggetto a scansione. | Accesso consentito. |
| 3 | L'accesso al dispositivo è consentito. | Non incluso nell'elenco dei dispositivi attendibili. | Accesso consentito. | Non soggetto a scansione. | Accesso consentito. |
| 4 | L'accesso al dispositivo dipende dal bus. | Non incluso nell'elenco dei dispositivi attendibili. | L'accesso dipende dal bus. | Accesso consentito. | Accesso consentito. |

| | | | | | |
|---|---|---|---|---|---|
| 5 | L'accesso al dispositivo dipende dal bus. | Non incluso nell'elenco dei dispositivi attendibili. | L'accesso dipende dal bus. | Accesso bloccato. | Accesso bloccato. |
| 6 | L'accesso al dispositivo è consentito. Nessuna regola di accesso al bus trovata. | Non incluso nell'elenco dei dispositivi attendibili. | Accesso consentito. | Nessuna regola di accesso al bus. | Accesso consentito. |
| 7 | L'accesso al dispositivo è bloccato. | Non incluso nell'elenco dei dispositivi attendibili. | Accesso bloccato. | Non soggetto a scansione. | Accesso bloccato. |
| 8 | Nessuna regola di accesso ai dispositivi o di accesso al bus trovata. | Non incluso nell'elenco dei dispositivi attendibili. | Nessuna regola di accesso. | Nessuna regola di accesso al bus. | Accesso consentito. |
| 9 | Nessuna regola di accesso ai dispositivi. | Non incluso nell'elenco dei dispositivi attendibili. | Nessuna regola di accesso. | Accesso consentito. | Accesso consentito. |
| 10 | Nessuna regola di accesso ai dispositivi. | Non incluso nell'elenco dei dispositivi attendibili. | Nessuna regola di accesso. | Accesso bloccato. | Accesso bloccato. |

È possibile modificare la regola di accesso ai dispositivi dopo la connessione del dispositivo. Se il dispositivo è connesso e la regola di accesso consente di accedervi, ma in seguito si modifica la regola e si blocca l'accesso, Kaspersky Endpoint Security blocca l'accesso alla successiva richiesta di un'operazione su un file da parte del dispositivo (visualizzazione della struttura di cartelle, lettura o scrittura). 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.

## Modifica di una regola di accesso ai dispositivi

A seconda del tipo di dispositivo, è possibile modificare varie impostazioni di accesso, ad esempio l'elenco degli utenti che ottengono l'accesso al dispositivo, la pianificazione di accesso e l'autorizzazione o il blocco dell'accesso.

*Per modificare una regola di accesso ai dispositivi:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo dispositivi**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo dispositivi.
3. Nella parte destra della finestra selezionare la scheda **Tipi di dispositivi**.

   La scheda **Tipi di dispositivi** contiene le regole di accesso per tutti i dispositivi inclusi nella classificazione del componente Controllo dispositivi.
4. Selezionare la regola di accesso che si desidera modificare.

5. Fare clic sul pulsante **Modifica**. Il pulsante è disponibile solo per i tipi di dispositivo che dispongono di un file system.

   Verrà visualizzata la finestra **Configurazione della regola di accesso ai dispositivi**.

   Per impostazione predefinita, una regola di accesso ai dispositivi consente agli utenti l'accesso completo al tipo di dispositivi specificato in qualsiasi momento. Nell'elenco **Utenti e/o gruppi di utenti** questa regola di accesso contiene il gruppo **Tutto**. Nella tabella **Diritti del gruppo di utenti selezionato per pianificazioni di accesso** questa regola di accesso contiene l'elemento **Pianificazione predefinita** per l'accesso ai dispositivi, con i diritti per l'esecuzione di tutti i tipi di operazioni con i dispositivi.

6. Modificare le impostazioni della regola di accesso ai dispositivi:

   a. Selezionare un utente e/o un gruppo di utenti nell'elenco **Utenti e/o gruppi di utenti**.

      Per modificare l'elenco **Utenti e/o gruppi di utenti**, utilizzare i pulsanti **Aggiungi**, **Modifica** e **Rimuovi**.

   b. Nella tabella **Diritti del gruppo di utenti selezionato per pianificazioni di accesso** configurare la pianificazione per l'accesso ai dispositivi per l'utente e/o il gruppo di utenti selezionato. A tale scopo, selezionare le caselle di controllo accanto ai nomi delle pianificazioni di accesso ai dispositivi che si desidera utilizzare nella regola di accesso ai dispositivi da modificare.

      Per modificare l'elenco delle pianificazioni di accesso ai dispositivi, utilizzare i pulsanti **Crea**, **Modifica**, **Copia** e **Rimuovi** nella tabella **Diritti del gruppo di utenti selezionato per pianificazioni di accesso**.

   c. Per ogni pianificazione per l'accesso ai dispositivi utilizzata nella regola di cui è in corso la modifica, specificare le operazioni consentite durante l'utilizzo dei dispositivi. A tale scopo, nella tabella **Diritti del gruppo di utenti selezionato per pianificazioni di accesso** selezionare le caselle di controllo nelle colonne con i nomi delle operazioni corrispondenti.

   d. Fare clic su **OK**.

   Dopo aver modificato le impostazioni predefinite di una regola di accesso ai dispositivi, l'impostazione per l'accesso al tipo di dispositivo nella colonna **Accesso** della tabella nella scheda **Tipi di dispositivi** assume il valore *Limita in base alle regole*.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Aggiunta o esclusione di record del registro eventi

La registrazione degli eventi è disponibile solo per le operazioni con i file su unità rimovibili.

*Per abilitare o disabilitare la registrazione degli eventi:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo dispositivi**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo dispositivi.

3. Nella parte destra della finestra selezionare la scheda **Tipi di dispositivi**.

   La scheda **Tipi di dispositivi** contiene le regole di accesso per tutti i dispositivi inclusi nella classificazione del componente Controllo dispositivi.

4. Selezionare **Unità rimovibili** nella tabella dei dispositivi.

Il pulsante **Generazione di log** diventa disponibile nella parte superiore della tabella.

5. Fare clic sul pulsante **Generazione di log**.

   Verrà visualizzata la finestra **Impostazioni di generazione di log**.

6. Eseguire una delle seguenti operazioni:

   - Se si desidera abilitare la registrazione delle operazioni di eliminazione e scrittura di file su unità rimovibili, selezionare la casella di controllo **Abilita la generazione di log**.

     Kaspersky Endpoint Security salverà un evento nel file di log e invierà un messaggio a Kaspersky Security Center Administration Server ogni volta che l'utente esegue operazioni di scrittura o eliminazione con file su unità rimovibili.

   - In caso contrario, deselezionare la casella di controllo **Abilita la generazione di log**.

7. Specificare le operazioni da registrare. A tale scopo, eseguire una delle seguenti operazioni:

   - Se si desidera che Kaspersky Endpoint Security registri tutti gli eventi, selezionare la casella di controllo **Salva informazioni su tutti i file**.

   - Se si desidera che Kaspersky Endpoint Security registri solo le informazioni su un formato di file specifico, nella sezione **Filtro per i formati di file**, selezionare le caselle di controllo accanto ai formati di file desiderati.

8. Specificare le azioni degli utenti di Kaspersky Endpoint Security che devono essere registrate come eventi. A tale scopo:

   a. Nella sezione **Utenti** fare clic sul pulsante **Seleziona**.

      Verrà visualizzata la finestra standard di Microsoft Windows **Seleziona utenti e gruppi**.

   b. Specificare o modificare l'elenco degli utenti e/o dei gruppi di utenti.

   Quando gli utenti specificati nella sezione **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 un messaggio a Kaspersky Security Center Administration Server.

9. Nella finestra **Impostazioni di generazione di log** fare clic su **OK**.

10. Per salvare le modifiche, fare clic sul pulsante **Salva**.

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 di notifica per il componente Controllo dispositivi.

## 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. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo dispositivi**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo dispositivi.

3. Nella parte destra della finestra selezionare la scheda **Tipi di dispositivi**.

   La scheda **Tipi di dispositivi** contiene le regole di accesso per tutti i dispositivi inclusi nella classificazione del componente Controllo dispositivi.

4. Nella colonna **Accesso** accanto al dispositivo **Wi-Fi** fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida.

5. Selezionare l'opzione **Blocca con eccezioni**.

6. Nell'elenco dei dispositivi selezionare **Wi-Fi** e fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Reti Wi-Fi attendibili**.

7. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Rete Wi-Fi attendibile**.

8. Nella finestra **Rete Wi-Fi attendibile**:

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

9. Nella finestra **Rete Wi-Fi attendibile** fare clic su **OK**.

10. Nella finestra **Reti Wi-Fi attendibili** fare clic su **OK**.

## Modifica di una regola di accesso ai bus di connessione

*Per modificare una regola di accesso ai bus di connessione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo dispositivi**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo dispositivi.

3. Selezionare la scheda **Bus di connessione**.

La scheda **Bus di connessione** visualizza le regole di accesso per tutti i bus di connessione classificati nel componente Controllo dispositivi.

4. Selezionare la regola per i bus di connessione che si desidera modificare.
5. Modificare il valore del parametro di accesso:
   - Per consentire l'accesso a un bus di connessione, fare clic sulla colonna **Accesso** per aprire il menu di scelta rapida, quindi selezionare **Consenti**.
   - Per bloccare l'accesso a un bus di connessione, fare clic sulla colonna **Accesso** per aprire il menu di scelta rapida, quindi selezionare **Blocca**.
6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Azioni con i dispositivi attendibili

Questa sezione contiene informazioni sulle azioni con i dispositivi attendibili.

## 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo dispositivi**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo dispositivi.
3. Nella parte destra della finestra selezionare la scheda **Dispositivi attendibili**.
4. Fare clic sul pulsante **Seleziona**.

   Verrà visualizzata la finestra **Seleziona dispositivi attendibili**.
5. Selezionare la casella di controllo accanto al nome di un dispositivo da aggiungere all'elenco dei dispositivi attendibili.

   L'elenco nella colonna **Dispositivi** dipende dal valore selezionato nell'elenco a discesa **Visualizza dispositivi connessi**.
6. Fare clic sul pulsante **Seleziona**.

   Verrà visualizzata la finestra **Seleziona utenti e gruppi** di Microsoft Windows.
7. Nella finestra **Seleziona utenti e gruppi** di Microsoft Windows specificare gli utenti e/o i gruppi di utenti per cui Kaspersky Endpoint Security riconosce i dispositivi selezionati come attendibili.

I nomi di utenti e/o gruppi di utenti specificati nella finestra **Selezionare gli utenti e/o i gruppi di utenti** di Microsoft Windows vengono visualizzati nel campo **Consenti a utenti e/o gruppi di utenti**.

8. Nella finestra **Seleziona dispositivi attendibili** fare clic su **OK**.

   Nella tabella, nella scheda **Dispositivi attendibili** della finestra delle impostazioni del componente **Controllo dispositivi**, viene visualizzata una riga con i parametri del dispositivo attendibile che è stato aggiunto.

9. Ripetere i passaggi 4-7 per ogni dispositivo che si desidera aggiungere all'elenco dei dispositivi attendibili per gli utenti e/o i gruppi di utenti specificati.

10. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Aggiunta di un dispositivo all'elenco Attendibili in base al modello o all'ID del dispositivo

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 in base al modello o all'ID del dispositivo:*

1. Aprire Administration Console di Kaspersky Security Center.

2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera creare un elenco di dispositivi attendibili.

3. Nell'area di lavoro selezionare la scheda **Criteri**.

4. Selezionare il criterio desiderato.

5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:

   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.

   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

6. Nella sezione **Controllo endpoint** selezionare la sottosezione **Controllo dispositivi**.

7. Nella parte destra della finestra selezionare la scheda **Dispositivi attendibili**.

8. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzato il menu di scelta rapida del pulsante.

9. Nel menu di scelta rapida del pulsante **Aggiungi** eseguire una delle seguenti operazioni:

   - Selezionare il pulsante **Dispositivi per ID** se si desidera selezionare dispositivi con ID univoci noti per l'aggiunta all'elenco dei dispositivi attendibili.

   - Selezionare la voce **Dispositivi per modello** per aggiungere all'elenco i dispositivi attendibili con VID (ID produttore) e PID (ID prodotto) noti.

10. Nella finestra visualizzata selezionare nell'elenco a discesa **Tipo di dispositivo** il tipo di dispositivi da visualizzare nella tabella seguente.

11. Fare clic sul pulsante **Aggiorna**.

    Nella tabella viene visualizzato un elenco di dispositivi di cui sono noti gli ID e/o i modelli e che appartengono al tipo selezionato nell'elenco a discesa **Tipo di dispositivo**.

12. Selezionare le caselle di controllo accanto ai nomi dei dispositivi da aggiungere all'elenco dei dispositivi attendibili.

13. Fare clic sul pulsante **Seleziona**.

    Verrà visualizzata la finestra **Seleziona utenti e gruppi** di Microsoft Windows.

14. Nella finestra **Seleziona utenti e gruppi** di Microsoft Windows specificare gli utenti e/o i gruppi di utenti per cui Kaspersky Endpoint Security riconosce i dispositivi selezionati come attendibili.

    I nomi di utenti e/o gruppi di utenti specificati nella finestra **Selezionare gli utenti e/o i gruppi di utenti** di Microsoft Windows vengono visualizzati nel campo **Consenti a utenti e/o gruppi di utenti**.

15. Fare clic su **OK**.

    Vengono visualizzate delle righe con i parametri dei dispositivi attendibili che sono stati aggiunti nella tabella nella scheda **Dispositivi attendibili**.

16. Fare clic su **OK** o su **Applica** per salvare le modifiche.

## Aggiunta di un dispositivo all'elenco Attendibili in base alla maschera per l'ID del dispositivo

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).

I dispositivi possono essere aggiunti all'elenco Attendibili in base alla maschera del relativo ID solo in Kaspersky Security Center Administration Console.

*Per aggiungere dispositivi all'elenco Attendibili in base alla maschera del relativo ID:*

1. Aprire Administration Console di Kaspersky Security Center.

2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera creare un elenco di dispositivi attendibili.

3. Nell'area di lavoro selezionare la scheda **Criteri**.

4. Selezionare il criterio desiderato.

5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:

   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.

   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

6. Nella sezione **Controllo endpoint** selezionare la sottosezione **Controllo dispositivi**.

7. Nella parte destra della finestra selezionare la scheda **Dispositivi attendibili**.

8. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzato il menu di scelta rapida del pulsante.

9. Nel menu di scelta rapida del pulsante **Aggiungi** selezionare la voce **Dispositivi per maschera ID**.

   Verrà visualizzata la finestra **Aggiungi dispositivi attendibili per maschera ID**.

10. Nella finestra **Aggiungi dispositivi attendibili per maschera ID** immettere la maschera per gli ID dei dispositivi nel campo **Maschera**.

11. Fare clic sul pulsante **Seleziona**.

    Verrà visualizzata la finestra **Seleziona utenti e gruppi** di Microsoft Windows.

12. Nella finestra **Seleziona utenti e gruppi** di Microsoft Windows specificare gli utenti e/o i gruppi di utenti per cui Kaspersky Endpoint Security riconosce come attendibili i dispositivi con modelli o ID che corrispondono alla maschera specificata.

    I nomi di utenti e/o gruppi di utenti specificati nella finestra **Selezionare gli utenti e/o i gruppi di utenti** di Microsoft Windows vengono visualizzati nel campo **Consenti a utenti e/o gruppi di utenti**.

13. Fare clic su **OK**.

    Nella tabella nella scheda **Dispositivi attendibili** della finestra delle impostazioni del componente **Controllo dispositivi** viene visualizzata una riga con le impostazioni della regola per l'aggiunta dei dispositivi all'elenco dei dispositivi attendibili tramite la maschera dei relativi ID.

14. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione dell'accesso utente a un dispositivo attendibile

Per impostazione predefinita, quando si aggiunge un dispositivo all'elenco dei dispositivi attendibili, l'accesso al dispositivo è consentito a tutti gli utenti (il gruppo di utenti Everyone). È possibile configurare l'accesso degli utenti (o di gruppi di utenti) a un dispositivo attendibile.

*Per configurare l'accesso utente a un dispositivo attendibile:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo dispositivi**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo dispositivi.

3. Nella parte destra della finestra selezionare la scheda **Dispositivi attendibili**.

4. Nell'elenco dei dispositivi attendibili selezionare un dispositivo per cui modificare le regole di accesso.

5. Fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Configurazione della regola di accesso ai dispositivi attendibili**.

6. Fare clic sul pulsante **Seleziona**.

   Verrà visualizzata la finestra **Seleziona utenti e gruppi** di Microsoft Windows.

7. Nella finestra **Seleziona utenti e gruppi** di Microsoft Windows specificare gli utenti e/o i gruppi di utenti per cui Kaspersky Endpoint Security riconosce i dispositivi selezionati come attendibili.

8. Fare clic su **OK**.

   I nomi di utenti e/o gruppi di utenti specificati nella finestra **Selezionare gli utenti e/o i gruppi di utenti** di Microsoft Windows vengono visualizzati nel campo **Consenti a utenti e/o gruppi di utenti** della finestra **Configurazione della regola di accesso ai dispositivi attendibili**.

9. Fare clic su **OK**.

10. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Rimozione di un dispositivo dall'elenco dei dispositivi attendibili

*Per rimuovere un dispositivo dall'elenco dei dispositivi attendibili:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo dispositivi**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo dispositivi.

3. Nella parte destra della finestra selezionare la scheda **Dispositivi attendibili**.

4. Selezionare il dispositivo che si desidera rimuovere dall'elenco dei dispositivi attendibili.

5. Fare clic sul pulsante **Rimuovi**.

6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

Kaspersky Endpoint Security determina se concedere o meno l'accesso a un dispositivo rimosso dall'elenco dei dispositivi attendibili in base alle regole di accesso ai dispositivi e alle regole di accesso ai bus di connessione.

## 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. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo dispositivi**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo dispositivi.

3. Nella parte destra della finestra fare clic sul pulsante **Modelli**.

Verrà visualizzata la finestra **Modelli di messaggi**.

4. Eseguire una delle seguenti operazioni:

   - Per modificare il modello del messaggio relativo all'accesso bloccato al dispositivo o a un'operazione vietata con il contenuto del dispositivo, selezionare la scheda **Blocco**.

   - Per modificare il modello del messaggio inviato all'amministratore della rete LAN, selezionare la scheda **Messaggio all'amministratore**.

5. Modificare il modello di messaggio: È anche possibile utilizzare i seguenti pulsanti: **Variabile**, **Predefinito** e **Collegamento** (questo pulsante è disponibile solo nella scheda **Blocco**).

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Ottenimento dell'accesso a un dispositivo bloccato

Queste istruzioni sono destinate agli utenti di computer client in cui è installato Kaspersky Endpoint Security.

La funzionalità di Kaspersky Endpoint Security che garantisce l'accesso temporaneo a un dispositivo è disponibile solo quando Kaspersky Endpoint Security opera in base al criterio di Kaspersky Security Center e questa funzionalità è abilitata nelle impostazioni del criterio (vedere la *Guida dell'amministratore di Kaspersky Security Center*).

*Per richiedere l'accesso a un dispositivo bloccato dalla finestra delle impostazioni del componente Controllo dispositivi:*

1. Nella finestra principale dell'applicazione selezionare la scheda **Protezione e controllo**.

2. Fare clic sulla sezione **Controllo endpoint**.

   Verrà aperta la sezione **Controllo endpoint**.

3. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente Controllo dispositivi.

   Verrà visualizzato un menu per la selezione delle azioni sul componente.

4. Fare clic sul pulsante **Accesso al dispositivo**.

   Verrà visualizzata la finestra **Richiedi accesso al dispositivo**.

5. Dall'elenco dei dispositivi connessi selezionare il dispositivo a cui si desidera ottenere l'accesso.

6. Fare clic sul pulsante **Genera file della richiesta di accesso**.

   Verrà visualizzata la finestra **Creazione del file della richiesta di accesso**.

7. Nel campo **Durata accesso** specificare il periodo di tempo per cui si desidera avere accesso al dispositivo.

8. Fare clic sul pulsante **Salva**.

   Verrà visualizzata la finestra standard di Microsoft Windows **Salva file della richiesta di accesso**.

9. Nella finestra **Salva file della richiesta di accesso** di Microsoft Windows selezionare la cartella in cui salvare il file della richiesta di accesso per il dispositivo, quindi fare clic sul pulsante **Salva**.
10. Inviare il file della richiesta di accesso per il dispositivo all'amministratore della rete LAN.
11. Ottenere il file della chiave di accesso dispositivo dall'amministratore della rete LAN.
12. Nella finestra **Richiedi accesso al dispositivo** fare clic sul pulsante **Attiva chiave di accesso**.

    Verrà visualizzata la finestra standard di Microsoft Windows **Apri chiave di accesso**.
13. Nella finestra **Apri chiave di accesso** di Microsoft Windows selezionare il file della chiave di accesso dispositivo ricevuto dall'amministratore della rete LAN, quindi fare clic su **Apri**.

    Verrà visualizzata la finestra **Attivazione della chiave di accesso per il dispositivo**, che contiene informazioni sul tipo di accesso concesso.
14. Nella finestra **Attivazione della chiave di accesso per il dispositivo** fare clic su **OK**.

*Per richiedere l'accesso a un dispositivo bloccato facendo clic sul collegamento nel messaggio che informa del blocco del dispositivo:*

1. Nella finestra con il messaggio che informa che un dispositivo o un bus di connessione è stato bloccato fare clic sul collegamento **Richiedi accesso**.

   Verrà visualizzata la finestra **Creazione del file della richiesta di accesso**.
2. Nel campo **Durata accesso** specificare il periodo di tempo per cui si desidera avere accesso al dispositivo.
3. Fare clic sul pulsante **Salva**.

   Verrà visualizzata la finestra standard di Microsoft Windows **Salva file della richiesta di accesso**.
4. Nella finestra **Salva file della richiesta di accesso** di Microsoft Windows selezionare la cartella in cui salvare il file della richiesta di accesso per il dispositivo, quindi fare clic sul pulsante **Salva**.
5. Inviare il file della richiesta di accesso per il dispositivo all'amministratore della rete LAN.
6. Ottenere il file della chiave di accesso dispositivo dall'amministratore della rete LAN.
7. Nella finestra **Richiedi accesso al dispositivo** fare clic sul pulsante **Attiva chiave di accesso**.

   Verrà visualizzata la finestra standard di Microsoft Windows **Apri chiave di accesso**.
8. Nella finestra **Apri chiave di accesso** di Microsoft Windows selezionare il file della chiave di accesso dispositivo ricevuto dall'amministratore della rete LAN, quindi fare clic su **Apri**.

   Verrà visualizzata la finestra **Attivazione della chiave di accesso per il dispositivo**, che contiene informazioni sul tipo di accesso concesso.
9. Nella finestra **Attivazione della chiave di accesso per il dispositivo** fare clic su **OK**.

Il periodo di tempo per cui viene concesso l'accesso al dispositivo può essere diverso dal periodo di tempo richiesto. L'accesso al dispositivo viene concesso per il periodo di tempo specificato dall'amministratore della rete LAN al momento della generazione della chiave di accesso per il dispositivo.

# Creazione di una chiave per l'accesso a dispositivo bloccato tramite Kaspersky Security Center

Per consentire a un utente di accedere in modo temporaneo a un dispositivo bloccato, è necessaria una chiave di accesso per il dispositivo. È possibile creare una chiave di accesso utilizzando Kaspersky Security Center.

*Per creare una chiave di accesso per un dispositivo bloccato:*

1. Aprire Administration Console di Kaspersky Security Center.
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 a un dispositivo bloccato.
5. Dal menu di scelta rapida del computer selezionare **Concedi l'accesso a dispositivi e dati in modalità offline**.

   Verrà visualizzata la finestra **Concedi l'accesso a dispositivi e dati in modalità offline**.
6. Selezionare la scheda **Controllo dispositivi**.
7. Nella scheda **Controllo dispositivi** fare clic sul pulsante **Sfoglia**.

   Verrà visualizzata la finestra standard di Microsoft Windows **Seleziona il file della richiesta di accesso**.
8. Nella finestra **Seleziona il file della richiesta di accesso** selezionare il file della richiesta di accesso ricevuto dall'utente, quindi fare clic sul pulsante **Apri**.

   In **Controllo dispositivi** vengono visualizzati i dettagli del dispositivo bloccato a cui l'utente ha richiesto l'accesso.
9. Specificare il valore dell'impostazione **Durata accesso**.

   Questa impostazione definisce il periodo di tempo per cui l'utente può accedere al dispositivo bloccato. Il valore predefinito è quello specificato dall'utente durante la creazione del file della richiesta di accesso.
10. Specificare il valore dell'impostazione **Periodo di attivazione**.

    Questa impostazione definisce il periodo di tempo per cui l'utente può attivare l'accesso al dispositivo bloccato con la chiave di accesso fornita.
11. Fare clic sul pulsante **Salva**.

    Verrà visualizzata la finestra standard di Microsoft Windows **Salva chiave di accesso**.
12. Selezionare la cartella di destinazione in cui salvare il file che contiene la chiave di accesso per il dispositivo bloccato.
13. Fare clic sul pulsante **Salva**.

# Controllo Web

Questo componente è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per workstation. Il componente non è disponibile se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

Questa sezione contiene informazioni su Controllo Web e istruzioni su come configurare le impostazioni del componente.

## Informazioni su Controllo Web

Controllo Web consente di controllare le azioni degli utenti all'interno di una rete LAN, limitando o bloccando l'accesso alle risorse Web.

Una risorsa Web è una singola pagina Web, un gruppo di pagine Web, un sito Web o un gruppo di siti Web caratterizzati da una caratteristica comune.

Controllo Web fornisce le seguenti opzioni:

- Riduzione del traffico.

  Il traffico viene controllato limitando o bloccando il download di file multimediali oppure limitando o bloccando l'accesso alle risorse Web non correlate alle mansioni lavorative degli utenti.

- Delimitazione dell'accesso in base alle categorie di contenuti delle risorse Web.

  Per ridurre il traffico e le potenziali perdite associate all'utilizzo inappropriato del tempo dei dipendenti, è possibile limitare o bloccare l'accesso a specifiche categorie di risorse Web, ad esempio bloccando l'accesso alle risorse Web che appartengono alla categoria "Supporti di comunicazione Internet".

- Controllo centralizzato dell'accesso alle risorse Web.

  Quando si utilizza Kaspersky Security Center, sono disponibili impostazioni personali e di gruppo per l'accesso alle risorse Web.

Tutte le restrizioni e i blocchi applicati per l'accesso alle risorse Web vengono implementati come regole di accesso alle risorse Web.

## Abilitazione e disabilitazione di Controllo Web

Controllo Web è abilitato per impostazione predefinita. Se necessario, è possibile disabilitare Controllo Web.

È possibile abilitare o disabilitare il componente in due modi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

*Per abilitare o disabilitare Controllo Web nella scheda **Protezione e controllo** della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Controllo endpoint**.

   Verrà aperta la sezione **Controllo endpoint**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con le informazioni sul componente Controllo Web.

   Verrà visualizzato un menu per la selezione delle azioni sul componente.
5. Eseguire una delle seguenti operazioni:
   - Per abilitare il componente Controllo Web, selezionare **Avvia** dal menu.
   - Per disabilitare il componente Controllo Web, selezionare **Interrompi** dal menu.

*Per abilitare o disabilitare Controllo Web dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo Web.
3. Eseguire una delle seguenti operazioni:
   - Per abilitare Controllo Web, selezionare la casella di controllo **Abilita Controllo Web**.
   - Per disabilitare Controllo Web, deselezionare la casella di controllo **Abilita Controllo Web**.

   Se Controllo Web è disabilitato, Kaspersky Endpoint Security non controlla l'accesso alle risorse Web.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Categorie di contenuti delle risorse Web

Le categorie di contenuti delle risorse Web (di seguito denominate "categorie") elencate di seguito sono state selezionate per descrivere nel modo più completo possibile le sezioni di dati ospitate dalle risorse Web, tenendo conto delle relative caratteristiche funzionali e tematiche. L'ordine in cui vengono riportate le categorie in questo elenco non riflette l'importanza relativa o la rilevanza di tali categorie su Internet. I nomi delle categorie sono provvisori e vengono utilizzati esclusivamente per gli scopi previsti dai siti Web e dai prodotti Kaspersky. I nomi non riflettono necessariamente il significato attribuito loro dalla legge. Una risorsa Web può appartenere a più categorie contemporaneamente.

## Contenuti per adulti

Questa categoria include i seguenti tipi di risorse Web:

- Risorse Web contenenti materiali fotografici o video che rappresentano organi genitali di esseri umani o creature umanoidi, rapporti sessuali o atti di autostimolazione compiuti da esseri umani o creature umanoidi.

- Risorse Web contenenti materiali di testo, inclusi materiali letterari o artistici, che descrivono organi genitali di esseri umani o creature umanoidi, rapporti sessuali o atti di autostimolazione compiuti da esseri umani o creature umanoidi.
- Risorse Web dedicate alla discussione degli aspetti sessuali delle relazioni umane.

  Può coincidere parzialmente con la categoria "Supporti di comunicazione Internet".

- Risorse Web contenenti materiali erotici, opere che forniscono una rappresentazione realistica del comportamento sessuale degli esseri umani o opere d'arte pensate per stimolare l'eccitazione sessuale.
- Risorse Web di organi di stampa o community online ufficiali rivolte a un gruppo di destinatari ben definito, contenenti una sezione speciale e/o singoli articoli dedicati agli aspetti sessuali delle relazioni umane.
- Risorse Web dedicate alle perversioni sessuali.
- Risorse Web che pubblicizzano e vendono articoli per l'utilizzo in rapporti sessuali e per la stimolazione dell'eccitazione sessuale, servizi sessuali e incontri intimi, inclusi servizi forniti online tramite chat video di carattere erotico, "sesso telefonico", "sexting" ("sesso virtuale").
- Risorse Web con i seguenti contenuti:
  - Articoli e blog che parlano di educazione sessuale con temi scientifici e di interesse generale.
  - Enciclopedie mediche, in particolare le sezioni sulla riproduzione sessuale.
  - Risorse di istituiti medici, in particolare le sezioni che parlano di sistemi di cura degli organi sessuali.

### Software, audio, video

Questa categoria include le seguenti sottocategorie che è possibile selezionare singolarmente:

- **Audio e video**.

  Questa sottocategoria include le risorse Web che distribuiscono materiali audio e video: film, registrazioni di trasmissioni sportive, registrazioni di concerti, canzoni, filmati, video, registrazioni di tutorial audio e video e così via.

- **Torrent**.

  Questa sottocategoria include i siti Web di tracker di torrent utilizzati per condividere file di dimensioni illimitate.

- **Condivisione file**.

  Questa sottocategoria include i siti Web di condivisione file, indipendentemente dalla posizione fisica dei file distribuiti.

### Alcolici, tabacco, narcotici

Questa categoria include le risorse Web il cui contenuto è direttamente o indirettamente correlato a prodotti alcolici o contenenti alcol, prodotti con tabacco e sostanze narcotiche, psicotrope e/o inebrianti.

- Risorse Web che pubblicizzano e vendono tali sostanze e accessori per consumarle.

Può coincidere parzialmente con la categoria "Commercio elettronico".

- Risorse Web con istruzioni su come consumare o produrre sostanze narcotiche, psicotrope e/o inebrianti.

Questa categoria include le risorse Web di argomento scientifico e medico.

## Violenza

Questa categoria include le risorse Web che contengono materiali fotografici, video e di testo che rappresentano atti di violenza fisica o psicologica contro esseri umani o atti di crudeltà contro animali.

- Risorse Web che rappresentano o descrivono scene di esecuzioni, tortura o abuso, oltre a strumenti destinati a tali pratiche.

  Può coincidere parzialmente con la categoria "Armi, esplosivi, pirotecnica".

- Risorse Web che rappresentano o descrivono scene di uccisione, lotta, maltrattamento o stupro oppure scene di abuso o umiliazione contro esseri umani, animali o creature immaginarie.
- Risorse Web con informazioni che incitano ad atti che possono mettere a rischio la vita e/o la salute, inclusi autolesionismo o suicidio.
- Risorse Web con informazioni che sostengono o giustificano l'ammissibilità della violenza e/o della crudeltà oppure che incitano ad atti di violenza contro esseri umani o animali.
- Risorse Web con rappresentazioni o descrizioni particolarmente realistiche di vittime e atrocità di eventi bellici, conflitti armati e scontri militari, incidenti, catastrofi, disastri naturali, cataclismi industriali o sociali o sofferenze umane.
- Giochi per computer tramite browser con scene di violenza e crudeltà, inclusi i cosiddetti giochi di genere "shooter", "fighting", "slasher" e così via.

  Può coincidere parzialmente con la categoria "Giochi per computer".

## Armi, esplosivi, pirotecnica

Questa categoria include le risorse Web con informazioni su armi, esplosivi e prodotti pirotecnici:

- Siti Web di produttori e negozi di armi, esplosivi e prodotti pirotecnici.

  Può coincidere parzialmente con la categoria "Commercio elettronico".

- Risorse Web dedicate alla produzione o all'utilizzo di armi, esplosivi e prodotti pirotecnici.
- Risorse Web contenenti materiali analitici, storici, relativi alla produzione ed enciclopedici dedicati ad armi, esplosivi e prodotti pirotecnici.

Il termine "armi" si riferisce a congegni, articoli e strumenti atti a causare danni per la vita o la salute di esseri umani e animali e/o attrezzature e strutture atte a cagionare danni.

### Espressioni volgari

Questa categoria include le risorse Web in cui è stato rilevato un linguaggio volgare.

Può coincidere parzialmente con la categoria "Contenuti per adulti".

Questa categoria include anche le risorse Web con materiali linguistici o filologici contenenti espressioni volgari come oggetto di studio.

### Gioco d'azzardo, lotterie, scommesse

Questa categoria include le risorse Web che offrono agli utenti la possibilità di partecipare finanziariamente a giochi d'azzardo, anche se tale partecipazione finanziaria non è una condizione obbligatoria per l'accesso al sito Web. Questa categoria include le risorse Web che offrono:

- Giochi d'azzardo in cui ai partecipanti viene richiesto di contribuire in termini monetari.

  Può coincidere parzialmente con la categoria "Giochi per computer".

- Scommesse che implicano puntate di somme di denaro.
- Lotterie che implicano l'acquisto di biglietti o numeri.
- Informazioni che possono suscitare il desiderio di partecipare a giochi d'azzardo, lotterie e scommesse.

Può coincidere parzialmente con la categoria "Commercio elettronico".

Questa categoria include i giochi che consentono la partecipazione gratuita come modalità separata, oltre alle risorse Web che pubblicizzano attivamente per gli utenti risorse Web che ricadono in questa categoria.

### Comunicazioni di rete

Questa categoria include le risorse Web che consentono agli utenti (registrati o meno) di inviare messaggi personali ad altri utenti delle stesse risorse Web o di altri servizi online e/o di aggiungere contenuti (accessibili pubblicamente o in modo limitato) alle risorse Web a determinate condizioni. È possibile selezionare singolarmente le seguenti sottocategorie:

- **Chat e forum**.

Questa sottocategoria include le risorse Web destinate alla discussione pubblica di vari argomenti tramite speciali applicazioni Web, nonché le risorse Web progettate per distribuire o supportare applicazioni di messaggistica istantanea che consentono la comunicazione in tempo reale.

- **Blog**.

  Questa sottocategoria include le piattaforme per blog, ovvero i siti Web che forniscono servizi gratuiti o a pagamento per creare e gestire blog.

- **Social network**.

  Questa sottocategoria include i siti Web progettati per la creazione, la visualizzazione e la gestione di contatti tra persone, organizzazioni e istituzioni, che richiedono la registrazione di un account utente come condizione per la partecipazione.

- **Siti di incontri**.

  Questa sottocategoria include le risorse Web che offrono servizi social network a pagamento o gratuitamente.

  Può coincidere parzialmente con le categorie "Contenuti per adulti" e "Commercio elettronico".

- **E-mail basata sul Web**.

  Questa sottocategoria include pagine per l'accesso esclusivo a un servizio e-mail e pagine di cassette postali contenenti messaggi e-mail e relativi dati (ad esempio, contatti personali). Questa categoria non include le altre pagine Web di un provider di servizi Internet che offre anche un servizio e-mail.

### Acquisti online, banche e sistemi di pagamento

Questa categoria include le risorse Web progettate per qualsiasi transazione online con fondi non monetari tramite applicazioni Web specializzate. È possibile selezionare singolarmente le seguenti sottocategorie:

- **Negozi e aste**.

  Questa sottocategoria include negozi e aste online che vendono merci, lavoro o servizi a persone fisiche e/o giuridiche, inclusi siti Web di negozi che svolgono vendite esclusivamente online e profili online di negozi fisici che accettano pagamenti online.

- **Banche**.

  Questa sottocategoria include pagine Web specializzate di banche con funzionalità per operazioni bancarie online, inclusi bonifici tra conti bancari, esecuzione di depositi bancari, conversione di valute, pagamento di servizi di terze parti e così via.

- **Sistemi di pagamento**.

  Questa sottocategoria include pagine Web di sistemi e-money che forniscono l'accesso al conto personale dell'utente.

In termini tecnici, il pagamento può essere effettuato utilizzando sia carte bancarie di qualsiasi tipo (fisiche o virtuali, di debito o di credito, locali o internazionali) che e-money. Le risorse Web possono essere classificate in questa categoria indipendentemente dal fatto che dispongano o meno di aspetti tecnici quali trasmissione dei dati tramite protocollo SSL, utilizzo di autenticazione 3D Secure e così via.

### Ricerca di lavoro

Questa categoria include le risorse Web progettate per mettere in contatto datori di lavoro e persone in cerca di lavoro:

- Siti Web di agenzie di selezione del personale (uffici di collocamento e/o agenzie di head-hunting).
- Siti Web di datori di lavoro con descrizioni delle posizioni disponibili e dei relativi vantaggi.
- Portali indipendenti con offerte di impiego da datori di lavoro e agenzie di selezione del personale.
- Social network professionali che, tra l'altro, rendono possibile pubblicare o individuare informazioni su specialisti che non stanno cercando attivamente un impiego.

  Può coincidere parzialmente con la categoria "Supporti di comunicazione Internet".

## Sistemi di accesso anonimi

Questa categoria include le risorse Web che operano come intermediari per il download di contenuti da altre risorse Web utilizzando speciali applicazioni Web allo scopo di:

- Bypassare le limitazioni imposte dall'amministratore di una rete LAN per l'accesso a indirizzi Web o indirizzi IP.
- Accedere in modo anonimo a risorse Web, incluse le risorse Web che rifiutano specificamente le richieste HTTP da determinati indirizzi IP o dai relativi gruppi (ad esempio, indirizzi IP raggruppati per paese di origine).

Questa categoria include sia le risorse Web destinate esclusivamente agli scopi citati in precedenza ("strumenti per la navigazione in anonimato") che le risorse Web con funzionalità tecniche analoghe.

## Giochi per computer

Questa categoria include le risorse Web dedicate ai giochi per computer di vari generi:

- Siti Web di sviluppatori di giochi per computer.
- Risorse Web dedicate alla discussione di giochi per computer.

  Può coincidere parzialmente con la categoria "Supporti di comunicazione Internet".

- Risorse Web che forniscono capacità tecniche per la partecipazione online a giochi, insieme ad altri partecipanti o individualmente, con l'installazione di applicazioni in locale o senza tale installazione ("giochi tramite browser").
- Risorse Web progettate per pubblicizzare, distribuire e supportare software per i giochi.

  Può coincidere parzialmente con la categoria "Commercio elettronico".

## Religioni, associazioni religiose

Questa categoria include le risorse Web con materiali su movimenti pubblici, associazioni e organizzazioni con ideologie e/o culti religiosi con manifestazioni di qualsiasi tipo.

- Siti Web di organizzazioni religiose ufficiali a diversi livelli, da religioni internazionali a comunità religiose locali.
- Siti Web di società e associazioni religiose non registrate che sono emerse storicamente attraverso una scissione da un'associazione o una comunità religiosa dominante.
- Siti Web di comunità e associazioni religiose che sono emerse indipendentemente dai movimenti religiosi tradizionali, incluse quelle nate per iniziativa di uno specifico fondatore.
- Siti Web di organizzazioni interconfessionali che promuovono la cooperazione tra i rappresentanti di diverse religioni tradizionali.
- Risorse Web con materiali accademici, storici ed enciclopedici su argomenti religiosi.
- Risorse Web con rappresentazioni o descrizioni dettagliate di forme di venerazione nell'ambito di culti religiosi, inclusi riti e rituali che implicano l'adorazione di divinità, esseri e/o elementi ritenuti dotati di poteri sovrannaturali.

### Notizie

Questa categoria include le risorse Web con contenuti relativi a notizie di carattere pubblico creati da mass media o pubblicazioni online che consentono agli utenti di aggiungere notizie:

- Siti Web di organi di stampa ufficiali.
- Siti Web che offrono servizi informativi con l'attribuzione di fonti di informazioni ufficiali.
- Siti Web che offrono servizi di aggregazione, attraverso raccolte di notizie da varie fonti ufficiali e non ufficiali.
- Siti Web in cui i contenuti delle notizie sono creati dagli stessi utenti ("siti di notizie di social network").

  Può coincidere parzialmente con la categoria "Supporti di comunicazione Internet".

### Banner

Questa categoria include le risorse Web con banner. I contenuti pubblicitari dei banner possono distrarre gli utenti dalle loro attività, mentre i download dei banner aumentano la quantità di traffico.

## Informazioni sulle regole di accesso alle risorse Web

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 determinate categorie di contenuti e tipi di dati. 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 "Scenari 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.esempio.com/style.css, http://www.esempio.com/style.css?mode=normal.

- La "Regola predefinita", che consente a tutti gli utenti di accedere in qualsiasi momento a qualsiasi risorsa Web.

## Azioni con le regole di accesso alle risorse Web

È possibile eseguire le seguenti azioni sulle regole di accesso alle risorse Web:

- Aggiungere una nuova regola

- Modificare una regola

- Assegnare la priorità a una regola

  La priorità di una regola è definita dalla posizione della riga che contiene una breve descrizione della regola nella tabella delle regole di accesso disponibile nella finestra delle impostazioni del componente Controllo Web. Una regola che si trova in una posizione superiore nella tabella delle regole di accesso ha una priorità più alta di una regola che si trova in una posizione inferiore.

  Se la risorsa Web a cui l'utente tenta di accedere corrisponde ai parametri di più regole, Kaspersky Endpoint Security esegue un'azione in base alla regola con la priorità più alta.

- Verificare una regola.

  È possibile verificare la coerenza delle regole utilizzando la funzione Diagnostica regole.

- Abilitare e disabilitare una regola.

  Una regola di accesso alle risorse Web può essere abilitata *(stato dell'operazione: Attivato)*) o disabilitato (stato dell'operazione: *Disattivato*). Per impostazione predefinita, dopo la creazione, una regola è abilitata (stato dell'operazione: *Attivato)*. È possibile disabilitare la regola.

- Elimina la regola

# Aggiunta e modifica di una regola di accesso alle risorse Web

*Per aggiungere o modificare una regola di accesso alle risorse Web:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo Web.
3. Eseguire una delle seguenti operazioni:

   - Per aggiungere una regola, fare clic sul pulsante **Aggiungi**.
   - Se si desidera modificare una regola, selezionare la regola nella tabella e fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Regola di accesso alle risorse Web**.
4. Specificare o modificare le impostazioni della regola. A tale scopo:

   a. Nel campo **Nome** immettere o modificare il nome della regola.

   b. Dall'elenco a discesa **Filtro contenuto** selezionare l'opzione desiderata:

      - **Qualsiasi contenuto**.
      - **Per categorie di contenuti**.
      - **Per tipi di dati**.
      - **Per categorie di contenuti e tipi di dati**.

   c. Se è selezionata un'opzione diversa da **Qualsiasi contenuto**, vengono aperte le sezioni per selezionare le categorie di contenuti e/o tipi di dati. 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.

   d. Dall'elenco a discesa **Applica agli indirizzi** selezionare l'opzione desiderata:

      - **A tutti gli indirizzi**.
      - **A singoli indirizzi**.

   e. Se l'opzione **A singoli indirizzi** è selezionata, verrà visualizzata una sezione in cui creare un elenco di risorse Web. È possibile aggiungere o modificare gli indirizzi delle risorse Web utilizzando i pulsanti **Aggiungi**, **Modifica** ed **Elimina**.

   f. Selezionare la casella di controllo **Specificare utenti e/o gruppi**.

   g. Fare clic sul pulsante **Seleziona**.

      Verrà visualizzata la finestra **Seleziona utenti e gruppi** di Microsoft Windows.

h. Specificare o modificare l'elenco degli utenti e/o gruppi di utenti a cui consentire o bloccare l'accesso alle risorse Web descritte dalla regola.

i. Dall'elenco a discesa **Azione** selezionare l'opzione desiderata:

- **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.

j. 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:

1. Accanto all'elenco a discesa **Pianificazione regola** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Pianificazione regola**.

2. Per aggiungere alla pianificazione della regola un intervallo di tempo durante il quale la regola non viene applicata, nella tabella che mostra la pianificazione della regola fare clic sulle celle della tabella che corrispondono all'ora e al giorno della settimana che si desidera selezionare.

   Il colore delle celle diventa grigio.

3. Per sostituire un intervallo di tempo durante il quale la regola viene applicata con un intervallo di tempo durante il quale la regola non viene applicata, fare clic sulle celle grigie della tabella che corrispondono all'ora e al giorno della settimana che si desidera selezionare.

   Il colore delle celle diventa verde.

4. Fare clic sul pulsante **Salva con nome**.

   Verrà visualizzata la finestra **Nome pianificazione regola**.

5. Digitare il nome della pianificazione della regola oppure mantenere il nome predefinito suggerito.

6. Fare clic su **OK**.

5. Nella finestra **Regola di accesso alle risorse Web** fare clic su **OK**.

6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Assegnazione di priorità alle regole di accesso alle risorse Web

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. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo Web**.

Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo Web.

3. Nella parte destra della finestra selezionare la regola per cui si desidera modificare la priorità.
4. Utilizzare i pulsanti **Sposta su** e **Sposta giù** per spostare la regola nella posizione desiderata nell'elenco delle regole.
5. Ripetere i passaggi 3–4 per le regole di cui si desidera modificare la priorità.
6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo Web.
3. Nella parte destra della finestra fare clic sul pulsante **Diagnostica**.

   Verrà visualizzata la finestra **Diagnostica regole**.
4. Compilare i campi nella sezione **Condizioni**:

   a. 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.

   b. 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.

   c. Se si desidera verificare le regole utilizzate da Kaspersky Endpoint Security per controllare l'accesso alle risorse Web delle categorie di contenuti e/o tipi di dati specificate, dall'elenco a discesa **Filtro contenuto** selezionare l'opzione desiderata (**Per categorie di contenuti**, **Per tipi di dati** o **Per categorie di contenuti e tipi di dati**).

   d. 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.
5. Fare clic sul pulsante **Verifica**.

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 **Verifica**. 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.

## Abilitazione e disabilitazione di una regola di accesso alle risorse Web

*Per abilitare o disabilitare una regola di accesso alle risorse Web:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo Web.
3. Nella parte destra della finestra selezionare la regola che si desidera abilitare o disabilitare.
4. 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*.
5. Per salvare le modifiche, fare clic sul pulsante **Salva**.

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

Quando si esegue l'upgrade della versione Service Pack 1 Maintenance Release 1 o di una versione precedente dell'applicazione a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, 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 "Forum e chat", "Webmail" e "Social network" vengono migrate alla categoria di contenuti delle risorse Web "Supporti di comunicazione Internet".
- Le regole di accesso alle risorse Web basate su una o più categorie di contenuti delle risorse Web negli elenchi "Negozi online" e "Sistemi di pagamento" vengono migrate alla categoria di contenuti delle risorse Web "Commercio elettronico".
- 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.

## 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 esportare un elenco di indirizzi di risorse Web in un file:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo Web.
3. Selezionare la regola di cui si desidera esportare in un file l'elenco di indirizzi delle risorse Web.
4. Fare clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Regola di accesso alle risorse Web**.
5. Se non si desidera esportare l'intero elenco di indirizzi di risorse Web, ma solo una parte, selezionare gli indirizzi delle risorse Web desiderate.
6. A destra del campo con l'elenco di indirizzi di risorse Web fare clic sul pulsante .

   Verrà aperta una finestra di conferma dell'azione.
7. Eseguire una delle seguenti operazioni:

   - Per esportare solo gli elementi selezionati dell'elenco di indirizzi di risorse Web, nella finestra di conferma dell'azione fare clic sul pulsante **Sì**.
   - Per esportare tutti gli elementi dell'elenco di indirizzi di risorse Web, nella finestra di conferma dell'azione fare clic sul pulsante **No**.

     Verrà visualizzata la finestra standard di Microsoft Office **Salva con nome**.
8. Nella finestra **Salva con nome** di Microsoft Windows selezionare il file in cui esportare l'elenco di indirizzi di risorse Web. Fare clic sul pulsante **Salva**.

*Per importare in una regola l'elenco di indirizzi di risorse Web da un file:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo Web**.

   Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo Web.
3. Eseguire una delle seguenti operazioni:

   - Per creare una nuova regola di accesso alle risorse Web, fare clic sul pulsante **Aggiungi**.
   - Selezionare la regola di accesso alle risorse Web che si desidera modificare. Fare quindi clic sul pulsante **Modifica**.

   Verrà visualizzata la finestra **Regola di accesso alle risorse Web**.
4. Eseguire una delle seguenti operazioni:

- Se si sta creando una nuova regola di accesso alle risorse Web, selezionare **A singoli indirizzi** dall'elenco a discesa **Applica agli indirizzi**.

- Se si sta modificando una regola di accesso alle risorse Web, procedere al passaggio 5 di queste istruzioni.

5. A destra del campo con l'elenco di indirizzi di risorse Web fare clic sul pulsante .

   Se si sta creando una nuova regola, verrà visualizzata la finestra standard di Microsoft Windows **Apri file**.

   Se si sta modificando una regola, verrà visualizzata una finestra che richiede di confermare l'operazione.

6. Eseguire una delle seguenti operazioni:

   - Se si sta creando una nuova regola di accesso alle risorse Web, procedere al passaggio 7 di queste istruzioni.

   - Se si sta modificando una regola di accesso alle risorse Web, eseguire una delle seguenti operazioni nella finestra di conferma dell'azione:

     - Per aggiungere gli elementi importati dell'elenco di indirizzi di risorse Web a quelli esistenti, fare clic sul pulsante **Sì**.

     - Per eliminare gli elementi esistenti dell'elenco di indirizzi di risorse Web e aggiungere quelli importati, fare clic sul pulsante **No**.

   Verrà visualizzata la finestra **Apri file** di Microsoft Windows.

7. Nella finestra **Apri file** di Microsoft Windows selezionare un file con l'elenco di indirizzi di risorse Web da importare.

8. Fare clic sul pulsante **Apri**.

9. Nella finestra **Regola di accesso alle risorse Web** fare clic su **OK**.

## 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.esempio.com/page_0-9abcdef.html.

   Per includere il carattere `*` nella maschera di indirizzi, immettere il carattere `*` due volte.

2. La sequenza di caratteri `www.` all'inizio di una maschera di indirizzi viene interpretata come una sequenza `*.`.

   Esempio: la maschera di indirizzi www.esempio.com viene gestita come *.esempio.com.

3. Se una maschera di indirizzi non inizia con il carattere `*`, il contenuto della maschera di indirizzi è equivalente allo stesso contenuto con il prefisso `*.`.

4. Una sequenza di caratteri `*.` all'inizio di una maschera di indirizzi viene interpretata come `*.` o come una stringa vuota.

   Esempio: la maschera di indirizzi http://www.*.esempio.com include l'indirizzo http://www2.esempio.com.

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.esempio.com include indirizzi come http://www.esempio.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 esempio.com include gli indirizzi http://esempio.com e https://esempio.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://*.esempio.com include l'indirizzo http://www.esempio.com , ma non l'indirizzo https://www.esempio.com.

9. Una maschera di indirizzi tra virgolette viene trattata senza considerare alcuna sostituzione aggiuntiva, tranne il carattere `*` se è stato inizialmente incluso nella maschera di indirizzi. Le regole 5 e 7 non si applicano alle maschere di indirizzi racchiuse tra virgolette doppie (vedi gli esempi 14 - 18 nella tabella seguente).

10. Il nome utente e la password, la porta di connessione e la distinzione tra caratteri maiuscoli e minuscoli non vengono presi in considerazione durante il confronto con la maschera di indirizzi di una risorsa Web.

Esempi di utilizzo di regole per la creazione di maschere di indirizzi

| N. | Maschera di indirizzo | Indirizzo della risorsa Web da verificare | L'indirizzo è incluso nella maschera di indirizzi? | Commento |
|---|---|---|---|---|
| 1 | *.esempio.com | http://www.123esempio.com | No | Vedere la regola 1. |
| 2 | *.esempio.com | http://www.123.esempio.com | Sì | Vedere la regola 1. |
| 3 | *esempio.com | http://www.123esempio.com | Sì | Vedere la regola 1. |
| 4 | *esempio.com | http://www.123.esempio.com | Sì | Vedere la regola 1. |
| 5 | http://www.*.esempio.com | http://www.123esempio.com | No | Vedere la regola 1. |
| 6 | www.esempio.com | http://www.esempio.com | Sì | Vedere le regole 2, 1. |
| 7 | www.esempio.com | https://www.esempio.com | Sì | Vedere le regole 2, 1. |
| 8 | http://www.*.esempio.com | http://123.esempio.com | Sì | Vedere le regole 2, 4, 1. |

| | | | | |
|---|---|---|---|---|
| 9 | www.esempio.com | http://www.esempio.com/abc | Sì | Vedere le regole 2, 5, 1. |
| 10 | esempio.com | http://www.esempio.com | Sì | Vedere le regole 3, 1. |
| 11 | http://esempio.com/ | http://esempio.com/abc | Sì | Vedere la regola 6. |
| 12 | http://esempio.com/* | http://esempio.com | Sì | Vedere la regola 7. |
| 13 | http://esempio.com | https://esempio.com | No | Vedere la regola 8. |
| 14 | "esempio.com" | http://www.esempio.com | No | Vedere la regola 9. |
| 15 | "http://www.esempio.com" | http://www.esempio.com/abc | No | Vedere la regola 9. |
| 16 | "*.esempio.com" | http://www.esempio.com | Sì | Vedere le regole 1, 9. |
| 17 | "http://www.esempio.com/*" | http://www.esempio.com/abc | Sì | Vedere le regole 1, 9. |
| 18 | "www.esempio.com" | http://www.esempio.com; https://www.esempio.com | Sì | Vedere le regole 9, 8. |
| 19 | www.esempio.com/abc/123 | http://www.esempio.com/abc | No | Una maschera di indirizzo contiene più informazioni rispetto all'indirizzo di una risorsa Web. |

## 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 visualizza un messaggio di avviso se l'opzione **Avvisa** è selezionata nel menu a discesa **Azione** 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 visualizza un messaggio che segnala che una risorsa Web è stata bloccata, se l'opzione **Blocca** è selezionata nel menu a discesa **Azione** 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. Aprire la finestra delle impostazioni dell'applicazione.

2. Nel riquadro sinistro della finestra, nella sezione **Controllo endpoint**, selezionare la sottosezione **Controllo Web**.

Nella parte destra della finestra sono visualizzate le impostazioni del componente Controllo Web.

3. Nella parte destra della finestra fare clic sul pulsante **Modelli**.

   Verrà visualizzata la finestra **Modelli di messaggi**.

4. Eseguire una delle seguenti operazioni:

   - Se si desidera modificare il modello del messaggio che segnala all'utente che visitare una risorsa Web non è consigliato, selezionare la scheda **Avviso**.
   - Se si desidera modificare il modello del messaggio che informa l'utente che l'accesso a una risorsa Web è stato bloccato, selezionare la scheda **Blocco**.
   - Per modificare il modello del messaggio inviato all'amministratore, selezionare la scheda **Messaggio all'amministratore**.

5. Modificare il modello di messaggio: È anche possibile utilizzare l'elenco a discesa **Variabile** e i pulsanti **Predefinito** e **Collegamento** (questo pulsante non è disponibile nella scheda **Messaggio all'amministratore**).

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# KATA Endpoint Sensor

Le impostazioni del componente KATA Endpoint Sensor sono disponibili solo in Kaspersky Security Center Administration Console. Per utilizzare questo componente, è necessario installare il plug-in di amministrazione.

Questa sezione contiene informazioni su KATA Endpoint Sensor e istruzioni su come abilitare o disabilitare il componente.

## Informazioni su KATA Endpoint Sensor

*KATA Endpoint Sensor* è un componente di Kaspersky Anti Targeted Attack Platform. Questa soluzione è progettata per il rilevamento rapido di minacce come gli attacchi mirati.

Questo componente è installato nei computer client. In questi computer, il componente monitora continuamente i processi, le connessioni di rete attive e i file modificati, quindi passa queste informazioni a Kaspersky Anti Targeted Attack Platform.

La funzionalità del componente è disponibile con i seguenti sistemi operativi:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1.
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

Per ulteriori informazioni su Kaspersky Anti Targeted Attack Platform che non sono disponibili nel presente documento, consultare la Guida di Kaspersky Anti Targeted Attack Platform.

Le connessioni in entrata ai computer con il componente KATA Endpoint Sensor devono essere consentite direttamente dal server Kaspersky Anti Targeted Attack Platform, senza un server proxy.

## Abilitazione e disabilitazione del componente KATA Endpoint Sensor

*Per abilitare o disabilitare il componente KATA Endpoint Sensor:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera modificare le impostazioni del criterio.

3. Nell'area di lavoro selezionare la scheda **Criteri**.

4. Selezionare il criterio desiderato.

5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:

   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.

   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

6. Nella sezione **Impostazioni avanzate** selezionare la sottosezione **KATA Endpoint Sensor**.

7. Eseguire una delle seguenti operazioni:

   - Se si desidera abilitare KATA Endpoint Sensor, selezionare la casella di controllo **KATA Endpoint Sensor**.

   - Se si desidera disabilitare KATA Endpoint Sensor, deselezionare la casella di controllo **KATA Endpoint Sensor**.

8. Se è stata selezionata la casella di controllo **KATA Endpoint Sensor** durante il passaggio precedente, nel campo **Indirizzo server** specificare l'indirizzo del server Kaspersky Anti Targeted Attack Platform, che comprende le seguenti parti:

   a. Nome del protocollo

   b. Indirizzo IP o nome di dominio completo (FQDN) del server

   c. Percorso di Raccolta eventi Windows sul server

9. Fare clic su **OK**.

10. Applicare il criterio.

    Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

# Criptaggio dei dati

Se Kaspersky Endpoint Security è installato in un computer che esegue un sistema Microsoft Windows per workstation, la funzionalità di criptaggio dei dati è completamente disponibile. Se Kaspersky Endpoint Security è installato in un computer che esegue Microsoft Windows for File Servers, è disponibile solo il criptaggio del disco rigido con la tecnologia BitLocker Drive Encryption.

Questa sezione contiene informazioni sul criptaggio e il decriptaggio di dischi rigidi, unità rimovibili e file e cartelle nelle unità locali del computer. Vengono inoltre fornite istruzioni su come configurare ed eseguire il criptaggio e il decriptaggio dei dati utilizzando Kaspersky Endpoint Security e il plug-in di amministrazione di Kaspersky Endpoint Security.

Se non è possibile accedere ai dati criptati, vedere le speciali istruzioni per l'utilizzo dei dati criptati (Gestione dei file criptati con funzionalità limitate di criptaggio dei file, Utilizzo dei dispositivi criptati quando non è possibile accedervi).

## Abilitazione della visualizzazione delle impostazioni di criptaggio nel criterio di Kaspersky Security Center

*Per abilitare la visualizzazione delle impostazioni di criptaggio nel criterio di Kaspersky Security Center:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nel menu di scelta rapida del nodo **Administration Server – <Nome computer>** della struttura di Administration Console selezionare **Visualizza → Impostazioni interfaccia**.

   Verrà visualizzata la finestra **Impostazioni interfaccia**.
3. Nella finestra **Impostazioni interfaccia** selezionare la casella di controllo **Mostra criptaggio e protezione dei dati**.
4. Fare clic su **OK**.

## Informazioni sul 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.

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 del programma 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, 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 dei 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 di Kaspersky Security Center, 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.

  Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

- **Criptaggio delle 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.

  L'applicazione esegue l'azione specificata nella regola di criptaggio quando viene applicato il criterio di Kaspersky Security Center.

- **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 archivi 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 dei dischi rigidi**. È possibile selezionare una tecnologia di criptaggio: Kaspersky Disk Encryption o BitLocker Drive Encryption (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 TPM 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 dei dischi rigidi e creare un elenco di dischi rigidi da escludere dal criptaggio. Kaspersky Endpoint Security esegue il criptaggio dei dischi rigidi a livello di settore dopo l'applicazione del criterio di Kaspersky Security Center. L'applicazione cripta tutte le partizioni dei dischi rigidi contemporaneamente. Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

  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 locale tramite le attività di gestione dell'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 possibile gestire gli account per l'agente di autenticazione e utilizzare la tecnologia Single Sign-On (SSO) che consente di accedere automaticamente al sistema operativo utilizzando il nome utente e la password dell'account per l'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. Per ulteriori informazioni sul relativo utilizzo, consultare la *Guida dell'amministratore di Kaspersky Security Center*.

  > Quando si esegue l'upgrade della versione dell'applicazione a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, l'elenco degli account per l'agente di autenticazione non viene salvato.

  L'accesso alla unità criptate è possibile solo dai computer in cui è installato Kaspersky Endpoint Security con la funzionalità di criptaggio dei dischi rigidi. 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. Di conseguenza, man mano che viene eseguita la scrittura dei nuovi file nel dispositivo durante l'avvio del normale criptaggio con la funzione **Cripta solo lo spazio su disco utilizzato** attivata nel computer, tutti i settori risulteranno criptati dopo un certo periodo di tempo.

I dati necessari per decriptare i file vengono forniti dall'Administration Server di Kaspersky Security Center che controllava il computer al momento del criptaggio. Se il computer con i file criptati per qualsiasi motivo si trova sotto il controllo di un altro Administration Server e non è mai stato eseguito l'accesso ai file criptati, è possibile ottenere l'accesso in uno dei modi seguenti:

- Richiedere l'accesso agli oggetti criptati all'amministratore della rete LAN.
- Ripristinare i dati nei dispositivi criptati utilizzando l'utilità di ripristino.
- Ripristinare la configurazione dell'Administration Server di Kaspersky Security Center 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.

L'applicazione crea file di servizio durante il criptaggio. Per archiviarli è necessario il 2-3% circa dello spazio non frammentato disponibile sul disco rigido. Se lo spazio non frammentato disponibile sul disco rigido è insufficiente, il criptaggio non verrà avviato finché non viene liberato spazio sufficiente.

La compatibilità tra la funzionalità di criptaggio di Kaspersky Endpoint Security e Kaspersky Anti-Virus for UEFI non è supportata. Il criptaggio dei dischi rigidi dei computer in cui è installato Kaspersky Anti-Virus for UEFI rende inutilizzabile Kaspersky Anti-Virus for UEFI.

## Limitazioni della funzionalità di criptaggio

La creazione di nuove partizioni nei dischi rigidi criptati e la formattazione di partizioni esistenti dei dischi rigidi criptati può determinare la perdita dei dati in tali dischi rigidi.

Il criptaggio dei dischi rigidi con la tecnologia Kaspersky Disk Encryption non è disponibile per i dischi rigidi che non soddisfano i requisiti hardware e software.

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.
- 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 quattro partizioni estese.
- File di scambio in 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 2% 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.

## Modifica dell'algoritmo di criptaggio

L'algoritmo di criptaggio utilizzato da Kaspersky Endpoint Security per il criptaggio dei dati dipende dalle librerie di criptaggio incluse nel kit di distribuzione.

*Per modificare l'algoritmo di criptaggio:*

1. Decriptare gli oggetti criptati da Kaspersky Endpoint Security prima di iniziare a modificare l'algoritmo di criptaggio.

   Dopo avere modificato l'algoritmo di criptaggio, gli oggetti precedentemente criptati diventano non disponibili.

2. Rimuovere Kaspersky Endpoint Security.
3. Installare Kaspersky Endpoint Security dal kit di distribuzione che contiene le librerie di criptaggio per i diversi numeri di bit.

## Abilitazione della tecnologia Single Sign-On (SSO)

La tecnologia Single Sign-On (SSO) è incompatibile con i fornitori di terzi di credenziali di account.

*Per abilitare la tecnologia Single Sign-On (SSO):*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera abilitare la tecnologia Single Sign-On (SSO).
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Impostazioni di criptaggio generali**.

7. Nella sottosezione **Impostazioni di criptaggio generali** fare clic sul pulsante **Configura** nella sezione **Impostazioni password**.

   Verrà aperta la scheda **Agente di autenticazione** della finestra **Impostazioni password di criptaggio**.

8. Selezionare la casella di controllo **Utilizza la tecnologia SSO (Single Sign-On)**.

9. Fare clic su **OK**.

10. Per salvare le modifiche, nella finestra **Proprietà: <Nome criterio>** fare clic su **OK**.

11. Applicare il criterio.

    Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

## Considerazioni speciali sul criptaggio dei file

Quando si utilizza la funzionalità di criptaggio dei file, tenere presenti i seguenti aspetti:

- Il criterio di Kaspersky Security Center 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 criptaggio/decriptaggio alle 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.

- Kaspersky Endpoint Security cripta/decripta i file nelle cartelle predefinite solo per i profili utente locali del sistema operativo. Kaspersky Endpoint Security non cripta/decripta i file nelle cartelle predefinite di profili utente mobili, profili utente bloccati, profili utente temporanei e cartelle reindirizzate. L'elenco delle cartelle standard consigliate da Kaspersky per il criptaggio include le seguenti cartelle:

  - Documenti
  - Preferiti
  - Cookie
  - Desktop
  - File temporanei di Internet Explorer
  - File temporanei
  - File di Outlook

- Kaspersky Endpoint Security non esegue il criptaggio di file e cartelle quando tale operazione 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%, %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 un'attività di criptaggio di file e cartelle.

- 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 dei file nelle unità locali del computer

Il criptaggio dei file nelle unità locali del computer è disponibile se Kaspersky Endpoint Security è installato in un computer con un sistema operativo Microsoft Windows per workstation. Il criptaggio dei file nelle unità locali del computer non è disponibile se Kaspersky Endpoint Security è installato in un computer con un sistema operativo Microsoft Windows per file server.

In questa sezione viene descritto il criptaggio dei file nelle unità locali del computer e vengono fornite istruzioni su come configurare ed eseguire il criptaggio dei file nelle unità locali del computer con Kaspersky Endpoint Security e il plug-in della console di Kaspersky Endpoint Security.

## Criptaggio dei file nelle unità locali del computer

*Per criptare i file nelle unità locali:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare il criptaggio dei file nelle unità locali.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio di file e cartelle**.
7. Nella parte destra della finestra selezionare la scheda **Criptaggio**.
8. Nell'elenco a discesa **Modalità di criptaggio** selezionare la voce **Regole predefinite**.
9. 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.

   Verrà visualizzata la finestra **Seleziona cartelle predefinite**.

b. Selezionare l'elemento **Cartella personalizzata** per aggiungere a una regola di criptaggio il percorso di una cartella immesso manualmente.

   Verrà visualizzata la finestra **Aggiungi cartella personalizzata**.

c. Selezionare l'elemento **File per estensione** per aggiungere 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.

   Verrà visualizzata la finestra **Aggiungi/modifica elenco di estensioni di file**.

d. Selezionare l'elemento **File per gruppo di estensioni** per aggiungere gruppi di estensioni di file a una regola di criptaggio. Kaspersky Endpoint Security cripta i file con le estensioni elencate nei gruppi di estensioni in tutte le unità locali del computer.

   Verrà visualizzata la finestra **Seleziona gruppi di estensioni di file**.

10. Per salvare le modifiche, nella finestra **Proprietà: <Nome criterio>** fare clic su **OK**.

11. Applicare il criterio.

    Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

Non appena il criterio viene applicato, Kaspersky Endpoint Security cripta i file inclusi nella regola di criptaggio e non inclusi nella regola di decriptaggio.

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.

Kaspersky Endpoint Security cripta i file non criptati se le relative proprietà (percorso del file / nome del file / estensione del file) soddisfano comunque i criteri della regola di criptaggio dopo la modifica.

Kaspersky Endpoint Security rimanda il criptaggio dei file aperti finché non vengono chiusi.

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.

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.

## 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 Administration Console di Kaspersky Security Center.

2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare le regole di accesso ai file criptati per le applicazioni.

3. Nell'area di lavoro selezionare la scheda **Criteri**.

4. Selezionare il criterio desiderato.

5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:

   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio di file e cartelle**.

7. Nell'elenco a discesa **Modalità di criptaggio** selezionare la voce **Regole predefinite**.

   Le regole di accesso sono applicate solo nella modalità **Regole predefinite**. Dopo avere applicato le regole di accesso nella modalità **Regole predefinite**, 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.

8. Nella parte destra della finestra selezionare la scheda **Regole per le applicazioni**.

9. 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**.

   Verrà visualizzata la finestra **Aggiungi applicazioni dall'elenco di Kaspersky Security Center**.

   Eseguire le seguenti operazioni:

   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 nella sezione **Gruppo**.

   b. Fare clic sul pulsante **Aggiorna**.

      Nella tabella verranno elencate le applicazioni che corrispondono ai filtri applicati.

   c. Nella colonna **Applicazioni** selezionare le caselle di controllo accanto alle applicazioni per cui si desidera creare le regole di accesso ai file criptati.

   d. Nell'elenco a discesa **Regola per le applicazioni** selezionare la regola che determinerà l'accesso delle applicazioni ai file criptati.

   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 accesso ai file criptati create in precedenza per tali applicazioni.

   f. Fare clic su **OK**.

   I dettagli di una regola di accesso ai file criptati per le applicazioni vengono visualizzati nella tabella nella scheda **Regole per le applicazioni**.

10. Se si desidera selezionare manualmente le applicazioni, fare clic sul pulsante **Aggiungi** e selezionare nell'elenco a discesa l'elemento **Applicazioni personalizzate**.

    Verrà visualizzata la finestra **Aggiungi/modifica i nomi dei file eseguibili delle applicazioni**.

    Eseguire le seguenti operazioni:

    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.

d. Fare clic su **OK**.

I dettagli di una regola di accesso ai file criptati per le applicazioni vengono visualizzati nella tabella nella scheda **Regole per le applicazioni**.

11. Fare clic su **OK** per 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 Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare il criptaggio dei file creati da applicazioni specifiche.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio di file e cartelle**.
7. Nell'elenco a discesa **Modalità di criptaggio** selezionare la voce **Regole predefinite**.

   Le regole di criptaggio sono applicate solo nella modalità **Regole predefinite**. Dopo avere applicato le regole di criptaggio nella modalità **Regole predefinite**, 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.

8. Nella parte destra della finestra selezionare la scheda **Regole per le applicazioni**.

9. 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**.

   Verrà visualizzata la finestra **Aggiungi applicazioni dall'elenco di Kaspersky Security Center**.

   Eseguire le seguenti operazioni:

   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 nella sezione **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 è necessario 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.

   f. Fare clic su **OK**.

   Le informazioni sulla regola di criptaggio per i file creati o modificati dalle applicazioni selezionate vengono visualizzate nella tabella nella scheda **Regole per le applicazioni**.

10. Se si desidera selezionare manualmente le applicazioni, fare clic sul pulsante **Aggiungi** e selezionare nell'elenco a discesa l'elemento **Applicazioni personalizzate**.

    Verrà visualizzata la finestra **Aggiungi/modifica i nomi dei file eseguibili delle applicazioni**.

    Eseguire le seguenti operazioni:

    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**.

    d. Fare clic su **OK**.

    Le informazioni sulla regola di criptaggio per i file creati o modificati dalle applicazioni selezionate vengono visualizzate nella tabella nella scheda **Regole per le applicazioni**.

11. Fare clic su **OK** per salvare le modifiche.

## Generazione di una regola di decriptaggio

*Per generare una regola di decriptaggio:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera generare un elenco di file da decriptare.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio di file e cartelle**.
7. Nella parte destra della finestra selezionare la scheda **Decriptaggio**.
8. Nell'elenco a discesa **Modalità di criptaggio** selezionare la voce **Regole predefinite**.
9. 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.
      Verrà visualizzata la finestra **Seleziona cartelle predefinite**.
   b. Selezionare l'elemento **Cartella personalizzata** per aggiungere a una regola di decriptaggio il percorso di una cartella immesso manualmente.
      Verrà visualizzata la finestra **Aggiungi cartella personalizzata**.
   c. Selezionare l'elemento **File per estensione** per aggiungere 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.
      Verrà visualizzata la finestra **Aggiungi/modifica elenco di estensioni di file**.
   d. Selezionare l'elemento **File per gruppo di estensioni** per aggiungere gruppi di estensioni di file a una regola di decriptaggio. Kaspersky Endpoint Security non cripta i file con le estensioni elencate nei gruppi di estensioni in tutte le unità locali dei computer.
      Verrà visualizzata la finestra **Seleziona gruppi di estensioni di file**.
10. Per salvare le modifiche, nella finestra **Proprietà: <Nome criterio>** fare clic su **OK**.
11. Applicare il criterio.
    Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

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 Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare il decriptaggio dei file nelle unità locali.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio di file e cartelle**.
7. Nella parte destra della finestra selezionare la scheda **Criptaggio**.
8. 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**.

   È possibile eliminare diversi elementi dall'elenco di criptaggio contemporaneamente. A tale scopo, tenendo premuto il tasto **CTRL** fare clic sui file desiderati per selezionarli e 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.
9. Creare un elenco di decriptaggio dei file.
10. Per salvare le modifiche, nella finestra **Proprietà: <Nome criterio>** fare clic su **OK**.
11. Applicare il criterio.

Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

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

Kaspersky Endpoint Security non esegue la compressione dei file durante la creazione di un pacchetto criptato.

*Per creare un pacchetto criptato:*

1. In un computer in cui è installato Kaspersky Endpoint Security ed è abilitata la funzionalità di criptaggio utilizzare qualsiasi programma di gestione dei file per selezionare i file e/o le cartelle che si desidera aggiungere a un pacchetto criptato. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.

2. Dal menu di scelta rapida selezionare **Aggiungi a pacchetto criptato**.

   Verrà visualizzata la finestra di dialogo standard di Microsoft Windows **Scegliere il percorso in cui salvare il pacchetto criptato**.

3. Nella finestra di dialogo standard di Microsoft Windows **Scegliere il percorso in cui salvare il pacchetto criptato** selezionare una destinazione per il salvataggio del pacchetto criptato nell'unità rimovibile. Fare clic sul pulsante **Salva**.

   Verrà visualizzata la finestra **Aggiungi a pacchetto criptato**.

4. Nella finestra **Aggiungi a pacchetto criptato** digitare e confermare una password.

5. Fare clic sul pulsante **Crea**.

   Verrà avviato il processo di creazione del pacchetto criptato. Al termine del processo, verrà creato un pacchetto criptato autoestraente protetto da password nella cartella di destinazione selezionata nell'unità rimovibile.

Se si annulla la creazione di un pacchetto criptato, Kaspersky Endpoint Security esegue le seguenti operazioni:

1. Termina i processi di copia dei file nel pacchetto e qualsiasi eventuale operazione di criptaggio del pacchetto in corso.

2. Rimuove tutti i file temporanei creati durante il processo di creazione e criptaggio del pacchetto e il file del pacchetto criptato stesso.

3. Segnala all'utente che il processo di creazione del pacchetto criptato è stato terminato.

## Estrazione di pacchetti criptati

*Per estrarre un pacchetto criptato:*

1. In qualsiasi programma per la gestione dei file selezionare un pacchetto criptato. Fare clic per avviare la procedura guidata di decompressione.

   Verrà visualizzata la finestra **Immettere la password**.

2. Immettere la password utilizzata per proteggere il pacchetto criptato.

3. Nella finestra **Immettere la password** fare clic su **OK**.

   Se la password viene immessa correttamente, verrà visualizzata la finestra di dialogo standard **Sfoglia** di Microsoft Windows.

4. Nella finestra di dialogo standard **Sfoglia** di Microsoft Windows selezionare la cartella di destinazione per l'estrazione del pacchetto criptato, quindi fare clic su **OK**.

Verrà avviato il processo di estrazione del pacchetto criptato nella cartella di destinazione.

Se il pacchetto criptato è stato estratto in precedenza nella cartella di destinazione specificata, i file esistenti nella cartella verranno sovrascritti dai file nel pacchetto criptato.

Se si annulla l'estrazione di un pacchetto criptato, Kaspersky Endpoint Security esegue le seguenti operazioni:

1. Interrompe il processo di decriptaggio del pacchetto e termina qualsiasi eventuale operazione di copia dei file dal pacchetto criptato in corso.
2. Elimina tutti i file temporanei creati nel corso del decriptaggio e dell'estrazione del pacchetto criptato, nonché tutti i file già copiati dal pacchetto criptato nella cartella di destinazione.
3. Segnala all'utente che il processo di estrazione del pacchetto criptato è stato terminato.

## Criptaggio delle unità rimovibili

Il criptaggio delle unità rimovibili è disponibile se Kaspersky Endpoint Security è installato in un computer con un sistema operativo Microsoft Windows per workstation. Il criptaggio dei file delle unità rimovibili non è disponibile se Kaspersky Endpoint Security è installato in un computer con un sistema operativo Microsoft Windows per file server.

Questa sezione contiene informazioni sul criptaggio delle unità rimovibili e istruzioni su come configurare ed eseguire il criptaggio delle unità rimovibili utilizzando Kaspersky Endpoint Security e il plug-in di amministrazione di Kaspersky Endpoint Security.

## Avvio del criptaggio delle unità rimovibili

*Per criptare le unità rimovibili:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare il criptaggio delle unità rimovibili.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio delle unità rimovibili**.

7. Nell'elenco a discesa **Modalità di criptaggio** selezionare l'azione predefinita che deve essere eseguita da Kaspersky Endpoint Security su tutte le unità rimovibili connesse ai computer del gruppo di amministrazione selezionato:

   - **Cripta intera unità rimovibile**. Se questa opzione è selezionata, quando viene applicato il criterio di Kaspersky Security Center con le impostazioni di criptaggio specificate per le unità rimovibili, Kaspersky Endpoint Security cripta il contenuto delle unità rimovibili a livello di settore. Come risultato, l'applicazione cripta non solo i file archiviati nelle unità rimovibili, ma anche i file system delle unità rimovibili, inclusi i nomi di file e le strutture di cartelle. Kaspersky Endpoint Security non cripta nuovamente le unità già criptate.

     Questo scenario di criptaggio è reso possibile dalla funzionalità di criptaggio dei dischi rigidi di Kaspersky Endpoint Security.

   - **Cripta tutti i file**. Se questa opzione è selezionata, quando viene applicato il criterio di Kaspersky Security Center 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 cripta nuovamente i file già criptati. L'applicazione non cripta i file system delle unità rimovibili, inclusi i nomi dei file criptati e le strutture di cartelle.

   - **Cripta solo i nuovi file**. Se questa opzione è selezionata, quando viene applicato il criterio di Kaspersky Security Center con le impostazioni di criptaggio specificate per le unità rimovibili, Kaspersky Endpoint Security cripta solo i file aggiunti alle unità rimovibili o archiviati nelle unità rimovibili e modificati dopo l'ultima applicazione del criterio di Kaspersky Security Center.

   - **Decripta intera unità rimovibile**. Se questa opzione è selezionata, quando viene applicato il criterio di Kaspersky Security Center 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.

     Questo scenario di criptaggio è reso possibile dalle funzionalità di criptaggio dei file e dei dischi rigidi offerte da Kaspersky Endpoint Security.

   - **Mantieni invariato**. Se questa opzione è selezionata, quando viene applicato il criterio di Kaspersky Security Center con le impostazioni di criptaggio specificate per le unità rimovibili, Kaspersky Endpoint Security non cripta o decripta i file nelle unità rimovibili.

8. Creare le regole di criptaggio per i file nelle unità rimovibili di cui si desidera criptare il contenuto.

9. Applicare il criterio.

Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

Non appena viene applicato il criterio, quando un utente connette un'unità rimovibile o se un'unità rimovibile è già connessa, Kaspersky Endpoint Security segnala all'utente che l'unità rimovibile è soggetta a una regola di criptaggio per cui i dati archiviati nell'unità rimovibile verranno criptati.

Se è specificata la regola *Mantieni invariato* per il criptaggio dei dati in un'unità rimovibile, l'applicazione non visualizza all'utente alcuna notifica.

L'applicazione segnala all'utente che il processo di criptaggio può richiedere un certo tempo.

L'applicazione richiede all'utente di confermare l'operazione di criptaggio ed esegue le seguenti azioni:

- Cripta i dati in base alle impostazioni del criterio, se l'utente accetta di eseguire il criptaggio.
- Mantiene i dati non criptati se l'utente rifiuta il criptaggio e consente di accedere in sola lettura ai file nell'unità rimovibile.
- Mantiene i dati non criptati se l'utente ignora la richiesta di conferma del criptaggio, consente di accedere in sola lettura ai file nell'unità rimovibile e richiede nuovamente all'utente di confermare il criptaggio dai dati alla successiva applicazione del criterio di Kaspersky Security Center o alla connessione di un'unità rimovibile.

Il criterio di Kaspersky Security Center con le impostazioni preimpostate per il criptaggio dei dati nelle unità rimovibili viene creato per uno specifico gruppo di computer gestiti. Di conseguenza, il risultato del criptaggio dei dati nelle unità rimovibili dipende dal computer a cui è connessa l'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.

Se il criptaggio di un'unità rimovibile non è riuscito, 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.

## Aggiunta di una regola di criptaggio per le unità rimovibili

*Per aggiungere una regola di criptaggio per le unità rimovibili:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera aggiungere le regole di criptaggio delle unità rimovibili.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio delle unità rimovibili**.
7. 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**.

     Verrà visualizzata la finestra **Aggiungi dispositivi dall'elenco dei dispositivi attendibili**.
   - 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**.

     Verrà visualizzata la finestra **Aggiungi dispositivi dall'elenco di Kaspersky Security Center**.

8. Se è stato selezionato **Dall'elenco di dispositivi di Kaspersky Security Center** durante il passaggio precedente, specificare i filtri per visualizzare i dispositivi nella tabella. A tale scopo:

   a. Specificare i valori dei seguenti parametri: **Visualizza nella tabella i dispositivi per cui sono definiti i seguenti elementi**, **Tipo di dispositivo**, **Nome**, **Computer** e **Kaspersky Disk Encryption**.

   b. Fare clic sul pulsante **Aggiorna**.

9. Nella colonna **Tipo di dispositivo** selezionare le caselle di controllo accanto ai nomi delle unità rimovibili per cui si desidera creare le regole di criptaggio.

10. 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.

11. 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.

12. 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.

13. 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**.

14. Fare clic su **OK**.

    Le righe con i parametri delle regole di criptaggio create vengono visualizzate nella tabella **Regole personalizzate**.

15. Fare clic su **OK** per salvare le modifiche.

Le regole di criptaggio delle unità rimovibili aggiunte sono applicate alle unità rimovibili connesse a qualsiasi computer controllato dal criterio di Kaspersky Security Center modificato.

## Modifica di una regola di criptaggio per le unità rimovibili

*Per modificare una regola di criptaggio per un'unità rimovibile:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera modificare una regola di criptaggio delle unità rimovibili.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio delle unità rimovibili**.
7. Nell'elenco delle unità rimovibili per cui sono state configurate regole di criptaggio selezionare la voce corrispondente all'unità rimovibile desiderata.
8. Fare clic sul pulsante **Imposta una regola** per modificare la regola di criptaggio per l'unità rimovibile selezionata.
   Verrà visualizzato il menu di scelta rapida del pulsante **Imposta una regola**.
9. Nel menu di scelta rapida del pulsante **Imposta una regola** selezionare l'azione che deve essere eseguita da Kaspersky Endpoint Security sui file archiviati nell'unità rimovibile selezionata.
10. Fare clic su **OK** per salvare le modifiche.

Le regole di criptaggio delle unità rimovibili modificate sono applicate alle unità rimovibili connesse a qualsiasi computer controllato dal criterio di Kaspersky Security Center modificato.

## Abilitazione della modalità portatile per l'accesso ai file criptati nelle unità rimovibili

*Per abilitare la modalità portatile per l'accesso ai file criptati nelle unità rimovibili:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera abilitare la modalità portatile per l'accesso ai file criptati nelle unità rimovibili.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio delle unità rimovibili**.

7. Selezionare la casella di controllo **Modalità portatile**.

   La modalità portatile è disponibile per il criptaggio di tutti i file o solo dei nuovi file.

8. Fare clic su **OK**.

9. Applicare il criterio.

   Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

10. Connettere l'unità rimovibile a un dispositivo a cui è stato applicato il criterio di Kaspersky Security Center.

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. Fare clic su **OK**.

    Kaspersky Endpoint Security cripta i file in un'unità rimovibile in base alle regole di criptaggio definite nel criterio di Kaspersky Security Center. Nell'unità rimovibile viene inoltre copiato Portable File Manager per l'utilizzo dei file criptati.

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.

## Decriptaggio delle unità rimovibili

*Per decriptare le unità rimovibili:*

1. Aprire Administration Console di Kaspersky Security Center.

2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare il decriptaggio delle unità rimovibili.

3. Nell'area di lavoro selezionare la scheda **Criteri**.

4. Selezionare il criterio desiderato.

5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:

   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio delle unità rimovibili**.

7. Per decriptare tutti i file criptati archiviati nelle unità rimovibili, dall'elenco a discesa **Modalità di criptaggio** selezionare **Decripta intera unità rimovibile**.

8. 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.

Verrà visualizzato il menu di scelta rapida del pulsante **Imposta una regola**.

c. Selezionare la voce **Decripta tutti i file** nel menu di scelta rapida del pulsante **Imposta una regola**.

9. Fare clic su **OK** per salvare le modifiche.

10. Applicare il criterio.

Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

Dopo l'applicazione del criterio, quando l'utente connette un'unità rimovibile o se un'unità rimovibile è già connessa, Kaspersky Endpoint Security segnala all'utente che l'unità rimovibile è soggetta a una regola di criptaggio per cui i file criptati archiviati nell'unità rimovibile e il file system dell'unità rimovibile (se criptato) verranno decriptati. L'applicazione segnala all'utente che il processo di decriptaggio può richiedere un certo tempo.

Il criterio di Kaspersky Security Center con le impostazioni preimpostate per il criptaggio dei dati nelle unità rimovibili viene creato per uno specifico gruppo di computer gestiti. Di conseguenza, il risultato del decriptaggio dei dati nelle unità rimovibili dipende dal computer a cui è connessa l'unità rimovibile.

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.

Se il decriptaggio di un'unità rimovibile non è riuscito, 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.

## Criptaggio dei dischi rigidi

Se Kaspersky Endpoint Security è installato in un computer che esegue Microsoft Windows for Workstations, le tecnologie BitLocker Drive Encryption e Kaspersky Disk Encryption sono disponibili per criptaggio. Se Kaspersky Endpoint Security è installato in un computer che esegue Microsoft Windows for File Servers, è disponibile solo la tecnologia BitLocker Drive Encryption.

Questa sezione contiene informazioni sul criptaggio dei dischi rigidi e istruzioni su come configurare ed eseguire il criptaggio dei dischi rigidi con Kaspersky Endpoint Security e il plug-in della console di Kaspersky Endpoint Security.

## Informazioni sul criptaggio dei dischi rigidi

Prima di avviare il criptaggio dei dischi rigidi, l'applicazione esegue una serie di controlli per stabilire se il dispositivo può essere criptato. I controlli includono la verifica della compatibilità dei dischi rigidi del sistema con l'agente di autenticazione e 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 del disco rigido 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 dei dischi rigidi 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 dei dischi rigidi 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 dei dischi rigidi, Kaspersky Endpoint Security cripta tutti i dati presenti nei dischi.

Se l'utente arresta o riavvia il computer durante il decriptaggio dei dischi rigidi, l'agente di autenticazione viene caricato prima del successivo avvio del sistema operativo. Kaspersky Endpoint Security riprende il criptaggio 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 criptaggio dei dischi rigidi, l'agente di autenticazione viene caricato all'uscita del sistema operativo dalla modalità di ibernazione. Kaspersky Endpoint Security riprende il criptaggio 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 sospensione durante il criptaggio dei dischi rigidi, Kaspersky Endpoint Security riprende il criptaggio dei dischi rigidi 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'agente di autenticazione supporta i layout di tastiera per le seguenti lingue:

- Inglese (Regno Unito)
- Inglese (Stati Uniti)
- Arabo (Algeria, Marocco, Tunisia; layout AZERTY)
- Spagnolo (America latina)
- Italiano
- Tedesco (Germania e Austria)
- Tedesco (Svizzera)

- Portoghese (Brasile, layout ABNT2)
- Russo (per tastiere IBM/WINDOWS a 105 tasti con layout QWERTY)
- Turco (layout QWERTY)
- Francese (Francia)
- Francese (Svizzera)
- Francese (Belgio, layout AZERTY)
- Giapponese (per tastiere a 106 tasti con layout QWERTY)

Un layout di tastiera diventa disponibile nell'agente di autenticazione se il layout è stato aggiunto nelle impostazioni della lingua e delle impostazioni internazionali del sistema operativo e risulta disponibile nella schermata di accesso a Microsoft Windows.

Se il nome dell'account per l'agente di autenticazione contiene simboli che non possono essere immessi utilizzando i layout di tastiera disponibili nell'agente di autenticazione, è possibile accedere ai dischi rigidi criptati solo dopo che ne è stato eseguito il ripristino tramite l'utilità di ripristino o dopo avere eseguito il ripristino del nome e della password dell'account per l'agente di autenticazione.

Kaspersky Endpoint Security supporta i seguenti token, lettori di smart card e smart card:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (smart card)
- SafeNet eToken 4100 72K Java (smart card)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (smart card)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (lettore)

- Gemalto IDPrime .NET 511

## Criptaggio dei dischi rigidi tramite la tecnologia Kaspersky Disk Encryption

Prima di criptare i dischi rigidi in un computer, è consigliabile verificare che il computer non sia infetto. A tale scopo, avviare l' attività Scansione Completa o Scansione delle aree critiche. Il criptaggio del disco rigido di un computer infetto da un rootkit può rendere inutilizzabile il sistema.

*Per criptare i dischi rigidi tramite la tecnologia Kaspersky Disk Encryption:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare il criptaggio dei dischi rigidi.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio dei dischi rigidi**.
7. Nell'elenco a discesa **Tecnologia di criptaggio** selezionare l'opzione **Kaspersky Disk Encryption**.

   La tecnologia Kaspersky Disk Encryption non può essere utilizzata se il computer dispone di dischi rigidi criptati tramite BitLocker.

8. Nell'elenco a discesa **Modalità di criptaggio** selezionare **Cripta tutti i dischi rigidi**.

   Se è necessario escludere alcuni dischi rigidi dal criptaggio, creare un elenco di tali dischi rigidi.

9. Selezionare uno dei seguenti metodi di criptaggio:
   - Se si desidera applicare il criptaggio solo ai settori del disco rigido che sono occupati da file, selezionare la casella di controllo **Cripta solo lo spazio su disco utilizzato**.

     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 si desidera applicare il criptaggio all'intero disco rigido, deselezionare la casella di controllo **Cripta solo lo spazio su disco utilizzato**.

Questa funzione è applicabile solo ai dispositivi non criptati. 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 tutti i dischi rigidi**, i settori che non sono occupati da file non saranno criptati.

10. Fare clic su **OK** per salvare le modifiche.

11. Applicare il criterio.

    Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

## Criptaggio dei dischi rigidi tramite la tecnologia BitLocker Drive Encryption

Prima di criptare i dischi rigidi in un computer, è consigliabile verificare che il computer non sia infetto. A tale scopo, avviare l' attività Scansione Completa o Scansione delle aree critiche. Il criptaggio del disco rigido di un computer infetto da un rootkit può rendere inutilizzabile il sistema.

L'utilizzo della tecnologia BitLocker Drive Encryption nei computer con un sistema operativo server può richiedere l'installazione del componente **BitLocker Drive Encryption** tramite la procedura guidata per l'aggiunta di ruoli e componenti.

*Per eseguire il criptaggio dei dischi rigidi tramite la tecnologia BitLocker Drive Encryption:*

1. Aprire Administration Console di Kaspersky Security Center.

2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare il criptaggio dei dischi rigidi.

3. Nell'area di lavoro selezionare la scheda **Criteri**.

4. Selezionare il criterio desiderato.

5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:

   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.

   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio dei dischi rigidi**.

7. Nell'elenco a discesa **Tecnologia di criptaggio** selezionare l'opzione **BitLocker Drive Encryption**.

8. Nell'elenco a discesa **Modalità di criptaggio** selezionare l'opzione **Cripta tutti i dischi rigidi**.

9. Se si desidera utilizzare una tastiera touchscreen per l'immissione di informazioni in un ambiente di preavvio, selezionare la casella di controllo **Consenti l'utilizzo dell'autenticazione tramite input da tastiera prima dell'avvio nei tablet**.

È consigliabile utilizzare questa impostazione solo per i dispositivi dotati di strumenti alternativi per l'input dei dati, ad esempio una tastiera USB in un ambiente di preavvio.

10. Selezionare uno dei seguenti tipi di criptaggio:

    - Se si desidera utilizzare il criptaggio hardware, selezionare la casella di controllo **Usa criptaggio hardware**.
    - Se si desidera utilizzare il criptaggio software, deselezionare la casella di controllo **Usa criptaggio hardware**.

11. Selezionare uno dei seguenti metodi di criptaggio:

    - Se si desidera applicare il criptaggio solo ai settori del disco rigido che sono occupati da file, selezionare la casella di controllo **Cripta solo lo spazio su disco utilizzato**.
    - Se si desidera applicare il criptaggio all'intero disco rigido, deselezionare la casella di controllo **Cripta solo lo spazio su disco utilizzato**.

    Questa funzione è applicabile solo ai dispositivi non criptati. 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 tutti i dischi rigidi**, i settori che non sono occupati da file non saranno criptati.

12. Selezionare un metodo per l'accesso ai dischi rigidi criptati con BitLocker.

    - Se si desidera utilizzare un TPM (Trusted Platform Module) per archiviare le chiavi di criptaggio, selezionare l'opzione **Usa Trusted Platform Module (TPM)**.
    - Se non si utilizza un TPM per il criptaggio dei dischi rigidi, selezionare l'opzione **Usa password** e specificare il numero minimo di caratteri per la password nel campo **Lunghezza minima password**.

    La disponibilità di un TPM è obbligatoria per i sistemi operativi Windows 7 e Windows 2008 R2, oltre che per le versioni precedenti.

13. Se è stata selezionata l'opzione **Usa Trusted Platform Module (TPM)** durante il passaggio precedente:

    - Se si desidera impostare un codice PIN che sarà richiesto quando l'utente tenta di accedere a una chiave di criptaggio, selezionare la casella di controllo **Usa PIN** e nel campo **Lunghezza minima PIN** specificare il numero minimo di cifre per il codice PIN.
    - Se si desidera accedere tramite una password ai dischi rigidi criptati senza un TPM sul computer, selezionare la casella di controllo **Usa password se Trusted Platform Module (TPM) non è disponibile** e nel campo **Lunghezza minima password** indicare il numero minimo di caratteri che la password deve contenere.

      In questo caso, l'accesso alle chiavi di criptaggio verrà eseguito utilizzando la password specificata, come quando è selezionata la casella di controllo **Usa password**.

    Se la casella di controllo **Usa password se Trusted Platform Module (TPM) non è disponibile** non è selezionata e il TPM non è disponibile, il criptaggio del disco rigido non verrà avviato.

14. Fare clic su **OK** per salvare le modifiche.

15. Applicare il criterio.

Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

Dopo avere applicato il criterio nel computer client in cui è installato Kaspersky Endpoint Security, verranno eseguite le seguenti query:

- Se il criterio di criptaggio è applicato a un disco rigido di sistema, verrà visualizzata la finestra del codice PIN se il TPM è in uso oppure la finestra di richiesta della password per l'autorizzazione del precaricamento.
- Se nel sistema operativo del computer è attivata la modalità di compatibilità con lo standard Federal Information Processing, in Windows 8 e versioni successive il sistema operativo visualizzerà una finestra di richiesta di connessione del dispositivo USB per il salvataggio del file della chiave di ripristino.

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 USB o sia andata persa).

## Creazione di un elenco di dischi rigidi esclusi dal criptaggio

È possibile creare un elenco di esclusioni dal criptaggio solo per tecnologia Kaspersky Disk Encryption.

*Per creare un elenco di dischi rigidi esclusi dal criptaggio:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera creare un elenco di dischi rigidi esclusi dal criptaggio.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio dei dischi rigidi**.
7. Nell'elenco a discesa **Tecnologia di criptaggio** selezionare l'opzione **Kaspersky Disk Encryption**.

   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.
8. Per aggiungere dischi rigidi all'elenco dei dischi rigidi esclusi dal criptaggio:
   a. Fare clic sul pulsante **Aggiungi**.

      Verrà visualizzata la finestra **Aggiungi dispositivi dall'elenco di Kaspersky Security Center**.

   b. Nella finestra **Aggiungi dispositivi dall'elenco di Kaspersky Security Center** specificare i valori dei seguenti parametri: **Nome**, **Computer**, **Tipo di disco** e **Kaspersky Disk Encryption**.

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**.

9. Se si desidera rimuovere dischi rigidi dalla tabella delle esclusioni, selezionare una o più righe nella tabella **Non criptare i seguenti dischi rigidi** e fare clic sul pulsante **Elimina**.

   Per selezionare più righe della tabella, fare clic su di esse tenendo premuto il tasto **CTRL**.

10. Fare clic su **OK** per salvare le modifiche.

## 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 Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare il decriptaggio dei dischi rigidi.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Criptaggio dei dischi rigidi**.
7. Nell'elenco a discesa **Tecnologia di criptaggio** selezionare la tecnologia con cui sono stati criptati i dischi rigidi.
8. 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 Kaspersky Disk Encryption.

9. Fare clic su **OK** per salvare le modifiche.

10. Applicare il criterio.

    Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

Se l'utente arresta o riavvia il computer durante il decriptaggio dei dischi rigidi criptati tramite la tecnologia Kaspersky Disk Encryption, 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 Kaspersky Disk Encryption, 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.

## Gestione dell'agente di autenticazione

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.

In alcuni casi per l'utente potrebbe essere impossibile eseguire l'autenticazione. Ad esempio, l'autenticazione è impossibile se l'utente ha dimenticato le credenziali dell'account per l'agente di autenticazione, ha dimenticato la password per il token o la smart card oppure ha smarrito il token o la smart card.

Se l'utente ha dimenticato le credenziali dell'account dell'agente di autenticazione o la password di un token o di una smart card, è necessario contattare l'amministratore della LAN aziendale per ripristinarle.

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 il ripristino dei dati nei dispositivi criptati.

## 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 del certificato elettronico di un token o una smart card al comando per la creazione di un 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.

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.

  Se il certificato elettronico del token o della smart card non soddisfa questo requisito, il plug-in di amministrazione non carica il file del certificato nel comando per la creazione di un account per l'agente di autenticazione e visualizza un messaggio di errore.

- Il parametro `KeyUsage` che definisce lo scopo del certificato deve avere il valore `keyEncipherment` o `dataEncipherment`.

  Se il certificato elettronico del token o della smart card non soddisfa questo requisito, il plug-in di amministrazione carica il file del certificato nel comando per la creazione di un account per l'agente di autenticazione e visualizza un messaggio di avviso.

- 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 questo requisito, il plug-in di amministrazione non carica il file del certificato nel comando per la creazione di un account per l'agente di autenticazione e visualizza un messaggio di errore.

## Modifica dei messaggi 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.

*Per modificare i messaggi della Guida dell'agente di autenticazione:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera modificare i messaggi della Guida dell'agente di autenticazione.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Impostazioni di criptaggio generali**.
7. Nella sezione **Modelli** fare clic sul pulsante **Guida**.

Verrà visualizzata la finestra **Messaggi della Guida dell'agente di autenticazione**.

8. Eseguire le seguenti operazioni:

   - 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 **Modifica 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.

9. Modificare i messaggi della Guida.

   Se si desidera ripristinare il testo originale, fare clic sul pulsante **Predefinito**.

10. Fare clic su **OK**.

11. Per salvare le modifiche, nella finestra **Proprietà: <Nome criterio>** fare clic su **OK**.

## 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.

## 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. Il file di traccia dell'Agente di Autenticazione può essere molto utile quando è necessario ripristinare i dati nei dischi rigidi criptati.

*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 nel corso del criptaggio dei dischi rigidi.

Il file di traccia dell'Agente di Autenticazione non viene inviato a Kaspersky, a differenza degli altri file di traccia dell'applicazione. Se necessario, l'amministratore di sistema può inviare manualmente il file di traccia dell'Agente di Autenticazione a Kaspersky per l'analisi.

## Gestione degli account per l'agente di autenticazione

Per la gestione degli account per l'agente di autenticazione, sono disponibili i seguenti strumenti di Kaspersky Security Center:

- Attività di gruppo per la gestione degli account per l'agente di autenticazione. Questa attività consente di gestire gli account per l'agente di autenticazione per un gruppo di computer client.
- Attività locale **Criptaggio (gestione account)**. Questa attività consente di gestire gli account per l'agente di autenticazione per singoli computer client.

*Per configurare le impostazioni per l'attività di gestione degli account per l'agente di autenticazione:*

1. Creare (Creazione di un'attività locale, Creazione di un'attività di gruppo) un'attività di gestione dell'account dell'agente di autenticazione.
2. Aprire la sezione **Impostazioni** nella finestra **Proprietà: <nome attività di gestione dell'account per l'agente di autenticazione>**.
3. Aggiungere i comandi per la creazione degli account per l'agente di autenticazione.
4. Aggiungere i comandi per la modifica degli account per l'agente di autenticazione.
5. Aggiungere i comandi per l'eliminazione degli account utente per l'agente di autenticazione.
6. Se necessario, modificare i comandi aggiunti per la gestione degli account per l'agente di autenticazione. A tale scopo, selezionare un comando nella tabella **Comandi per la gestione degli account per l'agente di autenticazione**, quindi fare clic sul pulsante **Modifica**.
7. Se necessario, eliminare i comandi aggiunti per la gestione degli account per l'agente di autenticazione. A tale scopo, selezionare uno o più comandi nella tabella **Comandi per la gestione degli account per l'agente di autenticazione**, quindi fare clic sul pulsante **Rimuovi**.

   Per selezionare più righe della tabella, fare clic su di esse tenendo premuto il tasto **CTRL**.

8. Per salvare le modifiche, fare clic su **OK** nella finestra delle proprietà dell'attività.
9. Eseguire l'attività.

Verranno eseguiti i comandi di gestione degli account per l'agente di autenticazione aggiunti all'attività.

# Aggiunta di un comando per la creazione di un account per l'agente di autenticazione

*Per aggiungere un comando per la creazione di un account per l'agente di autenticazione:*

1. Aprire la sezione **Impostazioni** nella finestra **Proprietà: <nome attività di gestione dell'account per l'agente di autenticazione>**.

2. Fare clic sul pulsante **Aggiungi** e selezionare **Comando di aggiunta account** nell'elenco a discesa.

   Verrà visualizzata la finestra **Aggiungi account utente**.

3. Nel campo **Aggiungi account utente** della finestra **Account di Windows** specificare il nome dell'account di Microsoft Windows in base al quale verrà creato l'account per l'agente di autenticazione.

   A tale scopo, digitare manualmente il nome dell'account o fare clic sul pulsante **Seleziona**.

4. Se è stato immesso manualmente il nome di un account di Microsoft Windows, fare clic sul pulsante **Consenti** per determinare l'identificatore di sicurezza (SID) dell'account.

   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.

   La determinazione del SID dell'account di Microsoft Windows al momento dell'aggiunta di un comando di creazione di un account per l'agente di autenticazione è un sistema pratico per verificare che il nome dell'account di Microsoft Windows immesso manualmente sia corretto. Se l'account utente Microsoft Windows immesso non esiste, appartiene a un dominio non attendibile o non è presente nel computer per cui viene modificata l'attività locale **Criptaggio (gestione account)**, l'attività di gestione degli account per l'agente di autenticazione termina con un errore.

5. Selezionare la casella di controllo **Modifica account utente attuale** per fare in modo che un account con nome identico creato in precedenza per l'agente di autenticazione venga sostituito dall'account di cui è in corso la 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 non è disponibile durante l'aggiunta di un comando per la creazione di un account per l'agente di autenticazione nelle proprietà di un'attività locale **Criptaggio (gestione account)**.

6. 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.

7. 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.

8. Se è stata selezionata la casella di controllo **Consenti l'autenticazione basata sulla password** durante il passaggio precedente:

   a. Nel campo **Password** digitare la password dell'account per l'agente di autenticazione che deve essere immessa durante l'autenticazione per l'accesso ai dischi rigidi criptati.

b. Nel campo **Conferma password** confermare la password dell'account per l'agente di autenticazione immessa nel passaggio precedente.

c. Eseguire una delle seguenti operazioni:

- Selezionare l'opzione **Modifica la password alla prima autenticazione** se si desidera che l'applicazione richieda all'utente di modificare la password dopo la prima autenticazione con l'account specificato nel comando.

- In caso contrario, selezionare l'opzione **Non richiedere la modifica della password**.

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.

10. Se è stata selezionata la casella di controllo **Consenti l'autenticazione basata sul certificato** durante il passaggio precedente, fare clic sul pulsante **Sfoglia** e selezionare il file del certificato elettronico del token o della smart card nella finestra **Seleziona file di certificato**.

11. Se necessario, nel campo **Descrizione del comando** immettere i dettagli sull'account per l'agente di autenticazione necessario per la gestione del comando.

12. Eseguire una delle seguenti operazioni:

- Selezionare la casella di controllo **Consenti autenticazione** se si desidera che l'applicazione consenta all'utente che utilizza l'account specificato nel comando di accedere alla finestra di dialogo di autenticazione nell'agente di autenticazione.

- Selezionare la casella di controllo **Blocca autenticazione** se si desidera che l'applicazione impedisca all'utente che utilizza l'account specificato nel comando di accedere alla finestra di dialogo di autenticazione nell'agente di autenticazione.

13. Nella finestra **Aggiungi account utente** fare clic su **OK**.

## Aggiunta di un comando di modifica dell'account per l'agente di autenticazione

*Per aggiungere un comando per la modifica di un account per l'agente di autenticazione:*

1. Nella sezione **Impostazioni** della finestra **Proprietà: <nome dell'attività di gestione dell'account per l'agente di autenticazione>** aprire il menu di scelta rapida del pulsante **Aggiungi** e selezionare la voce **Comando di modifica account**.

   Verrà visualizzata la finestra **Modifica account utente**.

2. Nel campo **Account di Windows** della finestra **Modifica account utente** specificare il nome dell'account utente di Microsoft Windows utilizzato per creare l'account per l'agente di autenticazione che si desidera modificare. A tale scopo, digitare manualmente il nome dell'account o fare clic sul pulsante **Seleziona**.

3. Se è stato immesso manualmente il nome di un account utente di Microsoft Windows, fare clic sul pulsante **Consenti** per determinare l'identificatore di sicurezza (SID) dell'account utente.

   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.

La determinazione del SID dell'account di Microsoft Windows al momento dell'aggiunta di un comando di modifica di un account per l'agente di autenticazione è un sistema pratico per verificare che il nome dell'account utente di Microsoft Windows immesso manualmente sia corretto. Se l'account utente di Microsoft Windows immesso non esiste o appartiene a un dominio non attendibile, l'attività di gruppo per la gestione degli account per l'agente di autenticazione termina con un errore.

4. 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**.

5. Selezionare la casella di controllo **Modifica le impostazioni di autenticazione basata sulla password** per rendere modificabili le impostazioni dell'autenticazione basata sulla password.

6. 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.

7. Se è stata selezionata la casella di controllo **Consenti l'autenticazione basata sulla password** durante il passaggio precedente:

   a. Nel campo **Password** immettere la nuova password dell'account per l'agente di autenticazione.

   b. Nel campo **Conferma password** confermare la password immessa nel passaggio precedente.

8. Selezionare la casella di controllo **Al momento dell'autenticazione nell'agente di autenticazione modifica la regola di modifica della password** 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**.

9. Specificare il valore dell'impostazione di modifica della password al momento dell'autenticazione nell'agente di autenticazione.

10. Selezionare la casella di controllo **Modifica le impostazioni di autenticazione basata sul certificato** per rendere modificabili le impostazioni dell'autenticazione basata sul certificato elettronico di un token o una smart card.

11. 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.

12. Se è stata selezionata la casella di controllo **Consenti l'autenticazione basata sul certificato** durante il passaggio precedente, fare clic sul pulsante **Sfoglia** e selezionare il file del certificato elettronico del token o della smart card nella finestra **Seleziona file di certificato**.

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. Nella finestra **Modifica account utente** fare clic su **OK**.

## Aggiunta di un comando per l'eliminazione di un account per l'agente di autenticazione

*Per aggiungere un comando per l'eliminazione di un account per l'agente di autenticazione:*

1. Nella sezione **Impostazioni** della finestra **Proprietà: <nome dell'attività di gestione dell'account per l'agente di autenticazione>** aprire il menu di scelta rapida del pulsante **Aggiungi** e selezionare la voce **Comando di eliminazione account**.

   Verrà visualizzata la finestra **Elimina account utente**.

2. Nel campo **Account di Windows** della finestra **Elimina account utente** specificare il nome dell'account utente di Microsoft Windows utilizzato per creare l'account per l'agente di autenticazione che si desidera eliminare. A tale scopo, digitare manualmente il nome dell'account o fare clic sul pulsante **Seleziona**.

3. Se è stato immesso manualmente il nome di un account utente di Microsoft Windows, fare clic sul pulsante **Consenti** per determinare l'identificatore di sicurezza (SID) dell'account utente.

   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.

   > La determinazione del SID dell'account di Microsoft Windows al momento dell'aggiunta di un comando di eliminazione di un account per l'agente di autenticazione è un sistema pratico per verificare che il nome dell'account utente di Microsoft Windows immesso manualmente sia corretto. Se l'account utente di Microsoft Windows immesso non esiste o appartiene a un dominio non attendibile, l'attività di gruppo per la gestione degli account per l'agente di autenticazione termina con un errore.

4. Nella finestra **Elimina account utente** fare clic su **OK**.

## Ripristino delle credenziali dell'account per l'agente di autenticazione

> Queste istruzioni sono destinate agli utenti di computer client in cui è installato Kaspersky Endpoint Security.

*Per ripristinare il nome utente e la password di un account per l'agente di autenticazione:*

1. L'agente di autenticazione viene caricato in un computer con dischi rigidi criptati prima del caricamento del sistema operativo. Nell'interfaccia dell'agente di autenticazione fare clic sul pulsante **Forgot your Password** per avviare il processo di ripristino del nome utente e della password di un account per l'agente di autenticazione.

2. Seguire le istruzioni dell'agente di autenticazione per ottenere le unità della richiesta per il ripristino del nome utente e della password dell'account per l'agente di autenticazione.

3. Fornire il contenuto delle sezioni della richiesta all'amministratore della rete LAN aziendale, insieme al nome del computer.

4. Immettere le sezioni della risposta alla richiesta di ripristino di nome utente e password dell'account per l'agente di autenticazione, generate e inviate dall'amministratore della rete LAN.

5. Immettere una nuova password dell'account per l'agente di autenticazione e confermarla.

   Il nome utente dell'account per l'agente di autenticazione viene definito utilizzando le sezioni della risposta alle richieste di ripristino di nome utente e password dell'account per l'agente di autenticazione.

Dopo avere immesso e confermato la nuova password dell'account per l'agente di autenticazione, la password verrà salvata e sarà possibile accedere ai dischi rigidi criptati.

## Risposta a una richiesta utente per il ripristino delle credenziali dell'account per l'agente di autenticazione

*Per creare e inviare all'utente le sezioni della risposta a una richiesta di ripristino di nome utente e password di un account per l'agente di autenticazione:*

1. Aprire Administration Console di Kaspersky Security Center.

2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione che include il computer dell'utente che ha richiesto il ripristino di nome utente e password di un account per l'agente di autenticazione.

3. Nell'area di lavoro selezionare la scheda **Dispositivi**.

4. Nella scheda **Dispositivi** selezionare il computer dell'utente che ha richiesto il ripristino di nome utente e password di un account per l'agente di autenticazione, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.

5. Dal menu di scelta rapida selezionare l'opzione **Concedi l'accesso a dispositivi e dati in modalità offline**.

   Verrà visualizzata la finestra **Concedi l'accesso a dispositivi e dati in modalità offline**.

6. Nella finestra **Concedi l'accesso a dispositivi e dati in modalità offline** selezionare la scheda **Agente di autenticazione**.

7. Nella sezione **Algoritmo di criptaggio in uso** selezionare il tipo di algoritmo di criptaggio.

8. 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.

9. Nell'elenco a discesa **Disco rigido** selezionare il disco rigido criptato per cui è necessario ripristinare l'accesso.

10. Nella sezione **Richiesta utente** immettere le sezioni della richiesta fornite dall'utente.

    Nel campo **Chiave di accesso** verrà visualizzato il contenuto delle sezioni della risposta alla richiesta dell'utente per il ripristino di nome utente e password di un account per l'agente di autenticazione.

11. Fornire all'utente il contenuto delle sezioni della risposta.

## Visualizzazione dei dettagli sul criptaggio dei dati

In questa sezione viene descritto come visualizzare i dettagli sul criptaggio dei dati.

## Informazioni sullo stato di criptaggio

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 non definito*. Non è stato definito un criterio di Kaspersky Security Center per il computer.
- *Criptaggio/decriptaggio 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 e/o decriptaggio 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.
- *Non supportato*. La funzionalità di criptaggio dei dati non è disponibile nel computer.

## Visualizzazione dello stato di criptaggio

*Per visualizzare lo stato di criptaggio dei dati del computer:*

1. Aprire Administration Console di Kaspersky Security Center.
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 desiderato.
3. Nell'area di lavoro selezionare la scheda **Dispositivi**.

   Nella scheda **Dispositivi** dell'area di lavoro vengono visualizzate le proprietà dei computer nel gruppo di amministrazione selezionato.
4. Nella scheda **Dispositivi** nell'area di lavoro trascinare la barra di scorrimento completamente a destra.

   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, sul criptaggio dei dischi rigidi del computer e sul criptaggio delle unità rimovibili connesse al computer.

## Visualizzazione delle statistiche sul criptaggio nei riquadri dei dettagli di Kaspersky Security Center

*Per visualizzare lo stato di criptaggio nei riquadri dei dettagli di Kaspersky Security Center:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella struttura della console selezionare il nodo **Administration Server - <Nome computer>**.
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**.
      Verrà visualizzata la finestra **Proprietà: statistiche**.
   b. Nella finestra **Proprietà: statistiche** fare clic su **Aggiungi**.
      Verrà visualizzata la finestra **Proprietà: nuova pagina**.
   c. Nella sezione **Generale** della finestra **Proprietà: nuova pagina** digitare il nome della pagina.
   d. Nella sezione **Riquadri dettagli** fare clic sul pulsante **Aggiungi**.
      Verrà visualizzata la finestra **Nuovo riquadro dettagli**.
   e. Nella finestra **Nuovo riquadro dettagli**, nel gruppo **Stato protezione**, selezionare l'elemento **Criptaggio dispositivo**.
   f. Fare clic su **OK**.
      Verrà visualizzata la finestra **Proprietà: controllo criptaggio**.
   g. Se necessario, modificare le impostazioni del riquadro dei dettagli. A tale scopo, utilizzare le sezioni **Visualizza** e **Dispositivi** della finestra **Proprietà: criptaggio dispositivo**.
   h. Fare clic su **OK**.
   i. Ripetere i passaggi d - h delle istruzioni, selezionando **Criptaggio delle unità rimovibili** nella sezione **Stato protezione** della finestra **Nuovo riquadro dettagli**.
      Il riquadro dei dettagli aggiunto viene visualizzato nell'elenco **Riquadri dettagli** della finestra **Proprietà: nuova pagina**.
   j. Verrà visualizzata la finestra **Proprietà: nuova pagina** fare clic su **OK**.
      Il nome della pagina con i riquadri dei dettagli creata nei passaggi precedenti viene visualizzato nell'elenco **Pagine** della finestra **Proprietà: statistiche**.
   k. Nella finestra **Proprietà: statistiche** fare clic su **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 Administration Console di Kaspersky Security Center.

2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione che include il computer client di cui si desidera visualizzare l'elenco degli errori di criptaggio dei file.

3. Nell'area di lavoro selezionare la scheda **Dispositivi**.

4. Nella scheda **Dispositivi** selezionare il nome del computer nell'elenco, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.

5. Eseguire una delle seguenti operazioni:

   - Dal menu di scelta rapida del computer selezionare **Protezione**.

   - Dal menu di scelta rapida del computer selezionare **Proprietà**. Nella finestra **Proprietà: <nome computer>** selezionare la sezione **Protezione**.

6. Nella sezione **Protezione** della finestra **Proprietà: <nome computer>** 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 Administration Console di Kaspersky Security Center.

2. Nel nodo **Administration Server** della struttura di Administration Console selezionare la scheda **Rapporti**.

3. Fare clic sul pulsante **Crea 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 sul criptaggio dei dati archiviati nei dispositivi**.

   - **Rapporto sugli errori di criptaggio**.

   - **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.

Verrà avviato il processo di generazione del rapporto. Il rapporto viene visualizzato in una nuova finestra.

## Gestione dei file criptati con funzionalità limitate di criptaggio dei file

Quando il criterio di Kaspersky Security Center viene applicato e i file vengono criptati, Kaspersky Endpoint Security riceve una chiave di criptaggio necessaria per l'accesso diretto 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 del 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.

## Accesso ai file criptati senza una connessione a Kaspersky Security Center

Queste istruzioni sono destinate agli utenti di computer client in cui è installato Kaspersky Endpoint Security.

*Per accedere ai file criptati senza una connessione a Kaspersky Security Center:*

1. Tentare di accedere al file criptato desiderato.

   Se non è disponibile la connessione a Kaspersky Security Center quando si tenta di accedere a un file archiviato in un'unità locale del computer, Kaspersky Endpoint Security genera un file con una richiesta di accesso per tutti i file criptati archiviati nelle unità locali del computer. Se si tenta di accedere a un file archiviato in un'unità rimovibile, Kaspersky Endpoint Security genera un file con una richiesta di accesso per tutti i file criptati archiviati nell'unità rimovibile. Verrà visualizzata la finestra **Accesso al file bloccato**.

2. Inviare il file che contiene la richiesta di accesso ai file criptati all'amministratore della rete LAN. A tale scopo, eseguire una delle seguenti operazioni:

   - Per inviare tramite e-mail il file della richiesta di accesso ai file criptati all'amministratore della rete LAN, fare clic sul pulsante **Invia tramite e-mail**.
   - Per salvare il file della richiesta di accesso ai file criptati e inviarlo all'amministratore della rete LAN con un altro metodo, fare clic sul pulsante **Salva**.

3. Ottenere il file chiave per l'accesso ai file criptati creato e fornito dall'amministratore della rete LAN.

4. Attivare la chiave di accesso ai file criptati in uno dei seguenti modi:

- In qualsiasi programma per la gestione dei file selezionare il file della chiave di accesso ai file criptati. Aprirlo facendo doppio clic.
- Eseguire le seguenti operazioni:

  a. Aprire la finestra principale di Kaspersky Endpoint Security.

  b. Fare clic sul pulsante .

  Verrà visualizzata la finestra **Eventi**.

  c. Selezionare la scheda **Stato dell'accesso a file e dispositivi**.

  La scheda contiene un elenco di tutte le richieste di accesso ai file criptati.

  d. Selezionare la richiesta per cui è stato ricevuto il file chiave per l'accesso ai file criptati.

  e. Per caricare il file chiave ricevuto per l'accesso ai file criptati, fare clic su **Sfoglia**.

  Verrà visualizzata la finestra di dialogo standard **Seleziona file chiave di accesso** di Microsoft Windows.

  f. Nella finestra standard di Microsoft Windows **Seleziona file chiave di accesso** selezionare il file fornito dall'amministratore con l'estensione .kesdr e il nome che corrisponde al nome del file della richiesta di accesso.

  g. Fare clic sul pulsante **Apri**.

  h. Nella finestra **Eventi** fare clic su **OK**.

Se un file con una richiesta di accesso ai file criptati viene generato quando si tenta di accedere a un file archiviato in un'unità locale del computer, Kaspersky Endpoint Security concede l'accesso a tutti i file criptati archiviati nelle unità locali del computer. Se un file con una richiesta di accesso ai file criptati viene generato quando si tenta di accedere a un file archiviato in un'unità rimovibile, Kaspersky Endpoint Security concede l'accesso a tutti i file criptati archiviati nell'unità rimovibile. Per accedere a file criptati archiviati in altre unità rimovibili, è necessario ottenere un file di chiave di accesso distinto per ogni unità rimovibile.

## Concessione dell'accesso utente ai file criptati senza una connessione a Kaspersky Security Center

*Per concedere l'accesso utente ai file criptati senza una connessione a Kaspersky Security Center:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione che include il computer dell'utente che richiede l'accesso ai file criptati.
3. Nell'area di lavoro selezionare la scheda **Dispositivi**.
4. Nella scheda **Dispositivi** selezionare il computer dell'utente che richiede l'accesso ai file criptati, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
5. Dal menu di scelta rapida selezionare l'opzione **Concedi l'accesso a dispositivi e dati in modalità offline**.

   Verrà visualizzata la finestra **Concedi l'accesso a dispositivi e dati in modalità offline**.
6. Nella finestra **Concedi l'accesso a dispositivi e dati in modalità offline** selezionare la scheda **Criptaggio**.

7. Nella scheda **Criptaggio** fare clic sul pulsante **Sfoglia**.

   Verrà visualizzata la finestra di dialogo standard **Seleziona il file della richiesta di accesso** di Microsoft Windows.

8. Nella finestra **Seleziona il file della richiesta di accesso** specificare il percorso del file di richiesta ricevuto dall'utente, quindi fare clic su **Apri**.

   Kaspersky Security Center genererà un file chiave per l'accesso ai file criptati. I dettagli della richiesta dell'utente sono visualizzati nella scheda **Criptaggio**.

9. Eseguire una delle seguenti operazioni:

   - Per inviare all'utente tramite e-mail il file chiave di accesso generato, fare clic sul pulsante **Invia tramite e-mail**.
   - Per salvare il file chiave per l'accesso ai file criptati e inviarlo all'utente con un altro metodo, fare clic sul pulsante **Salva**.

## 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 Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera modificare i modelli di messaggi per la richiesta dell'accesso ai file criptati.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:

   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

6. Nella sezione **Criptaggio dei dati** selezionare la sottosezione **Impostazioni di criptaggio generali**.
7. Nella sezione **Modelli** fare clic sul pulsante **Modelli**.

   Verrà visualizzata la finestra **Modelli**.

8. Eseguire le seguenti operazioni:

   - 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 negato al file**. Facendo clic sul pulsante **Invia tramite e-mail** nella finestra **Accesso negato al file**, viene creato automaticamente un messaggio dell'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.

9. Modificare i modelli dei messaggi.

   È possibile utilizzare il pulsante **Predefinito** e l'elenco a discesa **Variabile**.

10. Fare clic su **OK**.

11. Per salvare le modifiche, nella finestra **Proprietà: <Nome criterio>** fare clic su **OK**.

# 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 di 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 per i dispositivi criptati (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 di 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 di eseguire il ripristino dei dati nei dispositivi criptati, è consigliabile annullare il criterio di criptaggio di Kaspersky Security Center nel computer in cui deve essere eseguita questa operazione. Questo impedisce che l'unità venga nuovamente criptata.

## Ottenimento dell'accesso ai dispositivi criptati tramite l'interfaccia dell'applicazione

Queste istruzioni sono destinate agli utenti di computer client in cui è installato Kaspersky Endpoint Security.

*Per ottenere l'accesso ai dispositivi criptati tramite l'interfaccia dell'applicazione:*

1. Tentare di accedere al dispositivo criptato desiderato.

   Verrà visualizzata la finestra **Accesso ai dati bloccato**.

2. Inviare all'amministratore della rete LAN aziendale il file della richiesta di accesso con l'estensione kesdc per il dispositivo criptato. A tale scopo, eseguire una delle seguenti operazioni:

   - Per inviare tramite e-mail all'amministratore della rete LAN aziendale il file della richiesta di accesso generato per il dispositivo criptato, fare clic sul pulsante **Invia tramite e-mail**.

   - Per salvare il file della richiesta di accesso per il dispositivo criptato e inviarlo all'amministratore della rete LAN aziendale con un altro metodo, fare clic sul pulsante **Salva**.

   Se la finestra **Accesso ai dati bloccato** è stata chiusa senza salvare il file della richiesta di accesso o senza inviarlo all'amministratore della rete LAN aziendale, è possibile eseguire tale operazione in qualsiasi momento nella scheda **Stato dell'accesso a file e dispositivi** della finestra **Eventi**. Per aprire questa finestra, fare clic sul pulsante nella finestra principale dell'applicazione.

3. Ottenere e salvare il file chiave per l'accesso al dispositivo criptato che è stato creato e fornito dall'amministratore della rete LAN aziendale.

4. Utilizzare uno dei seguenti metodi per richiedere la chiave di accesso per il dispositivo criptato:

   - In qualsiasi programma per la gestione dei file individuare il file chiave per l'accesso al dispositivo criptato e fare doppio clic sul file per aprirlo.

   - Eseguire le seguenti operazioni:

a. Aprire la finestra principale di Kaspersky Endpoint Security.

b. Il pulsante apre la finestra **Eventi**.

c. Selezionare la scheda **Stato dell'accesso a file e dispositivi**.

La scheda contiene un elenco di tutte le richieste di accesso ai file e ai dispositivi criptati.

d. Selezionare la richiesta per cui è stato ricevuto il file chiave per l'accesso ai dispositivo criptato.

e. Per caricare il file chiave ricevuto per l'accesso al dispositivo criptato, fare clic su **Sfoglia**.

Verrà visualizzata la finestra di dialogo standard **Seleziona file chiave di accesso** di Microsoft Windows.

f. Nella finestra standard di Microsoft Windows **Seleziona file chiave di accesso** selezionare il file fornito dall'amministratore con l'estensione kesdr e il nome che corrisponde al nome del file della richiesta di accesso corrispondente per il dispositivo criptato.

g. Fare clic sul pulsante **Apri**.

h. Nella finestra **Stato dell'accesso a file e dispositivi** fare clic su **OK**.

Come risultato, Kaspersky Endpoint Security concede l'accesso al dispositivo criptato.

## Concessione dell'accesso utente ai dispositivi criptati

*Per concedere l'accesso utente a un dispositivo criptato:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione che include il computer dell'utente che ha richiesto l'accesso al dispositivo criptato.
3. Nell'area di lavoro selezionare la scheda **Dispositivi**.
4. Nella scheda **Dispositivi** selezionare il computer dell'utente che richiede l'accesso al dispositivo criptato, quindi fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida.
5. Dal menu di scelta rapida selezionare l'opzione **Concedi l'accesso a dispositivi e dati in modalità offline**.

   Verrà visualizzata la finestra **Concedi l'accesso a dispositivi e dati in modalità offline**.
6. Nella finestra **Concedi l'accesso a dispositivi e dati in modalità offline** selezionare la scheda **Criptaggio**.
7. Nella scheda **Criptaggio** fare clic sul pulsante **Sfoglia**.

   Verrà visualizzata la finestra di dialogo standard **Seleziona il file della richiesta di accesso** di Microsoft Windows.
8. Nella finestra **Seleziona il file della richiesta di accesso** specificare il percorso del file della richiesta con l'estensione kesdc che è stato ricevuto dell'utente.
9. Fare clic sul pulsante **Apri**.

   Kaspersky Security Center genera un file chiave di accesso al dispositivo criptato con l'estensione kesdr. I dettagli della richiesta dell'utente sono visualizzati nella scheda **Criptaggio**.
10. Eseguire una delle seguenti operazioni:

- Per inviare all'utente tramite e-mail il file chiave di accesso generato, fare clic sul pulsante **Invia tramite e-mail**.
- Per salvare il file chiave per l'accesso al dispositivo criptato e inviarlo all'utente con un altro metodo, fare clic sul pulsante **Salva**.

## Invio a un utente di una chiave di ripristino per i dischi rigidi criptati con BitLocker

*Per inviare a un utente una chiave di ripristino per un disco rigido di sistema criptato tramite BitLocker:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione che include il computer dell'utente che ha richiesto l'accesso all'unità criptata.
3. Nell'area di lavoro selezionare la scheda **Dispositivi**.
4. Nella scheda **Dispositivi** selezionare il computer che appartiene all'utente che ha richiesto l'accesso all'unità criptata.
5. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Concedi l'accesso a dispositivi e dati in modalità offline**.

   Verrà visualizzata la finestra **Concedi l'accesso a dispositivi e dati in modalità offline**.
6. Nella finestra **Concedi l'accesso a dispositivi e dati in modalità offline** 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.
8. Inviare all'utente la chiave indicata nel campo **Chiave di ripristino**.

*Per inviare a un utente una chiave di ripristino per un disco rigido non di sistema criptato tramite BitLocker:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella struttura di Administration Console selezionare la cartella **Avanzate** → **Criptaggio e protezione dei dati** → **Dispositivi criptati**.

   Nell'area di lavoro verrà visualizzato un elenco di dispositivi criptati.
3. Nell'area di lavoro selezionare il dispositivo criptato per cui è necessario ripristinare l'accesso.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Recupera chiave di accesso per il dispositivo criptato specificato**.

   Verrà visualizzata la finestra **Ripristina l'accesso al disco criptato con BitLocker**.

5. 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.

6. Inviare all'utente la chiave indicata nel campo **Chiave di ripristino**.

## Creazione del file eseguibile dell'utilità di ripristino

Queste istruzioni sono destinate agli utenti di computer client in cui è installato Kaspersky Endpoint Security.

*Per creare il file eseguibile dell'utilità di ripristino:*

1. Aprire la finestra principale dell'applicazione.
2. Fare clic sul pulsante nell'angolo inferiore sinistro della finestra principale dell'applicazione per aprire la finestra **Assistenza**.
3. Nella finestra **Assistenza** fare clic sul pulsante **Ripristina dispositivo criptato**.

   Verrà avviata l'utilità di ripristino per i dispositivi criptati.
4. Fare clic sul pulsante **Crea utilità di ripristino indipendente** nella finestra dell'utilità di ripristino.

   Verrà visualizzata la finestra **Crea utilità di ripristino indipendente**.
5. Nella finestra **Salva in** digitare manualmente il percorso per il salvataggio del file eseguibile dell'utilità di ripristino o fare clic sul pulsante **Sfoglia**.
6. Fare clic su **OK** nella finestra **Crea utilità di ripristino indipendente**.

   Il file eseguibile dell'utilità di ripristino (fdert.exe) verrà salvato nella cartella selezionata.

## Ripristino dei dati nei dispositivi criptati utilizzando l'utilità di ripristino

Queste istruzioni sono destinate agli utenti di computer client in cui è installato Kaspersky Endpoint Security.

*Per ripristinare l'accesso a un dispositivo criptato utilizzando l'utilità di ripristino:*

1. Eseguire l'utilità di ripristino in uno dei seguenti modi:
   - Fare clic sul pulsante nella finestra principale di Kaspersky Endpoint Security per aprire la finestra **Assistenza** e quindi sul pulsante **Ripristina dispositivo criptato**.
   - Eseguire il file eseguibile fdert.exe dell'utilità di ripristino. Questo file viene creato da Kaspersky Endpoint Security.

2. Nella finestra dell'utilità di ripristino, nell'elenco a discesa **Seleziona dispositivo**, selezionare un 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. 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 raccolta delle informazioni necessarie per lo sblocco o il decriptaggio del dispositivo.

5. Fare clic sul pulsante **Sblocca** o **Decripta**, a seconda dei risultati della diagnostica.

   Verrà visualizzata la finestra **Impostazioni di sblocco del dispositivo** o **Impostazioni di decriptaggio del dispositivo**.

6. Se si desidera ripristinare i dati utilizzando un account per l'Agente di Autenticazione:

   a. Selezionare l'opzione **Usa le impostazioni dell'account per l'Agente di Autenticazione**.

   b. Nei campi **Nome** e **Password** specificare le credenziali dell'account per l'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.

7. Se si desidera utilizzare una chiave di accesso per ripristinare i dati:

   a. Selezionare l'opzione **Specificare manualmente la chiave di accesso dispositivo**.

   b. Fare clic sul pulsante **Ricevi chiave di accesso**.

   c. Verrà visualizzata la finestra **Ricevi chiave di accesso dispositivo**.

   d. Fare clic sul pulsante **Salva** e selezionare la cartella in cui salvare il file della richiesta di accesso con l'estensione fdertc.

   e. Inviare il file della richiesta di accesso all'amministratore della rete LAN aziendale.

   > Non chiudere la finestra **Ricevi 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.

   f. Ottenere e salvare il file chiave di accesso che è stato creato e fornito dall'amministratore della rete LAN aziendale.

   g. Fare clic sul pulsante **Carica** e selezionare il file chiave di accesso con l'estensione fdertr nella finestra visualizzata.

8. Se si sta eseguendo il decriptaggio di un dispositivo, è necessario specificare anche le altre impostazioni di decriptaggio nella finestra **Impostazioni di decriptaggio del dispositivo**. A tale scopo:

- 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 utilizzare i campi **Avvia** e **Fine** per 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 **Salva dati nel file dopo il criptaggio**.
  - Se si desidera salvare i dati decriptati separatamente dai dati criptati originali, selezionare la casella di controllo **Salva dati nel file dopo il criptaggio** e utilizzare il pulsante **Sfoglia** per specificare il percorso in cui salvare i dati.

9. Fare clic su **OK**.

Verrà avviato il processo di sblocco o decriptaggio del dispositivo.

## Risposta a una richiesta utente per il ripristino dei dati nei dispositivi criptati

*Per creare e inviare a un utente un file chiave per l'accesso a un dispositivo criptato:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella struttura di Administration Console selezionare la cartella **Avanzate** → **Criptaggio e protezione dei dati** → **Dispositivi criptati**.
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 selezionare **Recupera chiave di accesso per il dispositivo criptato specificato**.

   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 sul collegamento **Recupera chiave di criptaggio dispositivo**.

   Verrà visualizzata la finestra **Consenti l'accesso al dispositivo**.
4. Selezionare l'algoritmo di criptaggio in uso. A tale scopo, selezionare una delle seguenti opzioni:
   - **AES256**, se Kaspersky Endpoint Security è stato installato da un pacchetto di distribuzione contenuto nella cartella aes256 nel computer in cui il dispositivo è stato criptato;
   - **AES56**, se Kaspersky Endpoint Security è stato installato da un pacchetto di distribuzione contenuto nella cartella aes56 nel computer in cui il dispositivo è stato criptato;
5. Fare clic sul pulsante **Sfoglia**.

   Verrà visualizzata la finestra di dialogo standard **Seleziona il file della richiesta di accesso** di Microsoft Windows.
6. Nella finestra **Seleziona il file della richiesta di accesso** specificare il percorso del file della richiesta con l'estensione fdertc che è stato ricevuto dell'utente.

7. Fare clic sul pulsante **Apri**.

   Kaspersky Security Center genera un file chiave di accesso con l'estensione fdertr per l'accesso al dispositivo criptato.

8. Eseguire una delle seguenti operazioni:

   - Per inviare all'utente tramite e-mail il file chiave di accesso generato, fare clic sul pulsante **Invia tramite e-mail**.
   - Per salvare il file chiave per l'accesso al dispositivo criptato e inviarlo all'utente con un altro metodo, fare clic sul pulsante **Salva**.

## 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 sistema Kaspersky Security Center Administration Server che controllava il computer durante il criptaggio dei dati.

L'accesso ai dati criptati verrà concesso alle stesse condizioni applicate prima che si verificasse il problema del sistema operativo.

## 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 per i dispositivi criptati.
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).

# Protezione della rete

Questa sezione contiene informazioni sul monitoraggio del traffico di rete e istruzioni su come configurare le impostazioni delle porte di rete monitorate.

## Informazioni sulla protezione della rete

Durante l'utilizzo di Kaspersky Endpoint Security, componenti come Anti-Virus Posta, Anti-Virus Web e Anti-Virus IM monitorano i flussi di dati trasmessi tramite specifici protocolli e che attraversano specifiche porte TCP e UDP aperte nel computer. Ad esempio, Anti-Virus Posta esamina i dati trasmessi tramite SMTP, mentre Anti-Virus Web esamina i dati trasmessi tramite HTTP e FTP.

Kaspersky Endpoint Security suddivide le porte TCP e UDP del sistema operativo in diversi gruppi, a seconda della probabilità che vengano compromesse. Alcune porte di rete sono riservate per servizi che possono essere vulnerabili. È consigliabile monitorare tali porte in modo più approfondito, perché la probabilità che vengano attaccate è superiore. 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. Queste porte e applicazioni vengono analizzate in modo particolarmente approfondito dai componenti Anti-Virus Posta, Anti-Virus Web e Anti-Virus IM durante il monitoraggio del traffico di rete.

## Configurazione delle impostazioni per il monitoraggio del traffico di rete

È possibile eseguire le seguenti azioni per configurare le impostazioni di monitoraggio del traffico di rete:

- Abilitare il monitoraggio di tutte le porte di rete.
- Creare un elenco di porte di rete monitorate.
- Creare un elenco di applicazioni per cui monitorare tutte le porte di rete.

## Abilitazione del monitoraggio di tutte le porte di rete

*Per abilitare il monitoraggio di tutte le porte di rete:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Protezione anti-virus**.
   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Porte da monitorare** selezionare **Tutte le porte di rete**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Creazione di un elenco di porte di rete monitorate

*Per creare un elenco di porte di rete monitorate:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Protezione anti-virus**.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Porte da monitorare** selezionare **Monitora solo le porte selezionate**.
4. Fare clic sul pulsante **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.
5. Nell'elenco delle porte di rete eseguire le seguenti operazioni:

   - Selezionare le caselle di controllo accanto alle porte di rete che si desidera includere nell'elenco delle porte di rete monitorate.

     Per impostazione predefinita, sono selezionate le caselle di controllo accanto a tutte le porte di rete elencate nella finestra **Porte di rete**.
   - Deselezionare le caselle di controllo accanto alle porte di rete che si desidera escludere dall'elenco delle porte di rete monitorate.
6. Se una porta di rete non viene visualizzata nell'elenco delle porte di rete, aggiungerla eseguendo le seguenti operazioni:

   a. Nell'elenco delle porte di rete fare clic sul collegamento **Aggiungi** per aprire la finestra **Porta di rete**.

   b. Immettere il numero della porta di rete nel campo **Porta**.

   c. Immettere il nome della porta di rete nel campo **Descrizione**.

   d. Fare clic su **OK**.

      La finestra **Porta di rete** verrà chiusa. La nuova porta di rete aggiunta verrà visualizzata in fondo all'elenco delle porte di rete.
7. Nella finestra **Porte di rete** fare clic su **OK**.
8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

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, selezionare la casella di controllo **Tutte le porte di rete** nella sezione **Porte da monitorare** o configurare il monitoraggio di tutte le porte per le applicazioni che stabiliscono la connessione 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Protezione anti-virus**.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Porte da monitorare** selezionare **Monitora solo le porte selezionate**.
4. Fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Porte di rete**.
5. Selezionare la casella di controllo **Monitora tutte le porte per le applicazioni specificate**.
6. Nell'elenco delle applicazioni sotto la casella di controllo **Monitora tutte le porte per le applicazioni specificate** eseguire le seguenti operazioni:

   - Selezionare le caselle di controllo accanto ai nomi delle applicazioni per cui si desidera monitorare tutte le porte di rete.

     Per impostazione predefinita, sono selezionate le caselle di controllo accanto a tutte le applicazioni elencate nella finestra **Porte di rete**.

   - Deselezionare le caselle di controllo accanto ai nomi delle applicazioni per cui non si desidera monitorare tutte le porte di rete.
7. Se un'applicazione non è inclusa nell'elenco delle applicazioni, aggiungerla nel modo seguente:

   a. Fare clic sul collegamento **Aggiungi** sotto l'elenco delle applicazioni e aprire il menu di scelta rapida.

   b. Nel menu di scelta rapida selezionare il modo in cui aggiungere l'applicazione all'elenco delle applicazioni:

      - Per selezionare un'applicazione dall'elenco delle applicazioni installate nel computer, selezionare il comando **Applicazioni**. Verrà visualizzata la finestra **Seleziona applicazione**, in cui è possibile specificare il nome dell'applicazione.

      - Per specificare il percorso del file eseguibile dell'applicazione, selezionare il comando **Sfoglia**. Verrà visualizzata la finestra standard di Microsoft Windows **Apri**, in cui è possibile specificare il nome del file eseguibile dell'applicazione.

     Dopo avere selezionato l'applicazione, verrà visualizzata la finestra **Applicazione**.

   c. Nel campo **Nome** immettere un nome per l'applicazione selezionata.

   d. Fare clic su **OK**.

      La finestra **Applicazione** verrà chiusa. L'applicazione aggiunta verrà visualizzata alla fine dell'elenco delle applicazioni.
8. Nella finestra **Porte di rete** fare clic su **OK**.
9. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Aggiornamento di database e moduli software dell'applicazione

Questa sezione contiene informazioni sugli aggiornamenti dei database e dei moduli dell'applicazione (anche denominati "aggiornamenti") e istruzioni su come configurare le impostazioni di aggiornamento.

## Informazioni sugli aggiornamenti di database e 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.

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 regolare le impostazioni di connessione.

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 sono visualizzate in **Aggiornamento**, nella sezione **Attività** della scheda **Protezione e controllo** della finestra principale dell'applicazione.

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.

## Informazioni sulle sorgenti degli aggiornamenti

Una *sorgente degli aggiornamenti* è una risorsa che contiene gli aggiornamenti per i database e i moduli dell'applicazione di Kaspersky Endpoint Security.

Le sorgenti degli aggiornamenti includono il server Kaspersky Security Center, i server degli aggiornamenti Kaspersky e cartelle di rete o locali.

## Configurazione delle impostazioni di aggiornamento

È possibile eseguire le seguenti azioni per configurare le impostazioni di aggiornamento:

- Aggiungere nuove sorgenti degli aggiornamenti.

  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.

  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.

  > Se si seleziona una risorsa esterna alla LAN come sorgente degli aggiornamenti, è necessario disporre di una connessione a Internet per poter eseguire l'aggiornamento.

- Selezionare la regione del server degli aggiornamenti Kaspersky.

  Se si utilizzano i server degli aggiornamenti Kaspersky come sorgente degli aggiornamenti, è possibile selezionare la posizione del server degli aggiornamenti Kaspersky utilizzato per scaricare il pacchetto di aggiornamento. I server degli aggiornamenti Kaspersky sono dislocati in più paesi. L'utilizzo dei server degli aggiornamenti Kaspersky più vicini consente di ridurre il tempo necessario per il recupero di un pacchetto di aggiornamento.

  Per impostazione predefinita, l'applicazione utilizza le informazioni sulla regione corrente dal registro del sistema operativo.

- Configurare l'aggiornamento di Kaspersky Endpoint Security da una cartella condivisa.

  Per ridurre il traffico Internet, è possibile configurare gli aggiornamenti di Kaspersky Endpoint Security in modo che i computer nella rete LAN ricevano gli aggiornamenti da una cartella condivisa. A tale scopo, uno dei computer nella rete LAN riceve il pacchetto di aggiornamento dal server Kaspersky Security Center o dai server degli aggiornamenti Kaspersky, quindi lo copia in una cartella condivisa. Gli altri computer della rete LAN sono quindi in grado di ricevere il pacchetto di aggiornamento da questa cartella condivisa.

- Selezionare la 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.

- Configurare l'attività di aggiornamento per l'esecuzione tramite i diritti di un account utente differente.

## Aggiunta di una sorgente degli aggiornamenti

*Per aggiungere una sorgente degli aggiornamenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Aggiornamento**.

   Nella parte destra della finestra sono visualizzate le impostazioni di aggiornamento dell'applicazione.
3. Nella sezione **Modalità di esecuzione e sorgente degli aggiornamenti** fare clic sul pulsante **Sorgente aggiornamenti**.

   Verrà aperta la scheda **Sorgente** nella finestra **Aggiornamento**.
4. Nella scheda **Sorgente** fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Seleziona sorgente degli aggiornamenti**.
5. Nella finestra **Seleziona sorgente degli aggiornamenti** selezionare una cartella con il pacchetto di aggiornamento o immetterne il percorso completo nel campo **Sorgente**.
6. Fare clic su **OK**.
7. Nella finestra **Aggiornamento** fare clic su **OK**.
8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Selezione della nazione del server degli aggiornamenti

*Per selezionare la nazione del server degli aggiornamenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Aggiornamento**.

   Nella parte destra della finestra sono visualizzate le impostazioni di aggiornamento dell'applicazione.
3. Nella sezione **Modalità di esecuzione e sorgente degli aggiornamenti** fare clic sul pulsante **Sorgente aggiornamenti**.

   Verrà aperta la scheda **Sorgente** nella finestra **Aggiornamento**.
4. Nella scheda **Sorgente**, nella sezione **Impostazioni internazionali**, scegliere **Selezionare dall'elenco**.
5. Nell'elenco a discesa selezionare il paese più vicino alla propria posizione corrente.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione degli aggiornamenti da una cartella condivisa

La configurazione degli aggiornamenti di Kaspersky Endpoint Security da una cartella condivisa consiste nei seguenti passaggi:

1. L'abilitazione della copia di un pacchetto di aggiornamento in una cartella condivisa in uno dei computer nella rete locale.

2. La configurazione degli aggiornamenti di Kaspersky Endpoint Security da una specifica cartella condivisa ai computer rimanenti della rete LAN.

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

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Aggiornamento**.

   Nella parte destra della finestra sono visualizzate le impostazioni di aggiornamento dell'applicazione.

3. Nella sezione **Avanzate** selezionare la casella di controllo **Copia aggiornamenti nella cartella**.

4. Specificare il percorso della cartella condivisa in cui posizionare il pacchetto di aggiornamento. È possibile eseguire questa operazione in uno dei seguenti modi:

   - Immettere il percorso della cartella condivisa nel campo della casella di controllo **Copia aggiornamenti nella cartella**.

   - Fare clic sul pulsante **Sfoglia**. Nella finestra visualizzata **Seleziona la cartella** selezionare la cartella desiderata, quindi fare clic su **OK**.

5. Per salvare le modifiche, fare clic sul pulsante **Salva**.

*Per configurare l'aggiornamento di Kaspersky Endpoint Security da una cartella condivisa:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Aggiornamento**.

   Nella parte destra della finestra sono visualizzate le impostazioni di aggiornamento dell'applicazione.

3. Nella sezione **Modalità di esecuzione e sorgente degli aggiornamenti** fare clic sul pulsante **Sorgente aggiornamenti**.

   Verrà aperta la scheda **Sorgente** nella finestra **Aggiornamento**.

4. Nella scheda **Sorgente** fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Seleziona sorgente degli aggiornamenti**.

5. Nella finestra **Seleziona sorgente degli aggiornamenti** selezionare la cartella condivisa che contiene il pacchetto di aggiornamento o immetterne il percorso completo nel campo **Sorgente**.

6. Fare clic su **OK**.

7. Nella scheda **Sorgente** deselezionare le caselle di controllo accanto ai nomi delle sorgenti degli aggiornamenti che non sono state specificate come cartella condivisa.

8. Fare clic su **OK**.

9. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Selezione della modalità di esecuzione dell'attività di aggiornamento

*Per selezionare la modalità di esecuzione dell'attività di aggiornamento:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Aggiornamento**.

   Nella parte destra della finestra sono visualizzate le impostazioni di aggiornamento dell'applicazione.

3. Fare clic sul pulsante **Modalità di esecuzione**.

   Verrà visualizzata la scheda **Modalità di esecuzione** della finestra **Aggiornamento**.

4. Nella sezione **Modalità di esecuzione** selezionare una delle seguenti opzioni per l'avvio di un'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 di avvio per l'attività di scansione, selezionare **In base alla pianificazione**.

5. Eseguire una delle seguenti operazioni:

   - Se è stata selezionata l'opzione **Automaticamente** o **Manualmente**, procedere al passaggio 6 di queste istruzioni.

   - Se è stata selezionata l'opzione **In base alla pianificazione**, specificare le impostazioni per la pianificazione di esecuzione dell'attività di aggiornamento. A tale scopo:

     a. Nell'elenco a discesa **Frequenza** specificare quando avviare l'attività di aggiornamento. Selezionare una delle seguenti opzioni: **Minuti**, **Ore**, **Giorni**, **Ogni settimana**, **A un'ora specificata**, **Ogni mese** o **Dopo l'avvio dell'applicazione**.

     b. A seconda dell'elemento selezionato nell'elenco a discesa **Frequenza**, specificare i valori per le impostazioni che definiscono l'ora di avvio dell'attività di aggiornamento.

     c. Nel campo **Rimanda l'esecuzione dopo l'avvio dell'applicazione di** specificare l'intervallo di tempo per cui rimandare l'esecuzione dell'attività di aggiornamento dopo l'avvio di Kaspersky Endpoint Security.

Il campo **Rimanda l'esecuzione dopo l'avvio dell'applicazione di** non è disponibile se è selezionato l'elemento **Dopo l'avvio dell'applicazione** nell'elenco a discesa **Frequenza**.

d. Se si desidera che le attività di aggiornamento ignorate vengano eseguite da Kaspersky Endpoint Security appena possibile, selezionare la casella di controllo **Esegui attività ignorate**.

Se è stata selezionata l'opzione **Ore**, **Minuti** o **Dopo l'avvio dell'applicazione** nell'elenco a discesa **Frequenza**, la casella di controllo **Esegui attività ignorate** non è disponibile.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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 di diritti sufficienti (ad esempio, da una cartella condivisa che contiene un pacchetto di aggiornamento) oppure perché è privo dei diritti utente necessari per un server proxy. 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. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Aggiornamento**.

   Nella parte destra della finestra sono visualizzate le impostazioni di aggiornamento dell'applicazione.

3. Nella sezione **Modalità di esecuzione e sorgente degli aggiornamenti** fare clic sul pulsante **Modalità di esecuzione**.

   Verrà visualizzata la scheda **Modalità di esecuzione** della finestra **Aggiornamento**.

4. Nella sezione **Utente** della scheda **Modalità di esecuzione** selezionare la casella di controllo **Esegui l'attività come**.

5. Nel campo **Nome** immettere il nome dell'account utente i cui diritti sono necessari per accedere alla sorgente degli aggiornamenti.

6. Nel campo **Password** immettere la password dell'utente i cui diritti sono necessari per accedere alla sorgente degli aggiornamenti.

7. Fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione degli aggiornamenti dei moduli dell'applicazione

*Per configurare gli aggiornamenti dei moduli dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Aggiornamento**.

   Nella parte destra della finestra sono visualizzate le impostazioni di aggiornamento dell'applicazione.
3. Nella sezione **Avanzate** eseguire una delle seguenti operazioni:
   - Selezionare la casella di controllo **Download degli aggiornamenti dei moduli dell'applicazione** se si desidera che l'applicazione includa gli aggiornamenti dei moduli dell'applicazione nei pacchetti di aggiornamento.
   - In caso contrario, deselezionare la casella di controllo **Download degli aggiornamenti dei moduli dell'applicazione**.
4. Se è stata selezionata la casella di controllo **Download degli aggiornamenti dei moduli dell'applicazione** nel passaggio precedente, specificare le condizioni per l'installazione degli aggiornamenti dei moduli dell'applicazione:
   - Selezionare l'opzione **Installa aggiornamenti critici e approvati** se si desidera che l'applicazione installi automaticamente gli aggiornamenti critici dei moduli dell'applicazione e gli altri aggiornamenti dopo l'approvazione della relativa installazione, in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center.
   - Selezionare l'opzione **Installa solo gli aggiornamenti approvati** se si desidera che l'applicazione installi gli aggiornamenti dei moduli dell'applicazione dopo l'approvazione della relativa installazione, in locale tramite l'interfaccia dell'applicazione o utilizzando Kaspersky Security Center.
5. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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 scaricare un pacchetto di aggiornamento dai server di Kaspersky, è necessaria una connessione a Internet.

*Per avviare o arrestare un'attività di aggiornamento:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Attività**.

   Verrà aperta la sezione **Attività**.

4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con il nome dell'attività di aggiornamento.

   Facendo clic su questa linea viene visualizzato un menu di azioni che è possibile eseguire sull'attività di aggiornamento.

5. Eseguire una delle seguenti operazioni:

   - Per avviare l'attività di aggiornamento, selezionare **Avvia aggiornamento** dal menu.

     Lo stato di avanzamento dell'attività di aggiornamento, visualizzato a destra del pulsante **Aggiornamento**, diventa *In esecuzione*.

   - Per interrompere l'attività di aggiornamento, selezionare **Interrompi aggiornamento** dal menu.

     Lo stato di avanzamento dell'attività di aggiornamento, visualizzato a destra del pulsante **Aggiornamento**, diventa *Interrotto*.

## Rollback dell'ultimo aggiornamento

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. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Attività**.

   Verrà aperta la sezione **Attività**.

4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività **Aggiornamento**.
5. Selezionare **Rollback aggiornamento**.

## Configurazione delle impostazioni del server proxy

*Per configurare le impostazioni del server proxy:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Aggiornamento**.

   Nella parte destra della finestra sono visualizzate le impostazioni di aggiornamento dell'applicazione.

3. Nella sezione **Server proxy** fare clic sul pulsante **Impostazioni**.

Verrà visualizzata la finestra **Impostazioni del server proxy**.

4. Nella finestra **Impostazioni del server proxy** selezionare la casella di controllo **Usa server proxy**.
5. Specificare le impostazioni del server proxy.
6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

È inoltre possibile configurare le impostazioni del server proxy nella finestra principale dell'applicazione, nella scheda **Impostazioni**, nella sezione **Impostazioni avanzate**.

# 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.

In questa sezione sono descritte le caratteristiche specifiche e le impostazioni delle attività di scansione, dei livelli di protezione, dei metodi e delle tecnologie di scansione. Vengono inoltre fornite istruzioni sulla gestione dei file non elaborati da Kaspersky Endpoint Security durante una scansione virus.

## Informazioni sulle attività di scansione

Per l'individuazione di virus e altri tipi di malware e il controllo dell'integrità dei moduli dell'applicazione, Kaspersky Endpoint Security include le seguenti attività:

- **Scansione Completa**. Una scansione approfondita dell'intero computer. Per impostazione predefinita, 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
- **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.
- **Scansione Personalizzata**. Kaspersky Endpoint Security esegue la scansione degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi dei seguenti oggetti:
  - Memoria del kernel
  - Oggetti caricati all'avvio del sistema operativo
  - Backup del sistema operativo
  - Cassetta postale di Outlook
  - Tutti i dischi rigidi, le unità rimovibili e di rete
  - Qualsiasi file selezionato
- **Controllo integrità**. Kaspersky Endpoint Security verifica se i moduli dell'applicazione risultano danneggiati o modificati.

Le attività Scansione Completa e Scansione delle aree critiche presentano alcune differenze rispetto alle altre attività. Per queste attività, non è consigliabile modificare l'ambito della scansione.

Dopo l'avvio delle attività di scansione, lo stato di avanzamento è visualizzato nel campo accanto al nome dell'attività di scansione in esecuzione, nella sezione **Attività** della scheda **Protezione e controllo** nella finestra principale di Kaspersky Endpoint Security.

Le informazioni sui risultati della scansione e sugli eventi che si sono verificati durante l'esecuzione delle attività di scansione vengono registrate in un rapporto di Kaspersky Endpoint Security.

## Avvio o arresto di un'attività di scansione

Indipendentemente dalla modalità di esecuzione selezionata per l'attività di scansione, è possibile avviare o arrestare un'attività di scansione in qualsiasi momento.

*Per avviare o arrestare un'attività di scansione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Attività**.

   Verrà aperta la sezione **Attività**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con il nome dell'attività di scansione.

   Verrà visualizzato un menu di azioni che è possibile eseguire sull'attività di scansione.
5. Eseguire una delle seguenti operazioni:

   - Per avviare l'attività di scansione, selezionare **Avvia scansione** dal menu.

     Lo stato di avanzamento dell'attività, visualizzato a destra del pulsante con il nome dell'attività di scansione, diventerà *In esecuzione*.

   - Per arrestare l'attività di scansione, selezionare **Interrompi scansione** dal menu.

     Lo stato di avanzamento dell'attività, visualizzato a destra del pulsante con il nome dell'attività di scansione, diventerà *Interrotto*.

## Configurazione delle impostazioni di un'attività di scansione

Per configurare le impostazioni di un'attività di scansione, è possibile eseguire le seguenti operazioni:

- Modificare il livello di protezione.

  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 protezione dei file, è possibile ripristinare in qualsiasi momento le impostazioni consigliate.

- Modificare l'azione eseguita da Kaspersky Endpoint Security quando viene rilevato un file infetto.

- Modificare l'ambito della scansione.

  È possibile estendere o restringere l'ambito della scansione aggiungendo o rimuovendo oggetti da esaminare oppure modificando i tipi di file da esaminare.

- Ottimizzare la 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 compositi. È anche possibile impostare un limite per la scansione di un singolo file. Al termine dell'intervallo di tempo specificato, il file viene escluso dalla scansione corrente (ad eccezione degli archivi e degli oggetti che contengono più file).

  È anche possibile abilitare l'utilizzo delle tecnologie iChecker e iSwift. Queste tecnologie ottimizzano la velocità di scansione dei file escludendo i file che non sono stati modificati dall'ultima scansione.

- Configurare la scansione dei file compositi.

- Configurare l'utilizzo dei metodi di scansione.

  Quando è attivato, Kaspersky Endpoint Security utilizza l'analisi delle firme. Durante l'analisi delle firme, Kaspersky Endpoint Security confronta l'oggetto rilevato con i record nel proprio database. In base alle raccomandazioni degli specialisti di Kaspersky, l'analisi delle firme è sempre abilitata.

  Per aumentare l'efficacia della protezione, è possibile utilizzare l'analisi euristica. Durante l'analisi euristica, Kaspersky Endpoint Security analizza l'attività degli oggetti nel sistema operativo. L'analisi euristica consente di rilevare gli oggetti dannosi per cui al momento non sono presenti record nel database di Kaspersky Endpoint Security.

- Selezionare la modalità di esecuzione dell'attività di scansione.

  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.

  È possibile rimandare l'esecuzione delle attività di scansione 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 scansione. L'attività di scansione potrà essere eseguita solo dopo il periodo di tempo specificato dall'avvio di Kaspersky Endpoint Security.

- Configurare l'attività di scansione per l'esecuzione tramite un account utente differente.

- Specificare le impostazioni per la scansione delle unità rimovibili quando vengono connesse al computer.

## Modifica del livello di protezione

Per eseguire le attività di scansione, Kaspersky Endpoint Security utilizza varie combinazioni di impostazioni. Queste combinazioni di impostazioni salvate nell'applicazione sono denominate *livelli di protezione*. Esistono tre livelli di protezione preimpostati: **Alto**, **Consigliato** e **Basso**. Le impostazioni del livello di protezione **Consigliato** sono considerate ottimali. Queste impostazioni sono consigliate dagli esperti di Kaspersky.

*Per modificare un livello di protezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività di scansione desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.

3. Nella sezione **Livello di sicurezza** eseguire una delle seguenti operazioni:

- Se si desidera applicare uno dei livelli di protezione preimpostati (**Alto**, **Consigliato** o **Basso**), selezionarlo con il dispositivo di scorrimento.
- Se si desidera configurare un livello di protezione personalizzato, fare clic sul pulsante **Impostazioni**, quindi specificare le impostazioni nella finestra visualizzata con il nome dell'attività di scansione.

  Al termine della configurazione di un livello di protezione personalizzato, il nome del livello di protezione nella sezione **Livello di sicurezza** viene modificato in **Personalizzato**.
- Se si desidera impostare il livello di protezione su **Consigliato**, fare clic sul pulsante **Predefinito**.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica dell'azione da eseguire sui file infetti

*Per modificare l'azione da eseguire sui file infetti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività di scansione desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.
3. Nella sezione **Azione se viene rilevata una minaccia** selezionare l'opzione desiderata:
   - **Seleziona azione automaticamente**.
   - **Esegui azione**.
4. Se è stata selezionata l'opzione **Esegui azione** durante il passaggio precedente, selezionare le caselle di controllo seguenti:
   - Selezionare la casella di controllo **Disinfetta** se si desidera che Kaspersky Endpoint Security disinfetti gli oggetti in cui vengono rilevate minacce.

     Anche se è selezionata questa opzione, Kaspersky Endpoint Security applica l'azione **Rimuovi** ai file che fanno parte dell'applicazione Windows Store.
   - Selezionare la casella di controllo **Elimina** se si desidera che Kaspersky Endpoint Security elimini gli oggetti in cui vengono rilevate minacce.
   - Selezionare entrambe le caselle di controllo **Disinfetta** ed **Elimina** se si desidera che Kaspersky Endpoint Security tenti di disinfettare gli oggetti in cui vengono rilevate minacce ed elimini gli oggetti che non possono essere disinfettati.
   - Deselezionare entrambe le caselle di controllo **Disinfetta** ed **Elimina** se si desidera che Kaspersky Endpoint Security non esegua alcuna azione sugli oggetti in cui vengono rilevate minacce, ma visualizzi semplicemente una notifica per l'utente sui risultati della scansione di questi oggetti.
5. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Generazione di un elenco di oggetti da esaminare

Per generare un elenco di oggetti da esaminare, è possibile utilizzare uno dei seguenti metodi:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

> Questo metodo è disponibile solo per le attività **Scansione Completa** e **Scansione delle aree critiche**. L'elenco di oggetti di esaminare per l'attività **Scansione Personalizzata** può essere creato solo nella scheda **Protezione e controllo**.

*Per creare un elenco di oggetti di esaminare nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Attività**.

   Verrà aperta la sezione **Attività**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga che contiene il nome dell'attività e selezionare **Ambito della scansione**.

   Verrà visualizzata la finestra **Ambito della scansione**.
5. Per aggiungere un nuovo oggetto all'ambito della scansione:
   a. Fare clic sul pulsante **Aggiungi**.

      Verrà visualizzata la finestra **Selezione ambito di scansione**.
   b. Selezionare l'oggetto e fare clic su **Aggiungi**.

      Tutti gli oggetti selezionati nella finestra **Selezione ambito di scansione** sono visualizzati nell'elenco **Ambito della scansione**.
   c. Fare clic su **OK**.
6. Per modificare il percorso di un oggetto nell'ambito della scansione:
   a. Selezionare l'oggetto nell'ambito della scansione.
   b. Fare clic sul pulsante **Modifica**.

      Verrà visualizzata la finestra **Selezione ambito di scansione**.
   c. Immettere il nuovo percorso dell'oggetto nell'ambito della scansione.
   d. Fare clic su **OK**.
7. Per rimuovere un oggetto dall'ambito della scansione:

a. Selezionare l'oggetto che si desidera rimuovere dall'ambito della scansione.

Per selezionare più oggetti, fare clic su di essi tenendo premuto il tasto **CTRL**.

b. Fare clic sul pulsante **Rimuovi**.

Verrà visualizzata una finestra per la conferma dell'eliminazione.

c. Fare clic su **Sì** nella finestra di conferma dell'eliminazione.

Non è possibile rimuovere o modificare gli oggetti che sono inclusi nell'ambito della scansione predefinito.

8. Per escludere un oggetto dall'ambito della scansione, deselezionare la casella di controllo accanto all'oggetto nella finestra **Ambito della scansione**.

L'oggetto rimane nell'elenco degli oggetti nell'ambito della scansione, ma non viene analizzato durante l'esecuzione dell'attività di scansione.

9. Fare clic su **OK**.

10. Per salvare le modifiche, fare clic sul pulsante **Salva**.

*Per creare un elenco di oggetti da esaminare dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività di scansione desiderata: **Scansione Completa** o **Scansione delle aree critiche**.

Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.

3. Fare clic sul pulsante **Ambito della scansione**.

Verrà visualizzata la finestra **Ambito della scansione**.

4. Creare un elenco di oggetti di esaminare seguendo i passaggi 5-10 delle istruzioni precedenti.

## Selezione del tipo di file da esaminare

È possibile utilizzare i due metodi seguenti per selezionare il tipo di file da esaminare:

- Nella scheda **Protezione e controllo** della finestra principale dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione

Questo metodo è disponibile solo per le attività **Scansione Completa** e **Scansione delle aree critiche**. Il tipo di file da esaminare per l'attività **Scansione Personalizzata** può essere selezionato solo nella scheda **Protezione e controllo**.

*Per selezionare i tipi di file da esaminare nella scheda Protezione e controllo della finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.

2. Selezionare la scheda **Protezione e controllo**.

3. Fare clic sulla sezione **Attività**.

   Verrà aperta la sezione **Attività**.

4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga che contiene il nome dell'attività e selezionare **Impostazioni**.

   Verrà visualizzata una finestra con il nome dell'attività di scansione selezionata.

5. Nella finestra con il nome dell'attività di scansione selezionata selezionare la scheda **Ambito**.

6. Nella sezione **Tipi di file** specificare il tipo di file che si desidera analizzare durante l'esecuzione dell'attività di scansione selezionata:

   - Per esaminare tutti i file, selezionare **Tutti i file**.
   - Per esaminare i file nei formati che presentano la maggiore vulnerabilità alle infezioni, selezionare **Esamina i file per formato**.
   - Per esaminare i file con le estensioni che in genere presentano la maggiore vulnerabilità alle infezioni, selezionare **Esamina i file per estensione**.

   Durante la selezione del tipo di file da esaminare, tenere presenti i seguenti elementi:

   - Per alcuni formati di file (ad esempio, TXT), la probabilità di penetrazione e attivazione di codice dannoso è bassa. Altri formati di file, al contrario, contengono o possono contenere codice eseguibile (ad esempio, exe, dll, doc). Il rischio di penetrazione e attivazione di codice dannoso in tali file è alto.
   - Un utente malintenzionato potrebbe inviare un virus o un altro programma dannoso 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, Anti-Virus File analizza l'intestazione del file indipendentemente dall'estensione. Se l'analisi rivela che il file è in formato EXE, l'applicazione lo esamina.

7. Nella finestra con il nome dell'attività di scansione fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

*Per selezionare il tipo di file da esaminare dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività di scansione desiderata: **Scansione Completa** o **Scansione delle aree critiche**.

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.

3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata una finestra con il nome dell'attività di scansione selezionata.

4. Nella finestra con il nome dell'attività di scansione selezionata selezionare la scheda **Ambito**.

5. Completare i passaggi 5-7 delle istruzioni precedenti.

## Ottimizzazione della scansione dei file

*Per ottimizzare la scansione dei file:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività di scansione desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.
3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata una finestra con il nome dell'attività di scansione selezionata.
4. Nella finestra visualizzata selezionare la scheda **Ambito**.
5. Nella sezione **Ottimizzazione della scansione** eseguire le seguenti operazioni:
   - Selezionare la casella di controllo **Esamina solo i file nuovi e modificati**.
   - Selezionare la casella di controllo **Ignora i file esaminati per più di**, quindi specificare la durata della scansione per un singolo file (in secondi).
6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Scansione dei file compositi

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

*Per configurare la scansione dei file compositi:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività di scansione desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.
3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata una finestra con il nome dell'attività di scansione selezionata.
4. Nella finestra visualizzata selezionare la scheda **Ambito**.

5. Nella sezione **Scansione dei file compositi** specificare i file compositi di cui eseguire la scansione: archivi, pacchetti di installazione, file nei formati di Office, file nei formati di posta elettronica e archivi protetti tramite password.

6. Se la casella di controllo **Esamina solo i file nuovi e modificati** è deselezionata nella sezione **Ottimizzazione della scansione**, fare clic sul collegamento **tutti / nuovi** accanto al nome del tipo di file composito se si desidera specificare per ogni tipo di file composito se esaminare tutti i file di questo tipo o solo i nuovi file di questo tipo.

   Quando si fa clic sul collegamento, il relativo valore viene modificato.

   Se la casella di controllo **Esamina solo i file nuovi e modificati** è selezionata, vengono esaminati solo i nuovi file.

7. Fare clic sul pulsante **Avanzate**.

   Verrà visualizzata la finestra **File compositi**.

8. Nella sezione **Dimensione massima** eseguire una delle seguenti operazioni:

   - Se non si desidera decomprimere i file compositi di grandi dimensioni, selezionare la casella di controllo **Non decomprimere i file compositi molto grandi**, quindi specificare il valore desiderato nel campo **Dimensione massima dei file**.

   - Se si desidera decomprimere i file compositi di grandi dimensioni, indipendentemente dalla dimensione, deselezionare la casella di controllo **Non decomprimere i file compositi molto grandi**.

   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 molto grandi** sia selezionata o meno.

9. Fare clic su **OK**.

10. Nella finestra con il nome dell'attività di scansione fare clic su **OK**.

11. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Utilizzo dei metodi di scansione

*Per utilizzare i metodi di scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività di scansione desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.

3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata una finestra con il nome dell'attività di scansione selezionata.

4. Nella finestra visualizzata selezionare la scheda **Avanzate**.

5. Se si desidera che l'applicazione utilizzi l'analisi euristica durante l'esecuzione dell'attività di scansione, nella sezione **Metodi di scansione** selezionare la casella di controllo **Analisi euristica. Utilizzare** quindi il dispositivo di scorrimento per impostare il livello dell'analisi euristica: **Superficiale**, **Media** o **Approfondita**.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Utilizzo delle tecnologie di scansione

*Per utilizzare le tecnologie di scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività di scansione desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.

3. Nella sezione **Livello di protezione** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata una finestra con il nome dell'attività di scansione selezionata.

4. Nella finestra visualizzata selezionare la scheda **Avanzate**.

5. Nella sezione **Tecnologie di scansione** selezionare le caselle di controllo accanto ai nomi delle tecnologie da utilizzare durante la scansione.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Selezione della modalità di esecuzione per l'attività di scansione

*Per selezionare la modalità di esecuzione dell'attività di scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.

3. Fare clic sul pulsante **Modalità di esecuzione**.

   Verrà visualizzata una finestra con le proprietà dell'attività selezionata nella scheda **Modalità di esecuzione**.

4. Nella sezione **Modalità di esecuzione** selezionare la modalità di esecuzione dell'attività: **Manualmente** o **In base alla pianificazione**.

5. Se è stata selezionata l'opzione **In base alla pianificazione**, specificare le impostazioni di pianificazione. A tale scopo:

   a. Nell'elenco a discesa **Frequenza** selezionare la frequenza di esecuzione dell'attività (**Minuti**, **Ore**, **Giorni**, **Ogni settimana**, **A un'ora specificata**, **Ogni mese**, **Dopo l'avvio dell'applicazione** o **Dopo ogni**

**aggiornamento**).

b. A seconda della frequenza selezionata, configurare le impostazioni avanzate che specificano la pianificazione di esecuzione dell'attività.

c. Se si desidera che le attività di scansione ignorate vengano avviate da Kaspersky Endpoint Security appena possibile, selezionare la casella di controllo **Esegui attività ignorate**.

> Se è stata selezionata la voce **Minuti**, **Ore**, **Dopo l'avvio dell'applicazione** o **Dopo ogni aggiornamento** nell'elenco a discesa **Frequenza**, la casella di controllo **Esegui attività ignorate** non è disponibile.

a. Se si desidera che un'attività venga sospesa da Kaspersky Endpoint Security quando le risorse del computer sono limitate, selezionare la casella di controllo **Esegui solo quando il computer è inattivo**.

Questa opzione di pianificazione consente di ridurre l'utilizzo delle risorse del computer.

6. Fare clic su **OK**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Avvio di un'attività di scansione tramite un account utente differente

Per impostazione predefinita, un'attività di scansione viene eseguita con le autorizzazioni dell'account con cui l'utente ha eseguito l'accesso al sistema operativo. Può essere tuttavia necessario eseguire un'attività di scansione tramite un altro account utente. È possibile specificare un utente che dispone dei diritti appropriati nelle impostazioni dell'attività di scansione ed eseguire l'attività di scansione tramite l'account di questo utente.

*Per configurare l'avvio di un'attività di scansione tramite un account utente differente:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare la sottosezione con il nome dell'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).

Nella parte destra della finestra sono visualizzate le impostazioni dell'attività di scansione selezionata.

3. Fare clic sul pulsante **Modalità di esecuzione**.

Verrà visualizzata una finestra con le proprietà dell'attività selezionata nella scheda **Modalità di esecuzione**.

4. Nella sezione **Utente** della scheda **Modalità di esecuzione** selezionare la casella di controllo **Esegui l'attività come**.

5. Nel campo **Nome** immettere il nome dell'account utente i cui diritti sono necessari per avviare l'attività di scansione.

6. Nel campo **Password** immettere la password dell'utente i cui diritti sono necessari per avviare l'attività di scansione.

7. Fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Scansione delle unità rimovibili quando vengono connesse al computer

Alcuni programmi dannosi sfruttano le vulnerabilità del sistema operativo per replicarsi tramite reti locali e unità rimovibili. Kaspersky Endpoint Security consente di eseguire la scansione delle unità rimovibili connesse al computer alla ricerca di virus e altro malware.

*Per configurare la scansione delle unità rimovibili quando vengono connesse:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Attività pianificate**.

   Le impostazioni dell'attività vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Scansione automatica delle unità rimovibili** selezionare l'azione desiderata nell'elenco a discesa **Azione alla connessione di unità rimovibili**:

   - **Non eseguire scansione**
   - **Scansione dettagliata**

     In questa modalità, Kaspersky Endpoint Security esamina tutti i file nell'unità rimovibile, inclusi i file all'interno di oggetti compositi.
   - **Scansione Rapida**

     In questa modalità, Kaspersky Endpoint Security esamina solo i file potenzialmente infettabili e non decomprime gli oggetti compositi.
4. Se si desidera che Kaspersky Endpoint Security esegua solo la scansione delle unità rimovibili di dimensioni inferiori a un valore specificato, selezionare la casella di controllo **Dimensione massima unità rimovibile** e specificare un valore in megabyte nel campo accanto ad essa.
5. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Gestione dei file non elaborati

Questa sezione contiene istruzioni sulla gestione dei file infetti e potenzialmente infetti non elaborati da Kaspersky Endpoint Security durante la scansione del computer alla ricerca di virus e altre minacce.

## Informazioni sui file non elaborati

Kaspersky Endpoint Security registra le informazioni sui file non elaborati. Queste informazioni vengono registrate sotto forma di eventi nell'elenco dei file non elaborati.

Un file infetto viene considerato *elaborato* se Kaspersky Endpoint Security esegue una delle seguenti azioni sul file, in base alle impostazioni dell'applicazione specificate, durante la scansione del computer alla ricerca di virus e altre minacce:

- Disinfetta.

- Rimuovi.
- Elimina se la disinfezione fallisce.

Un file infetto viene considerato *non elaborato* se Kaspersky Endpoint Security per qualsiasi motivo non riesce a 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).
- L'azione selezionata per le attività di scansione nella sezione **Azione se viene rilevata una minaccia** è **Avvisa** e l'utente seleziona l'azione **Ignora** quando viene visualizzata la notifica del file infetto.

È possibile avviare manualmente un'attività Scansione Personalizzata per i file nell'elenco dei file non elaborati dopo l'aggiornamento dei database e dei moduli dell'applicazione. Lo stato del file può cambiare dopo la scansione. È possibile eseguire le azioni desiderate sui file, a seconda del relativo stato.

È ad esempio possibile eseguire le seguenti azioni:

- Eliminare i file con lo stato *Infetto*.
- Ripristinare i file infetti che contengono informazioni importanti e ripristinare i file contrassegnati come *Disinfettato* o *Non infetto*.
- Spostare in quarantena i file con stato *Potenzialmente infetto*.

## Gestione dell'elenco dei file non elaborati

L'elenco dei file non elaborati viene visualizzato in una tabella.

È possibile eseguire le seguenti operazioni con i file non elaborati:

- Visualizzare l'elenco dei file non elaborati.
- Eseguire la scansione dei file non elaborati utilizzando la versione corrente dei database e dei moduli di Kaspersky Endpoint Security.
- Ripristinare i file dall'elenco dei file non elaborati nelle cartelle originali o in una cartella differente specificata dall'utente (quando non è possibile eseguire la scrittura nella cartella originale).
- Rimuovere file dall'elenco dei file non elaborati.
- Aprire la cartella in cui era originariamente posizionato il file non elaborato.

È inoltre possibile eseguire le seguenti azioni durante la gestione dei dati nella tabella:

- Filtrare gli eventi file non elaborato in base al valore della colonna o alle condizioni di un filtro personalizzato.
- Utilizzare la funzione di ricerca degli eventi file non elaborato.
- Ordinare gli eventi file non elaborato.

- Modificare l'ordine e il set di colonne visualizzate nell'elenco dei file non elaborati.
- Raggruppare gli eventi file non elaborato.

Se necessario, è possibile copiare negli Appunti gli eventi file non elaborato selezionati.

## Avvio di un'attività Scansione Personalizzata per i file non elaborati

È possibile avviare manualmente un'attività Scansione Personalizzata per i file non elaborati. È ad esempio possibile avviare la scansione se l'ultima scansione è stata interrotta per qualche motivo o se si desidera ripetere la scansione dei file non elaborati dopo l'aggiornamento più recente dei database e dei moduli dell'applicazione.

*Per avviare un'attività Scansione Personalizzata dei file non elaborati:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.
3. Nella finestra **Archivi** selezionare la scheda **File non elaborati**.
4. Nella tabella della scheda **File non elaborati** selezionare uno o più eventi associati ai file da esaminare.

   Per selezionare più eventi, fare clic su di essi tenendo premuto il tasto **CTRL**.
5. Avviare l'attività Scansione Personalizzata in uno dei seguenti modi:
   - Fare clic sul pulsante **Ripeti scansione**.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Ripeti scansione**.

## Eliminazione di file dall'elenco dei file non elaborati

*Per eliminare i file dall'elenco dei file non elaborati:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.
3. Nella finestra **Archivi** selezionare la scheda **File non elaborati**.
4. Nella tabella della scheda **File non elaborati** selezionare uno o più eventi associati ai file da eliminare.

   Per selezionare più eventi, fare clic su di essi tenendo premuto il tasto **CTRL**.
5. Eliminare i file in uno dei seguenti modi:
   - Fare clic sul pulsante **Rimuovi**.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Elimina**.

# Scansione Vulnerabilità

Questa sezione contiene informazioni su specifiche e impostazioni dell'attività Scansione Vulnerabilità e istruzioni sulla gestione dell'elenco di vulnerabilità rilevate da Kaspersky Endpoint Security durante l'esecuzione dell'attività Scansione Vulnerabilità.

## Visualizzazione delle informazioni sulle vulnerabilità delle applicazioni in esecuzione

Le informazioni sulle vulnerabilità delle applicazioni in esecuzione sono disponibili se Kaspersky Endpoint Security è installato in un computer con un sistema operativo Microsoft Windows per workstation. Queste informazioni non sono disponibili se Kaspersky Endpoint Security è installato in un computer che esegue un sistema operativo Microsoft Windows per file server.

*Per visualizzare le informazioni sulle vulnerabilità delle applicazioni in esecuzione:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Aprire la sezione **Controllo endpoint**.
4. Fare clic sul pulsante **Monitor attività applicazioni**.

   Verrà visualizzata la scheda **Monitor attività applicazioni** della finestra **Controllo privilegi applicazioni**. Nella tabella **Monitor attività applicazioni** sono visualizzate informazioni di riepilogo sulle attività delle applicazioni in esecuzione nel sistema operativo. Il livello di gravità delle vulnerabilità delle applicazioni in esecuzione, determinato dal componente Monitor vulnerabilità, è indicato nella colonna **Livello di gravità della vulnerabilità**.

## Informazioni sull'attività Scansione Vulnerabilità

Le vulnerabilità del sistema operativo possono ad esempio essere causate da errori di programmazione o progettazione, password vulnerabili o attività del malware. Durante la scansione delle vulnerabilità, l'applicazione analizza il sistema operativo e cerca le anomalie e le impostazioni danneggiate delle applicazioni Microsoft e di altri produttori.

La scansione delle vulnerabilità esegue la diagnostica della protezione del sistema operativo e consente di rilevare le vulnerabilità software che possono essere utilizzate da utenti malintenzionati per diffondere oggetti dannosi e ottenere l'accesso a informazioni personali.

Dopo l'avvio delle attività di scansione delle vulnerabilità, lo stato di avanzamento è visualizzato nel campo accanto al nome dell'attività **Scansione Vulnerabilità** nella sezione **Attività** della scheda **Protezione e controllo** nella finestra principale di Kaspersky Endpoint Security.

I risultati dell'attività Scansione Vulnerabilità vengono registrati nei rapporti.

## Avvio o arresto dell'attività Scansione Vulnerabilità

Indipendentemente dalla modalità di esecuzione selezionata per l'attività Scansione Vulnerabilità, è possibile avviarla o arrestarla in qualsiasi momento.

*Per avviare o arrestare l'attività Scansione Vulnerabilità:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Fare clic sulla sezione **Attività**.

   Verrà aperta la sezione **Attività**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con il nome dell'attività Scansione Vulnerabilità.

   Verrà visualizzato un menu di operazioni per l'attività Scansione Vulnerabilità.
5. Eseguire una delle seguenti operazioni:

   - Per avviare l'attività Scansione Vulnerabilità, selezionare **Avvia scansione** dal menu.

     Lo stato di avanzamento dell'attività, visualizzato a destra del pulsante con il nome dell'attività Scansione Vulnerabilità, diventerà *In esecuzione*.

   - Per arrestare l'attività Scansione Vulnerabilità, selezionare **Interrompi scansione** dal menu.

     Lo stato di avanzamento dell'attività, visualizzato a destra del pulsante con il nome dell'attività Scansione Vulnerabilità, diventerà *Interrotto*.

## Configurazione delle impostazioni di Scansione Vulnerabilità

Per configurare le impostazioni di Scansione Vulnerabilità, è possibile eseguire le seguenti operazioni:

- Creare l'ambito di Scansione Vulnerabilità.

  È possibile espandere o restringere l'ambito della scansione aggiungendo o rimuovendo applicazioni da esaminare alla ricerca di vulnerabilità.

- Selezionare la modalità di esecuzione per l'attività Scansione Vulnerabilità.

  Se per qualsiasi motivo non è possibile eseguire l'attività, ad esempio perché all'ora prevista il computer è spento, è possibile configurare l'attività non eseguita in modo che venga avviata automaticamente appena possibile.

- Configurare l'attività per l'esecuzione tramite i diritti di un account utente differente.

  Per impostazione predefinita, un'attività di scansione viene eseguita con le autorizzazioni dell'account con cui l'utente ha eseguito l'accesso al sistema operativo. Può essere tuttavia necessario eseguire un'attività di scansione tramite un altro account utente. È possibile specificare un utente che dispone dei diritti appropriati nelle impostazioni dell'attività ed eseguire l'attività tramite l'account di questo utente.

## Creazione dell'ambito della scansione delle vulnerabilità

Un ambito della scansione delle vulnerabilità è costituito da un produttore di software o dal percorso della cartella in cui è installato il software (ad esempio, tutte le applicazioni Microsoft nella cartella Programmi).

*Per creare un ambito della scansione delle vulnerabilità:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Scansione Vulnerabilità**.

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività Scansione Vulnerabilità.
3. Nella sezione **Ambito della scansione**:
   a. Per utilizzare Kaspersky Endpoint Security per la ricerca di vulnerabilità nelle applicazioni Microsoft installate nel computer, selezionare la casella di controllo **Microsoft**.
   b. Per utilizzare Kaspersky Endpoint Security per la ricerca di vulnerabilità nelle applicazioni non Microsoft installate nel computer, selezionare la casella di controllo **Altri produttori**.
   c. Nella finestra **Area di scansione vulnerabilità aggiuntive** fare clic sul pulsante **Impostazioni**.

      Verrà visualizzata la finestra **Ambito di Scansione Vulnerabilità**.
   d. Creare l'ambito di Scansione Vulnerabilità. A tale scopo, utilizzare pulsanti **Aggiungi** e **Rimuovi**.
   e. Nella finestra **Ambito di Scansione Vulnerabilità** fare clic su **OK**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Selezione della modalità di esecuzione per l'attività Scansione Vulnerabilità

*Per selezionare la modalità di esecuzione dell'attività Scansione Vulnerabilità:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Scansione Vulnerabilità**.

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività Scansione Vulnerabilità.
3. Fare clic sul pulsante **Modalità di esecuzione**.

   Verrà visualizzata la scheda **Modalità di esecuzione** della finestra **Scansione Vulnerabilità**.
4. Nella sezione **Modalità di esecuzione** selezionare una delle seguenti opzioni per l'avvio dell'attività Scansione Vulnerabilità:
   - Se si desidera avviare manualmente l'attività Scansione Vulnerabilità, selezionare **Manualmente**.
   - Se si desidera configurare una pianificazione di avvio per l'attività Scansione Vulnerabilità, selezionare **In base alla pianificazione**.
5. Eseguire una delle seguenti operazioni:

- Se è stata selezionata l'opzione **Manualmente**, procedere al passaggio 6 di queste istruzioni.
- Se è stata selezionata l'opzione **In base alla pianificazione**, specificare le impostazioni di avvio dell'attività Scansione Vulnerabilità. A tale scopo:

  a. Nell'elenco a discesa **Frequenza** specificare quando avviare l'attività Scansione Vulnerabilità. Selezionare una delle seguenti opzioni: **Giorni**, **Ogni settimana**, **A un'ora specificata**, **Ogni mese**, **Dopo l'avvio dell'applicazione** o **Dopo ogni aggiornamento**.

  b. A seconda dell'elemento selezionato nell'elenco a discesa **Frequenza**, specificare i valori per le impostazioni che definiscono l'ora di avvio dell'attività Scansione Vulnerabilità.

  c. Se si desidera che le attività Scansione Vulnerabilità ignorate vengano avviate da Kaspersky Endpoint Security appena possibile, selezionare la casella di controllo **Esegui attività ignorate**.

  > Se è stata selezionata l'opzione **Dopo l'avvio dell'applicazione** o **Dopo ogni aggiornamento** nell'elenco a discesa **Frequenza**, la casella di controllo **Esegui attività ignorate** non è disponibile.

6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Avvio dell'attività Scansione Vulnerabilità tramite i diritti di un account utente differente

Per impostazione predefinita, l'attività Scansione Vulnerabilità viene avviata tramite l'account con cui l'utente ha eseguito l'accesso al sistema operativo. Può essere tuttavia necessario avviare l'attività Scansione Vulnerabilità tramite un altro account utente. È possibile specificare un utente che dispone dei diritti appropriati nelle impostazioni dell'attività Scansione Vulnerabilità ed eseguire l'attività tramite l'account di questo utente.

*Per configurare l'avvio dell'attività Scansione Vulnerabilità tramite un account utente differente:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Scansione Vulnerabilità**.

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività Scansione Vulnerabilità.
3. Fare clic sul pulsante **Modalità di esecuzione**.

   Verrà visualizzata la scheda **Modalità di esecuzione** della finestra **Scansione Vulnerabilità**.
4. Nella sezione **Utente** della scheda **Modalità di esecuzione** selezionare la casella di controllo **Esegui l'attività come**.
5. Nel campo **Nome** immettere il nome dell'account dell'utente i cui diritti sono necessari per avviare l'attività Scansione Vulnerabilità.
6. Nel campo **Password** immettere la password dell'account dell'utente i cui diritti sono necessari per avviare l'attività Scansione Vulnerabilità.
7. Fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Gestione dell'elenco delle vulnerabilità

Durante la gestione dell'elenco delle vulnerabilità, è possibile eseguire le seguenti azioni:

- Visualizzare l'elenco delle vulnerabilità.
- Avviare nuovamente l'attività Scansione Vulnerabilità dopo l'aggiornamento dei database e dei moduli dell'applicazione.
- Visualizzare informazioni dettagliate sulla vulnerabilità e raccomandazioni sulla relativa correzione in una sezione distinta.
- Nascondere le voci selezionate nell'elenco delle vulnerabilità.
- Filtrare l'elenco delle vulnerabilità in base al livello di importanza.
- Filtrare l'elenco delle vulnerabilità in base ai valori *Corrette* e *Nascoste*.

È inoltre possibile eseguire le seguenti azioni durante la gestione dei dati nella tabella:

- Filtrare l'elenco delle vulnerabilità in base ai valori delle colonne o a condizioni di filtro personalizzate.
- Utilizzare la funzione di ricerca delle vulnerabilità.
- Nascondere le voci nell'elenco delle vulnerabilità.
- Modificare l'ordine e la disposizione delle colonne visualizzate nell'elenco delle vulnerabilità.
- Raggruppare le voci nell'elenco delle vulnerabilità.

## Informazioni sull'elenco delle vulnerabilità

Kaspersky Endpoint Security registra i risultati dell'attività Scansione Vulnerabilità nell'elenco delle vulnerabilità.

Una volta che l'utente esamina le specifiche vulnerabilità ed esegue le azioni consigliate per la loro correzione, Kaspersky Endpoint Security modifica lo stato delle vulnerabilità in *Corretta*.

Se non si desidera visualizzare le voci relative a specifiche vulnerabilità nell'elenco delle vulnerabilità, è possibile scegliere di nascondere tali voci. Kaspersky Endpoint Security assegna lo stato *Nascoste* a tali vulnerabilità.

L'elenco delle vulnerabilità viene visualizzato sotto forma di una tabella. Ogni riga della tabella contiene le seguenti informazioni:

- Un'icona che indica il livello di gravità della vulnerabilità. I livelli di criticità delle vulnerabilità sono i seguenti:
  - Icona . **Critico**. Questo livello di gravità si applica alle vulnerabilità altamente pericolose, che devono essere corrette immediatamente. Gli utenti malintenzionati sfruttano attivamente le vulnerabilità di questo livello per infettare il sistema operativo del computer o accedere ai dati personali dell'utente. Kaspersky consiglia di

eseguire tempestivamente tutti i passaggi necessari per correggere le vulnerabilità con livello di gravità "Critico".

- Icona . **Importante**. Questo livello di gravità si applica alle vulnerabilità importanti che devono essere corrette. Gli utenti malintenzionati possono sfruttare attivamente le vulnerabilità di questo livello. Gli utenti malintenzionati attualmente non sfruttano attivamente le vulnerabilità di livello “Importante”. Kaspersky consiglia di eseguire tempestivamente tutti i passaggi necessari per correggere le vulnerabilità con livello di gravità "Importante".

- Icona . **Attenzione**. Questo livello di gravità si applica alle vulnerabilità che possono essere corrette in un secondo momento. Tuttavia, tali vulnerabilità possono minacciare la sicurezza del computer in futuro.

- ID della vulnerabilità.
- Nome applicazione in cui è stata rilevata la vulnerabilità.
- Breve descrizione della vulnerabilità.
- Informazioni sull'autore del software, indicato nella firma digitale.
- Risultato delle azioni eseguite per correggere la vulnerabilità.

## Ripetizione dell'attività Scansione Vulnerabilità

Per aggiornare le informazioni sulle vulnerabilità rilevate in precedenza, è possibile avviare di nuovo l'attività Scansione Vulnerabilità. Può essere necessario ripetere l'attività di scansione se la scansione delle vulnerabilità è stata interrotta per qualche motivo o se si desidera eseguire la ricerca di vulnerabilità nel computer dopo l'aggiornamento dei database e dei moduli dell'applicazione più recente.

*Per avviare nuovamente l'attività Scansione Vulnerabilità:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.
3. Nella finestra **Archivi** selezionare la scheda **Vulnerabilità**.

   La scheda **Vulnerabilità** contiene un elenco delle vulnerabilità rilevate da Kaspersky Endpoint Security durante l'attività Scansione Vulnerabilità.
4. Nell'angolo inferiore destro della finestra **Archivi** fare clic sul pulsante **Ripeti scansione**.

Kaspersky Endpoint Security aggiorna le informazioni dettagliate sulle vulnerabilità nell'elenco delle vulnerabilità.

Lo stato di una vulnerabilità corretta attraverso l'installazione di una patch non viene modificato dopo un'ulteriore scansione delle vulnerabilità.

## Correzione di una vulnerabilità

È possibile correggere una vulnerabilità installando un aggiornamento del sistema operativo, modificando la configurazione dell'applicazione o installando una patch per l'applicazione.

Le vulnerabilità rilevate potrebbero non essere applicabili alle applicazioni installate, ma alle relative copie. Una patch consente di correggere una vulnerabilità solo se l'applicazione è installata.

*Per correggere una vulnerabilità:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.
3. Nella finestra **Archivi** selezionare la scheda **Vulnerabilità**.

   La scheda **Vulnerabilità** contiene un elenco delle vulnerabilità rilevate da Kaspersky Endpoint Security durante l'attività Scansione Vulnerabilità.
4. Nell'elenco delle vulnerabilità selezionare la voce che corrisponde alla vulnerabilità desiderata.

   Nella parte inferiore dell'elenco delle vulnerabilità verrà visualizzata una sezione con informazioni sulla vulnerabilità e raccomandazioni su come correggerla.

   Per ogni vulnerabilità selezionata sono disponibili le seguenti informazioni:

   - Nome applicazione in cui è stata rilevata la vulnerabilità.
   - Versione dell'applicazione in cui è stata rilevata la vulnerabilità.
   - Livello di gravità di una vulnerabilità.
   - ID della vulnerabilità.
   - Data e ora dell'ultimo rilevamento della vulnerabilità.
   - Raccomandazioni per la correzione della vulnerabilità (ad esempio, un collegamento un sito Web con un aggiornamento del sistema operativo o una patch per l'applicazione).
   - Collegamento a un sito Web con una descrizione della vulnerabilità.
5. Per visualizzare una descrizione dettagliata della vulnerabilità, fare clic sul collegamento **Informazioni aggiuntive** per aprire una pagina Web con una descrizione della minaccia associata alla vulnerabilità selezionata. Il sito Web www.secunia.com consente di scaricare e installare l'aggiornamento necessario per la versione corrente dell'applicazione.
6. Scegliere uno dei seguenti metodi per la correzione di una vulnerabilità:

   - Se sono disponibili una o più patch per l'applicazione, installare le patch necessarie seguendo le istruzioni fornite accanto al nome della patch.
   - Se è disponibile un aggiornamento del sistema operativo, installare l'aggiornamento necessario seguendo le istruzioni fornite accanto al nome dell'aggiornamento.

   La vulnerabilità viene corretta dopo l'installazione della patch o dell'aggiornamento. Kaspersky Endpoint Security assegna a questa vulnerabilità uno stato che indica che la vulnerabilità è stata corretta. La voce relativa alla vulnerabilità corretta viene visualizzata in grigio nell'elenco delle vulnerabilità.

7. Se nella parte inferiore della finestra non è disponibile alcuna informazione su come correggere una vulnerabilità, è possibile avviare nuovamente l'attività Scansione Vulnerabilità dopo l'aggiornamento dei database e dei moduli di Kaspersky Endpoint Security. Poiché Kaspersky Endpoint Security esegue la scansione delle vulnerabilità nel sistema utilizzando un database di vulnerabilità, è possibile che una voce relativa a una vulnerabilità corretta venga visualizzata dopo l'aggiornamento dell'applicazione.

## Occultamento delle voci nell'elenco delle vulnerabilità

È possibile nascondere la voce relativa a una vulnerabilità selezionata. Kaspersky Endpoint Security assegna lo stato *Nascosto* alle voci selezionate nell'elenco delle vulnerabilità e contrassegnate come nascoste. Sarà quindi possibile filtrare l'elenco delle vulnerabilità in base al valore dello stato *Nascosto*.

*Per nascondere una voce nell'elenco delle vulnerabilità:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.
3. Nella finestra **Archivi** selezionare la scheda **Vulnerabilità**.

   La scheda **Vulnerabilità** contiene un elenco delle vulnerabilità rilevate da Kaspersky Endpoint Security durante l'attività Scansione Vulnerabilità.
4. Nell'elenco delle vulnerabilità selezionare la voce relativa alla vulnerabilità che di desidera nascondere.

   Nella parte inferiore dell'elenco delle vulnerabilità verrà visualizzata una sezione con informazioni sulla vulnerabilità e raccomandazioni su come correggerla.
5. Fare clic sul pulsante **Nascondi**.

   Kaspersky Endpoint Security assegna lo stato *Nascosto* alla vulnerabilità selezionata. Le voci sulle vulnerabilità con stato *Nascosto* sono spostate alla fine dell'elenco delle vulnerabilità e visualizzate in grigio.
6. Per nascondere una voce relativa a una vulnerabilità nell'elenco delle vulnerabilità, selezionare la casella di controllo **Nascosto** nella parte superiore dell'elenco.

## Filtro dell'elenco delle vulnerabilità in base al livello di gravità

*Per filtrare l'elenco delle vulnerabilità in base al livello di gravità:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.
3. Nella finestra **Archivi** selezionare la scheda **Vulnerabilità**.

   La scheda **Vulnerabilità** contiene un elenco delle vulnerabilità rilevate da Kaspersky Endpoint Security durante l'attività Scansione Vulnerabilità. Vengono visualizzate tre icone relative al livello di gravità della vulnerabilità (Avviso, Importante, Critico) nella parte superiore dell'elenco delle vulnerabilità nella riga **Mostra livello di gravità**. Facendo clic su queste icone è possibile filtrare l'elenco delle vulnerabilità in base al livello di gravità.

4. Fare clic su una, due o tre icone relative al livello di gravità delle vulnerabilità. Le vulnerabilità che corrispondono ai livelli di gravità selezionati vengono visualizzate nell'elenco. Per non visualizzare più le vulnerabilità che corrispondono a un livello di gravità specifico nell'elenco, fare nuovamente clic sull'icona relativa al livello di gravità attinente. Se non è stato selezionato alcun livello di gravità, l'elenco delle vulnerabilità è vuoto.

Le condizioni di filtro specificate per le voci relative alle vulnerabilità vengono salvate alla chiusura della finestra **Archivi**.

## Filtro dell'elenco delle vulnerabilità in base ai valori Corrette e Nascoste

*Per filtrare l'elenco delle vulnerabilità in base ai valori Corretta e Nascosta:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.

3. Nella finestra **Archivi** selezionare la scheda **Vulnerabilità**.

   La scheda **Vulnerabilità** contiene un elenco delle vulnerabilità rilevate da Kaspersky Endpoint Security durante l'attività Scansione Vulnerabilità.

4. Accanto all'impostazione **Mostra vulnerabilità** sono visualizzate caselle di controllo che indicano lo stato delle vulnerabilità. Per filtrare l'elenco delle vulnerabilità in base allo stato *Corrette*, eseguire una delle seguenti operazioni:

   - Per visualizzare le voci sulle vulnerabilità corrette nell'elenco delle vulnerabilità, selezionare la casella di controllo **Corrette**. Le voci relative alle vulnerabilità corrette appaiono in grigio nell'elenco delle vulnerabilità.

   - Per nascondere le voci sulle vulnerabilità corrette nell'elenco delle vulnerabilità, deselezionare la casella di controllo **Corrette**.

5. Per filtrare l'elenco delle vulnerabilità in base allo stato *Nascosto*, eseguire una delle seguenti operazioni:

   - Per visualizzare le voci sulle vulnerabilità nascoste nell'elenco delle vulnerabilità, selezionare la casella di controllo **Nascosto**. Le voci relative alle vulnerabilità nascoste appaiono in grigio nell'elenco delle vulnerabilità.

   - Per nascondere le voci sulle vulnerabilità nascoste nell'elenco delle vulnerabilità, deselezionare la casella di controllo **Nascosto**.

Le condizioni di filtro specificate per le voci relative alle vulnerabilità non vengono salvate alla chiusura della finestra **Archivi**.

# Controllo dell'integrità dei moduli dell'applicazione

Questa sezione contiene informazioni sulle specifiche e le impostazioni dell'attività Controllo integrità.

## Informazioni sull'attività 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.

Dopo l'avvio delle attività Controllo integrità, lo stato di avanzamento è visualizzato nel campo accanto al nome dell'attività nella sezione **Attività** della scheda **Protezione e controllo** nella finestra principale di Kaspersky Endpoint Security.

I risultati dell'attività Controllo integrità vengono registrati nei rapporti.

## Avvio o arresto di un'attività Controllo integrità

Indipendentemente dalla modalità di esecuzione selezionata, è possibile avviare o arrestare un'attività Controllo integrità in qualsiasi momento.

*Per avviare o arrestare un'attività Controllo integrità:*

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la scheda **Protezione e controllo**.
3. Aprire la sezione **Attività**.
4. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida della riga con il nome dell'attività Controllo integrità.
5. Eseguire una delle seguenti operazioni:
   - Per avviare l'attività Controllo integrità, selezionare **Avvia scansione** dal menu di scelta rapida.

     Lo stato di avanzamento dell'attività, visualizzato a destra del pulsante con il nome dell'attività, diventerà *In esecuzione*.
   - Per arrestare l'attività Controllo integrità, selezionare **Interrompi scansione** dal menu di scelta rapida.

     Lo stato di avanzamento dell'attività, visualizzato a destra del pulsante con il nome dell'attività, diventerà *Interrotto*.

## Selezione della modalità di esecuzione per l'attività Controllo integrità

*Per selezionare la modalità di esecuzione per l'attività Controllo integrità:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Attività pianificate**, selezionare **Controllo integrità**.

   Nella parte destra della finestra sono visualizzate le impostazioni dell'attività Controllo integrità.
3. Nella sezione **Modalità di esecuzione** scegliere una delle seguenti opzioni:

   - Se si desidera avviare manualmente l'attività Controllo integrità, selezionare **Manualmente**.
   - Se si desidera configurare la pianificazione di avvio per l'attività Controllo integrità, selezionare **In base alla pianificazione**.
4. Se è stata selezionata l'opzione **In base alla pianificazione** durante il passaggio precedente, specificare le impostazioni della pianificazione di esecuzione dell'attività. A tale scopo:

   a. Nell'elenco a discesa **Frequenza** specificare quando avviare l'attività Controllo integrità. Selezionare una delle seguenti opzioni: **Minuti**, **Ore**, **Giorni**, **Ogni settimana**, **A un'ora specificata**, **Ogni mese** o **Dopo l'avvio dell'applicazione**.

   b. A seconda dell'elemento selezionato nell'elenco a discesa **Frequenza**, specificare i valori per le impostazioni che definiscono l'ora di avvio dell'attività.

   c. Se si desidera che le attività Controllo integrità ignorate vengano avviate da Kaspersky Endpoint Security appena possibile, selezionare la casella di controllo **Esegui attività ignorate**.

   > Se è stata selezionata l'opzione **Dopo l'avvio dell'applicazione**, **Minuti** o **Ore** nell'elenco a discesa **Frequenza**, la casella di controllo **Esegui attività ignorate** non è disponibile.

   d. Se si desidera che un'attività venga sospesa da Kaspersky Endpoint Security quando le risorse del computer sono limitate, selezionare la casella di controllo **Esegui solo quando il computer è inattivo**.

   Questa opzione di pianificazione consente di ridurre l'utilizzo delle risorse del computer.
5. Fare clic su **OK**.
6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Gestione dei rapporti

In questa sezione viene descritto come configurare le impostazioni dei rapporti e come gestire i rapporti.

## Principi di gestione dei rapporti

Nei rapporti vengono registrate informazioni sulle operazioni di Kaspersky Endpoint Security, sulle prestazioni di ogni attività di scansione, aggiornamento, controllo integrità e scansione delle vulnerabilità e sull'esecuzione complessiva dell'applicazione.

I dati dei rapporti sono presentati in una tabella, che contiene un elenco di eventi. 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 del grafico. Gli eventi registrati durante l'esecuzione dei vari componenti e attività hanno diversi set di attributi.

Sono disponibili i seguenti rapporti:

- Rapporto **Controllo 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.
- Rapporto **Tutti i componenti della protezione**. Contiene informazioni sugli eventi registrati durante l'esecuzione dei seguenti componenti di Kaspersky Endpoint Security:
  - Anti-Virus File
  - Anti-Virus Posta.
  - Anti-Virus Web.
  - Anti-Virus IM.
  - System Watcher.
  - Firewall.
  - Prevenzione attacchi di rete.
  - Prevenzione unità USB dannose.
- Rapporto sull'esecuzione di un componente o un'attività di Kaspersky Endpoint Security.
- Rapporto **Criptaggio**. 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:

- **Eventi informativi**. Icona . Eventi formali che in genere non contengono informazioni importanti.
- **Eventi importanti**. Icona . Eventi a cui è necessario prestare attenzione perché riflettono situazioni importanti nel funzionamento di Kaspersky Endpoint Security.

- **Eventi critici**. Icona . 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.
- 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. Kaspersky Endpoint Security elimina tutte le voci nei rapporti selezionati, a partire dalla voce meno recente fino al momento attuale.

## Configurazione delle impostazioni dei rapporti

È possibile configurare le impostazioni dei rapporti nei seguenti modi:

- Configurare il 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. È possibile annullare il limite di tempo o modificare la durata massima per l'archiviazione dei rapporti.

- Configurare del 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. È possibile annullare la limitazione per la dimensione del file del rapporto o impostare un valore differente.

## Configurazione del periodo massimo di archiviazione dei rapporti

*Per modificare il periodo massimo di archiviazione dei rapporti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rapporti e Backup**.
3. Nella parte destra della finestra, nella sezione **Parametri rapporto**, eseguire una delle seguenti operazioni:

- Per ridurre il periodo di archiviazione dei rapporti, selezionare la casella di controllo **Mantieni i rapporti per non più di**. Nel campo accanto alla casella di controllo **Mantieni i rapporti per non più di** specificare il periodo massimo di archiviazione dei rapporti.

  Per impostazione predefinita, il periodo massimo di archiviazione dei rapporti è di 30 giorni.

- Per annullare il limite per il periodo di archiviazione dei rapporti, deselezionare la casella di controllo **Mantieni i rapporti per non più di**.

Per impostazione predefinita, il limite per il periodo di archiviazione dei rapporti è abilitato.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione della dimensione massima dei file del rapporto

*Per configurare la dimensione massima dei file dei rapporti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rapporti e Backup**.
3. Nella parte destra della finestra, nella sezione **Parametri rapporto**, eseguire una delle seguenti operazioni:

   - Per limitare la dimensione del file del rapporto, selezionare la casella di controllo **Dimensione massima dei file**. Nel campo a destra della casella di controllo **Dimensione massima dei file** specificare la dimensione massima dei file del rapporto.

     Per impostazione predefinita, la dimensione del file del rapporto è 1024 MB.

   - Per rimuovere la limitazione per la dimensione del file del rapporto, deselezionare la casella di controllo **Dimensione massima dei file**.

   Per impostazione predefinita, il limite per la dimensione del file del rapporto è abilitato.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Visualizzazione dei rapporti

*Per visualizzare i rapporti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Rapporti** per aprire la finestra **Rapporti**.
3. Per generare il rapporto Tutti i componenti della protezione, nella parte sinistra della finestra **Rapporti** selezionare **Tutti i componenti della protezione** nell'elenco dei componenti e delle attività.

   Nella parte destra della finestra viene visualizzato il rapporto Tutti i componenti di protezione, che contiene un elenco degli eventi che si sono verificati durante l'esecuzione di tutti i componenti di protezione di Kaspersky Endpoint Security.

4. Per generare un rapporto sull'esecuzione di un componente o un'attività, nella parte sinistra della finestra **Rapporti** selezionare un componente o un'attività nell'elenco dei componenti e delle 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.

Per impostazione predefinita, gli eventi dei rapporti sono disposti in ordine crescente in base ai valori nella colonna **Data evento**.

## Visualizzazione di informazioni sugli eventi in un rapporto

È possibile visualizzare un riepilogo dettagliato di ogni evento nel rapporto.

*Per visualizzare un riepilogo dettagliato di un evento nel rapporto:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Rapporti** per aprire la finestra **Rapporti**.
3. Nella parte sinistra della finestra selezionare il rapporto desiderato sul componente o sull'attività.

   Gli eventi inclusi nell'ambito del rapporto sono visualizzati nella tabella nella parte destra della finestra. Per trovare eventi specifici nel rapporto, utilizzare le funzioni di filtro, ricerca e ordinamento.
4. Selezionare l'evento desiderato nel rapporto.

Una sezione con il riepilogo dell'evento viene visualizzata nella parte inferiore della finestra.

## Salvataggio di un rapporto in un file

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. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Rapporti** per aprire la finestra **Rapporti**.
3. Eseguire una delle seguenti operazioni:

   - Per generare il rapporto "Tutti i componenti della protezione", selezionare **Tutti i componenti della protezione** nell'elenco dei componenti e delle attività.

     Nella parte destra della finestra viene visualizzato il rapporto "Tutti i componenti di protezione", che contiene un elenco degli eventi che si sono verificati durante l'esecuzione di tutti i componenti di protezione.

   - Per generare un rapporto sull'esecuzione di un componente o un'attività, selezionare il componente o l'attività nell'elenco dei componenti e delle 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.

4. 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
5. Fare clic sul pulsante **Salva rapporto** nella parte superiore destra della finestra.

   Verrà visualizzato un menu di scelta rapida.
6. Nel menu di scelta rapida selezionare la codifica per salvare il file del rapporto: **Salva come ANSI** o **Salva come Unicode**.

   Verrà visualizzata la finestra standard di Microsoft Office **Salva con nome**.
7. Nella finestra **Salva con nome** specificare la cartella di destinazione per il file del rapporto.
8. Nel campo **Nome del file** digitare il nome del file del rapporto.
9. Nel campo **Tipo di file** selezionare il formato desiderato per il file del rapporto: TXT o CSV.
10. Fare clic sul pulsante **Salva**.

## Eliminazione dei rapporti

*Per rimuovere le informazioni dai rapporti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rapporti e Backup**.
3. Nella parte destra della finestra, nella sezione **Parametri rapporto**, fare clic sul pulsante **Elimina rapporti**.

   Verrà visualizzata la finestra **Eliminazione dei rapporti**.
4. Selezionare le caselle di controllo accanto ai rapporti di cui si desidera eliminare le informazioni:
   - **Tutti i rapporti**.
   - **Rapporto sulla protezione generale**. Contiene informazioni sulle operazioni dei seguenti componenti di Kaspersky Endpoint Security:
     - Anti-Virus File
     - Anti-Virus Posta.
     - Anti-Virus Web.

- Anti-Virus IM.
- System Watcher.
- Firewall.
- Prevenzione attacchi di rete.
- Prevenzione unità USB dannose.

- **Rapporto sulle attività di scansione**. Contiene informazioni sulle attività di scansione completate:
  - Scansione Completa
  - Scansione delle aree critiche
  - Scansione Personalizzata
  - Controllo integrità.
- **Rapporto attività di aggiornamento**. Contiene informazioni sulle attività di aggiornamento completate:
- **Rapporto del firewall**. Contiene informazioni sulle operazioni di Firewall.
- **Rapporto componenti di controllo**. Contiene informazioni sulle operazioni dei seguenti componenti di Kaspersky Endpoint Security:
  - Controllo avvio applicazioni.
  - Controllo privilegi applicazioni.
  - Monitor vulnerabilità.
  - Controllo dispositivi.
  - Controllo Web.
- **Rapporto sul criptaggio dei dati**.

5. Fare clic su **OK**.

# Servizio di notifica

Questa sezione contiene informazioni sul servizio di notifica utilizzato per segnalare agli utenti gli eventi che si verificano durante l'esecuzione di Kaspersky Endpoint Security, oltre a istruzioni per la configurazione dei parametri di notifica.

## Informazioni sulle notifiche di Kaspersky Endpoint Security

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.

## Configurazione del servizio di notifica

È possibile eseguire le seguenti azioni per configurare il servizio di notifica:

- Configurare le impostazioni dei registri eventi utilizzati da Kaspersky Endpoint Security per la registrazione degli eventi.
- Configurare la modalità di visualizzazione delle notifiche sullo schermo.
- Configurare l'invio delle notifiche e-mail.

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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rapporti e Backup**.

   Nella parte destra della finestra vengono visualizzate le impostazioni di Rapporti e Backup.
3. Nella sezione **Notifiche** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Notifiche**.

   I componenti e le attività di Kaspersky Endpoint Security sono visualizzati nella parte sinistra della finestra. Nella parte destra della finestra sono elencati gli eventi generati per l'attività o il componente selezionato.
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 registro locale** e **Salva nel registro eventi di Windows**.

   Gli eventi per cui sono selezionate le caselle di controllo nella colonna **Salva nel registro locale** sono visualizzati in **Log di applicazioni e servizi** nella sezione **Registro eventi Kaspersky**. Gli eventi per cui sono selezionate le caselle di controllo nella colonna **Salva nel registro eventi di Windows** sono visualizzati in **Registri di Windows** nella sezione **Applicazione**. Per aprire i registri eventi, fare clic su **Start** → **Pannello di controllo** → **Amministrazione** → **Visualizzatore eventi**.
6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione della visualizzazione e dell'invio delle notifiche

*Per configurare la visualizzazione e l'invio delle notifiche:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rapporti e Backup**.

   Nella parte destra della finestra vengono visualizzate le impostazioni di Rapporti e Backup.
3. Nella sezione **Notifiche** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Notifiche**.

   I componenti e le attività di Kaspersky Endpoint Security sono visualizzati nella parte sinistra della finestra. Nella parte destra della finestra sono elencati gli eventi generati per l'attività o il componente selezionato.
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 elementi desiderati.

   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 elementi desiderati.

   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 sul pulsante **Impostazioni delle notifiche via e-mail**.

   Verrà visualizzata la finestra **Impostazioni delle notifiche via e-mail**.

8. Selezionare la casella di controllo **Invia notifiche degli eventi** per abilitare l'invio delle informazioni sugli eventi di Kaspersky Endpoint Security selezionati nella colonna **Notifica tramite e-mail**.

9. Specificare le impostazioni per l'invio delle notifiche tramite e-mail.

10. Fare clic su **OK**.

11. Nella finestra **Impostazioni delle notifiche via e-mail** fare clic su **OK**.

12. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Interfaccia**.

   Le impostazioni dell'interfaccia di Kaspersky Endpoint Security sono visualizzate nella parte destra della finestra.

3. Nella sezione **Avvisi** 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. Per salvare le modifiche, fare clic sul pulsante **Salva**.

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.

# Gestione di Quarantena e Backup

In questa sezione viene descritto come configurare e gestire Quarantena e Backup.

## Informazioni su Quarantena e Backup

La *quarantena* è un elenco di file potenzialmente infetti. I *file potenzialmente infetti* sono file che possono contenere virus e altre minacce o varianti di tali minacce.

Quando Kaspersky Endpoint Security mette in quarantena un file potenzialmente infetto, non copia il file, ma lo sposta: l'applicazione elimina il file dal disco rigido o dal messaggio e-mail e lo salva in uno speciale archivio di dati. I file in quarantena vengono salvati in un formato speciale e non rappresentano una minaccia.

Kaspersky Endpoint Security può rilevare e mettere in quarantena un file potenzialmente infetto durante l'esecuzione di una scansione virus, nonché durante l'esecuzione dei componenti della protezione Anti-Virus File, Anti-Virus Posta e System Watcher.

I file sono messi in quarantena da Kaspersky Endpoint Security nei seguenti casi:

- Il codice del file ricorda un programma dannoso noto ma parzialmente modificato o ha una struttura simile a quella di un malware e non è elencato nel database di Kaspersky Endpoint Security. In questo caso, il file viene messo in quarantena dopo l'analisi euristica eseguita da Anti-Virus File e Anti-Virus Posta o durante una scansione virus. In rari casi, l'analisi euristica causa falsi positivi.

- La sequenza delle operazioni eseguite da un file è pericolosa. In questo caso, il file viene messo in quarantena dopo che il componente System Watcher ne ha analizzato il comportamento.

*Backup* è un elenco di copie di backup dei file che sono stati eliminati o modificati durante il processo di disinfezione. Una *copia di backup* è una copia di un file creata al primo tentativo di disinfettare o eliminare il file. Le copie di backup dei file vengono archiviate in un formato speciale e non rappresentano una minaccia.

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 la copia disinfettata del file nella cartella originale.

Dopo un successivo aggiornamento del database e dei moduli software dell'applicazione, Kaspersky Endpoint Security può identificare definitivamente la minaccia e neutralizzarla. È pertanto consigliabile sottoporre a scansione i file in quarantena dopo ogni aggiornamento dei database e dei moduli software dell'applicazione.

## Configurazione delle impostazioni di Quarantena e Backup

L'archiviazione dei dati include Quarantena e Backup. È possibile configurare le impostazioni di Quarantena e Backup nel modo seguente:

- Configurare il periodo massimo di archiviazione per i file in Quarantena e le copie dei file in Backup.

  Per impostazione predefinita, il periodo massimo di archiviazione per i file in Quarantena e le copie dei file in Backup è 30 giorni. Al termine del periodo massimo di archiviazione, Kaspersky Endpoint Security elimina i file meno recenti dall'archiviazione dei dati. È possibile annullare il limite di tempo o modificare il periodo massimo di archiviazione per i file.

- È possibile configurare la dimensione massima di Quarantena e Backup.

Per impostazione predefinita, la dimensione massima di Quarantena e Backup è 100 MB. Quando l'archiviazione dei dati raggiunge il limite, Kaspersky Endpoint Security elimina automaticamente i file meno recenti da Quarantena e Backup per evitare il superamento della dimensione massima per l'archiviazione dei dati. È possibile annullare il limite per la dimensione di Quarantena e Backup o modificare la dimensione massima.

## Configurazione del periodo massimo di archiviazione per i file in Quarantena e le copie dei file in Backup

*Per configurare il periodo massimo di archiviazione per i file in Quarantena e le copie dei file in Backup:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rapporti e Backup**.
3. Eseguire una delle seguenti operazioni:
   - Per limitare il periodo di archiviazione dei file in Quarantena e Backup, nella sezione **Impostazioni di quarantena e backup** nella parte destra della finestra selezionare la casella di controllo **Mantieni gli oggetti per non più di**. Nel campo a destra della casella di controllo **Mantieni gli oggetti per non più di**, specificare il periodo massimo di archiviazione per i file in Quarantena e le copie dei file in Backup. Per impostazione predefinita, il periodo di archiviazione per i file in Quarantena e le copie dei file in Backup è limitato a 30 giorni.
   - Per annullare il limite per il periodo di archiviazione dei file in Quarantena e Backup, nella sezione **Impostazioni di quarantena e backup** nella parte destra della finestra selezionare la casella di controllo **Mantieni gli oggetti per non più di**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Configurazione della dimensione massima di Quarantena e Backup

*Per configurare la dimensione massima di Quarantena e Backup:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rapporti e Backup**.
3. Eseguire una delle seguenti operazioni:
   - Per limitare le dimensioni totali di Quarantena e Backup, selezionare la casella di controllo **Dimensione massima archivio** nella parte destra della finestra nella sezione **Impostazioni di quarantena e backup** e specificare le dimensioni massime di Quarantena e Backup nel campo a destra della casella di controllo **Dimensione massima archivio**.

     Per impostazione predefinita, la dimensione massima di archiviazione per i dati (incluse la directory Quarantena e le copie di backup dei file) è 100 MB.
   - Per rimuovere il limite per le dimensioni di Quarantena e Backup, deselezionare la casella di controllo **Dimensione massima archivio** nella parte destra della finestra nella sezione **Impostazioni di quarantena e backup**.

Le dimensioni di Quarantena e Backup sono illimitate per impostazione predefinita.

4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Gestione della quarantena

Kaspersky Endpoint Security elimina i file automaticamente con qualsiasi stato da Quarantena allo scadere del periodo di archiviazione definito nelle impostazioni dell'applicazione.

Durante la gestione della quarantena sono disponibili le seguenti operazioni sui file:

- Visualizzare i file in quarantena da Kaspersky Endpoint Security.
- Esaminare i file potenzialmente infetti utilizzando la versione corrente dei database e dei moduli di Kaspersky Endpoint Security.
- Ripristinare i file dalla quarantena nelle cartelle originali.
- Rimuovere i file dalla quarantena.
- Aprire le cartelle in cui erano originariamente posizionati i file.

Il set di file in quarantena viene presentato sotto forma di tabella.

È inoltre possibile eseguire le seguenti azioni durante la gestione dei dati nella tabella:

- Filtrare i file in quarantena in base alle colonne e a condizioni di filtro personalizzate.
- Utilizzare la funzione di ricerca dei file in quarantena.
- Ordinare i file in quarantena.
- Modificare l'ordine e il set di colonne visualizzate nella tabella dei file in quarantena.

È possibile copiare negli Appunti gli eventi relativi a Quarantena selezionati. Per selezionare più file in quarantena, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di qualsiasi file e scegliere **Seleziona tutto**. Per deselezionare i file di cui non si desidera eseguire la scansione, fare clic su di essi tenendo premuto **CTRL**.

## Abilitazione e disabilitazione della scansione dei file in Quarantena dopo un aggiornamento

Se durante la scansione di un file vengono rilevati segni di infezione, ma non è possibile determinare lo specifico programma dannoso che ha causato l'infezione, Kaspersky Endpoint Security sposta il file in Quarantena. Kaspersky Endpoint Security può identificare definitivamente le minacce e neutralizzarle una volta eseguito l'aggiornamento dei database e dei moduli dell'applicazione. È possibile abilitare la scansione automatica dei file in quarantena dopo ogni aggiornamento dei database e dei moduli dell'applicazione.

È consigliabile aggiornare periodicamente i file in quarantena. La scansione potrebbe modificare lo stato dei file. Alcuni file potrebbero essere disinfettati e ripristinati nelle posizioni originali, in modo che l'utente possa continuare a utilizzarli.

*Per abilitare la scansione dei file in quarantena dopo gli aggiornamenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rapporti e Backup**.

   Nella parte destra della finestra sono visualizzate le impostazioni di gestione per rapporti e archivi.
3. Nella sezione **Impostazioni di quarantena e backup** eseguire una delle seguenti operazioni:
   - Per abilitare la scansione dei file in quarantena dopo ogni aggiornamento di Kaspersky Endpoint Security, selezionare la casella di controllo **Ripeti la scansione degli oggetti in Quarantena dopo l'aggiornamento**.
   - Per disabilitare la scansione dei file in quarantena dopo ogni aggiornamento di Kaspersky Endpoint Security, deselezionare la casella di controllo **Ripeti la scansione degli oggetti in Quarantena dopo l'aggiornamento**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Avvio di un'attività Scansione Personalizzata per i file in quarantena

Dopo un aggiornamento dei database e dei moduli software dell'applicazione, Kaspersky Endpoint Security è in grado di identificare e di neutralizzare le minacce contenute nei file in quarantena. Se l'applicazione non è configurata per la scansione automatica dei file in quarantena dopo ogni aggiornamento dei database e dei moduli dell'applicazione, è possibile avviare manualmente un'attività Scansione Personalizzata per i file in quarantena.

*Per avviare un'attività Scansione Personalizzata per i file in quarantena:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.

   Verrà visualizzata la scheda **Quarantena** della finestra **Archivi**.
3. Nella scheda **Quarantena** selezionare uno o più file potenzialmente infetti da esaminare.

   Per selezionare più file in quarantena, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di qualsiasi file e scegliere **Seleziona tutto**. Per deselezionare i file di cui non si desidera eseguire la scansione, fare clic su di essi tenendo premuto **CTRL**.
4. Avviare l'attività Scansione Personalizzata in uno dei seguenti modi:
   - Fare clic sul pulsante **Ripeti scansione**.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Ripeti scansione**.

Al termine della scansione, viene visualizzata una notifica con il numero di file esaminati e il numero di minacce rilevate.

## Ripristino di file dalla quarantena

*Per ripristinare i file in quarantena:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.

   Verrà visualizzata la scheda **Quarantena** della finestra **Archivi**.
3. Per ripristinare tutti i file in quarantena, selezionare **Ripristina tutto** dal menu di scelta rapida di qualsiasi file.

   Kaspersky Endpoint Security ripristina tutti i file dalla quarantena nelle cartelle originali.
4. Per ripristinare uno o più file in quarantena:

   a. Nella scheda **Quarantena** selezionare uno o più file da ripristinare dalla quarantena.

      Per selezionare più file in quarantena, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di qualsiasi file e scegliere **Seleziona tutto**. Per deselezionare i file di cui non si desidera eseguire la scansione, fare clic su di essi tenendo premuto **CTRL**.

   b. Ripristinare i file in uno dei seguenti modi:

      - Fare clic sul pulsante **Ripristina**.
      - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Ripristina**.

   I file selezionati verranno ripristinati nelle cartelle originali.

## Eliminazione di file dalla quarantena

*Per eliminare i file in quarantena:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.

   Verrà visualizzata la scheda **Quarantena** della finestra **Archivi**.
3. Per eliminare tutti i file in quarantena, selezionare **Elimina tutto** del menu di scelta rapida di qualsiasi file.

   Kaspersky Endpoint Security elimina tutti i file dalla quarantena.
4. Per eliminare uno o più file in quarantena:

   a. Nella tabella nella scheda **Quarantena** selezionare uno o più file potenzialmente infetti da eliminare dalla quarantena.

      Per selezionare più file in quarantena, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di qualsiasi file e scegliere **Seleziona tutto**. Per deselezionare i file di cui non si desidera eseguire la scansione, fare clic su di essi tenendo premuto **CTRL**.

   b. Eliminare i file in uno dei seguenti modi:

      - Fare clic sul pulsante **Rimuovi**.
      - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Elimina**.

Kaspersky Endpoint Security elimina i file selezionati dalla quarantena.

## Gestione di Backup

Se nel file viene rilevato codice dannoso, Kaspersky Endpoint Security blocca il file, 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.

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*).

Kaspersky Endpoint Security elimina automaticamente da Backup le copie di backup dei file con qualsiasi stato allo scadere del periodo di archiviazione definito nelle impostazioni dell'applicazione.

È anche possibile eliminare manualmente la copia di un file da Backup.

Il set di copie di backup dei file viene presentato sotto forma di tabella.

Durante la gestione di Backup, è possibile eseguire le seguenti azioni sulle copie di backup dei file:

- Visualizzare il set di copie di backup dei file.
- Ripristinare i file dalle copie di backup nelle cartelle originali.
- Eliminare le copie di backup dei file da Backup.

È inoltre possibile eseguire le seguenti azioni durante la gestione dei dati nella tabella:

- Filtrare le copie di backup per colonne, anche per condizioni di filtro personalizzate.
- Utilizzare la funzione di ricerca delle copie di backup.
- Ordinare le copie di backup.
- Modificare l'ordine e il set di colonne visualizzate nella tabella delle copie di backup.

È possibile copiare negli Appunti gli eventi relativi a Backup selezionati. Per selezionare più file di backup, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di qualsiasi file e scegliere **Seleziona tutto**. Per deselezionare i file di cui non si desidera eseguire la scansione, fare clic su di essi tenendo premuto **CTRL**.

## Ripristino di file da Backup

*Per ripristinare i file da Backup:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.

3. Nella finestra **Archivi** selezionare la scheda **Backup**.

4. Per ripristinare tutti i file da Backup, selezionare **Ripristina tutto** del menu di scelta rapida di qualsiasi file.

   Tutti i file verranno ripristinati nelle cartelle originali dalle copie di backup.

5. Per ripristinare uno o più file da Backup:

   a. Nella tabella, nella scheda **Backup**, selezionare uno o più file di backup.

      Per selezionare più file in quarantena, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di qualsiasi file e scegliere **Seleziona tutto**. Per deselezionare i file di cui non si desidera eseguire la scansione, fare clic su di essi tenendo premuto **CTRL**.

   b. Ripristinare i file in uno dei seguenti modi:

      - Fare clic sul pulsante **Ripristina**.
      - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Ripristina**.

   I file verranno ripristinati nelle cartelle originali dalle copie di backup selezionate.

## Eliminazione delle copie di backup dei file da Backup

*Per eliminare le copie di backup dei file da Backup:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte superiore della finestra principale dell'applicazione fare clic sul collegamento **Quarantena** per aprire la finestra **Archivi**.

3. Nella finestra **Archivi** selezionare la scheda **Backup**.

4. Se si desidera eliminare tutti i file da Backup, eseguire una delle seguenti azioni:

   - Nel menu di scelta rapida di qualsiasi file selezionare **Elimina tutto**.
   - Fare clic sul pulsante **Cancella archivio**.

   Kaspersky Endpoint Security eliminerà tutte le copie di backup dei file da Backup.

5. Per eliminare uno o più file da Backup:

   a. Nella tabella, nella scheda **Backup**, selezionare uno o più file di backup.

      Per selezionare più file di backup, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida di qualsiasi file e scegliere **Seleziona tutto**. Per deselezionare i file di cui non si desidera eseguire la scansione, fare clic su di essi tenendo premuto **CTRL**.

   b. Eliminare i file in uno dei seguenti modi:

      - Fare clic sul pulsante **Rimuovi**.

- Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Elimina**.

Kaspersky Endpoint Security eliminerà le copie di backup dei file selezionate da Backup.

# Impostazioni avanzate dell'applicazione

Questa sezione descrive le impostazioni avanzate di Kaspersky Endpoint Security e il modo in cui possono essere configurate.

# 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 kit 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni avanzate dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Gestione impostazioni** fare clic sul pulsante **Salva**.

   Verrà visualizzata la finestra standard di Microsoft Windows **Selezionare un file di configurazione**.
4. Specificare il percorso in cui 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. Fare clic sul pulsante **Salva**.

*Per importare le impostazioni di Kaspersky Endpoint Security da un file di configurazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni avanzate dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Gestione impostazioni** fare clic sul pulsante **Caricamento**.

   Verrà visualizzata la finestra standard di Microsoft Windows **Selezionare un file di configurazione**.
4. Specificare il percorso del file di configurazione.
5. Fare clic sul pulsante **Apri**.

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

# Area attendibile

Questa sezione contiene informazioni sull'area attendibile e istruzioni per la configurazione delle esclusioni dalla scansione e la creazione di un elenco di applicazioni attendibili.

# Informazioni sull'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. In altre parole, è un set di esclusioni dalla scansione.

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.

È possibile escludere i seguenti oggetti della scansione:

- File di particolari formati
- File selezionati tramite una maschera
- File selezionati
- Cartelle
- Processi delle applicazioni

## Esclusioni dalla scansione

Un'*esclusione dalla scansione* è un set di condizioni in base alle quali Kaspersky Endpoint Security non esegue la scansione di un 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 utilizzate come un componente ausiliario del malware. Le applicazioni di questo tipo includono strumenti di amministrazione remota, client IRC, server FTP, utilità per sospendere o nascondere processi, keylogger, programmi per l'hackeraggio delle password e auto-dialer. Tali applicazioni non vengono classificate come virus. I dettagli sul software legittimo che potrebbe essere utilizzato da utenti malintenzionati per danneggiare il computer o i dati dell'utente sono disponibili nell'Enciclopedia dei virus di Kaspersky Lab, all'indirizzo https://encyclopedia.kaspersky.com/knowledge/riskware/.

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 dei virus di Kaspersky. È ad esempio possibile che si utilizzi frequentemente un programma di amministrazione remota. Si tratta di un'applicazione di accesso remoto che consente di controllare un computer in modalità remota. 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 dei virus 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 questo comportamento, è possibile escludere l'applicazione dalla scansione configurando Kaspersky Endpoint Security come illustrato in questo documento.

Le esclusioni dalla scansione possono essere utilizzate dai seguenti componenti e attività dell'applicazione configurati dall'amministratore di sistema:

- Anti-Virus File
- Anti-Virus Posta.
- Anti-Virus Web.
- Controllo privilegi applicazioni.
- Attività di scansione
- System Watcher.

### 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 programma e controlla l'attività di tutte le applicazioni e il traffico di rete che generano. Kaspersky Endpoint Security esclude dalla scansione le applicazioni nell'elenco delle applicazioni attendibili.

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.

## Creazione di un'esclusione dalla 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.

*Per creare un'esclusione dalla scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Protezione anti-virus** a sinistra.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la scheda **Esclusioni dalla scansione** della finestra **Area attendibile**.
4. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Esclusione dalla scansione**. In questa finestra è possibile creare un'esclusione dalla scansione utilizzando uno o entrambi i criteri nella sezione **Proprietà**.
5. 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 **selezionare il file o la cartella** nella sezione **Descrizione dell'esclusione dalla scansione** 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 **Sfoglia**.

   Nella maschera per il nome di un file o di una cartella è possibile utilizzare il carattere asterisco (*) per sostituire qualsiasi set di caratteri nel nome del file.

   È ad esempio possibile utilizzare le maschere per aggiungere i seguenti percorsi:

   - I percorsi dei file che si trovano in qualsiasi cartella:
     - La maschera "*.exe" includerà tutti i percorsi dei file con estensione EXE.
     - La maschera "test" includerà tutti i percorsi dei file con il nome "test".
   - I percorsi dei file che si trovano in una cartella specificata:
     - La maschera "C:\dir*.*" includerà tutti i percorsi dei file che si trovano nella cartella C:\dir\, ma non nelle sottocartelle di C:\dir\.
     - La maschera "C:\dir*" includerà tutti i percorsi dei file che si trovano nella cartella C:\dir\, ma non nelle sottocartelle di C:\dir\.
     - La maschera "C:\dir\" includerà tutti i percorsi dei file che si trovano nella cartella C:\dir\, ma non nelle sottocartelle di C:\dir\.
     - La maschera "C:\dir*.exe" includerà tutti i percorsi dei file con estensione EXE che si trovano nella cartella C:\dir\, ma non nelle sottocartelle di C:\dir\.
     - La maschera "C:\dir\test" includerà tutti i percorsi dei file con il nome "test" che si trovano nella cartella C:\dir\, ma non nelle sottocartelle di C:\dir\.
     - La maschera "C:\dir*\test" includerà tutti i percorsi dei file con il nome "test" che si trovano nella cartella C:\dir\ e nelle sottocartelle di C:\dir\.
   - I percorsi dei file che si trovano in tutte le cartelle con un nome specificato:

- La maschera "dir*.*" includerà tutti i percorsi dei file nelle cartelle con il nome "dir", ma non nelle sottocartelle di tali cartelle.
- La maschera "dir*" includerà tutti i percorsi dei file nelle cartelle con il nome "dir", ma non nelle sottocartelle di tali cartelle.
- La maschera "dir\" includerà tutti i percorsi dei file nelle cartelle con il nome "dir", ma non nelle sottocartelle di tali cartelle.
- La maschera "dir*.exe" includerà tutti i percorsi dei file con estensione EXE nelle cartelle con il nome "dir", ma non nelle sottocartelle di tali cartelle.
- La maschera "dir\test" includerà tutti i percorsi dei file con il nome "test" nelle cartelle con il nome "dir", ma non nelle sottocartelle di tali cartelle.

d. Nella finestra **Nome del file o della cartella** fare clic su **OK**.

Nella sezione **Descrizione dell'esclusione dalla scansione** della finestra **Esclusione dalla scansione** viene visualizzato un collegamento al file o alla cartella aggiunta.

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

a. Nella sezione **Proprietà** selezionare la casella di controllo **Nome dell'oggetto**.

b. Fare clic sul collegamento **inserire il nome dell'oggetto** nella sezione **Descrizione dell'esclusione dalla scansione** per aprire la finestra **Nome dell'oggetto**.

c. Immettere il nome dell'oggetto o la maschera per il nome in base alla classificazione dell'Enciclopedia dei virus di Kaspersky:

d. Fare clic su **OK** nella finestra **Nome dell'oggetto**.

Nella sezione **Descrizione dell'esclusione dalla scansione** della finestra **Esclusione dalla scansione** viene visualizzato un collegamento al nome dell'oggetto aggiunto.

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

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

a. Fare clic sul collegamento **qualsiasi** nella sezione **Descrizione dell'esclusione dalla scansione** per attivare il collegamento **selezionare il componente**.

b. Fare clic sul collegamento **selezionare il componente** per visualizzare la finestra **Componenti della protezione**.

c. Selezionare le caselle di controllo accanto ai componenti a cui deve essere applicata l'esclusione dalla scansione.

d. Nella finestra **Componenti della protezione** fare clic su **OK**.

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.

9. Nella finestra **Esclusione dalla scansione** fare clic su **OK**.

L'esclusione dalla scansione aggiunta viene visualizzata nella tabella disponibile nella scheda **Esclusioni dalla scansione** della finestra **Area attendibile**. Le impostazioni configurate per l'esclusione dalla scansione sono visualizzate nella sezione **Descrizione dell'esclusione dalla scansione**.

10. Nella finestra **Area attendibile** fare clic su **OK**.

11. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica di un'esclusione dalla scansione

*Per modificare un'esclusione dalla scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Selezionare la sezione **Protezione anti-virus** a sinistra.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.

3. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la scheda **Esclusioni dalla scansione** della finestra **Area attendibile**.

4. Selezionare nell'elenco l'esclusione dalla scansione che si desidera modificare.

5. Modificare le impostazioni dell'esclusione dalla scansione utilizzando uno dei seguenti metodi:

   - Fare clic sul pulsante **Modifica**.

     Verrà visualizzata la finestra **Esclusioni dalla scansione**.

   - Aprire la finestra per la modifica dell'impostazione desiderata facendo clic sul collegamento nel campo **Descrizione dell'esclusione dalla scansione**.

6. Se è stato fatto clic sul pulsante **Modifica** durante il passaggio precedente, fare clic su **OK** nella finestra **Esclusione dalla scansione**.

   Le impostazioni modificate per l'esclusione dalla scansione sono visualizzate nella sezione **Descrizione dell'esclusione dalla scansione**.

7. Nella finestra **Area attendibile** fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Eliminazione di un'esclusione dalla scansione

*Per eliminare un'esclusione dalla scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Selezionare la sezione **Protezione anti-virus** a sinistra.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.

3. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Impostazioni**.

Verrà visualizzata la scheda **Esclusioni dalla scansione** della finestra **Area attendibile**.

4. Selezionare l'esclusione dalla scansione desiderata nell'elenco delle esclusioni dalla scansione.
5. Fare clic sul pulsante **Rimuovi**.
   L'esclusione dalla scansione eliminata non è più visualizzata nell'elenco.
6. Nella finestra **Area attendibile** fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Abilitazione e disabilitazione di un'esclusione dalla scansione

*Per abilitare o disabilitare un'esclusione dalla scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Protezione anti-virus** a sinistra.
   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Impostazioni**.
   Verrà visualizzata la scheda **Esclusioni dalla scansione** della finestra **Area attendibile**.
4. Selezionare l'esclusione desiderata nell'elenco delle esclusioni dalla scansione.
5. Eseguire una delle seguenti operazioni:
   - Per abilitare un'esclusione dalla scansione, selezionare la casella di controllo accanto al nome dell'esclusione dalla scansione.
   - Per disabilitare un'esclusione dalla scansione, deselezionare la casella di controllo accanto al nome dell'esclusione dalla scansione.
6. Fare clic su **OK**.
7. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Modifica dell'elenco di applicazioni attendibili

*Per modificare l'elenco di applicazioni attendibili:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Protezione anti-virus** a sinistra.
   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Impostazioni**.
   Verrà visualizzata la finestra **Area attendibile**.

4. Nella finestra **Area attendibile** selezionare la scheda **Applicazioni attendibili**.

5. Per aggiungere un'applicazione all'elenco di applicazioni attendibili:

   a. Fare clic sul pulsante **Aggiungi**.

   b. Nel menu di scelta rapida visualizzato eseguire una delle seguenti operazioni:

   - Per trovare l'applicazione nell'elenco delle applicazioni installate nel computer, selezionare **Applicazioni** dal menu.

     Verrà visualizzata la finestra **Seleziona applicazione**.

   - Per specificare il percorso del file eseguibile dell'applicazione desiderata, selezionare **Sfoglia**.

     Verrà visualizzata la finestra standard di Microsoft Windows **Apri file**.

   c. Selezionare l'applicazione in uno dei seguenti modi:

   - Se è stato selezionato **Applicazioni** durante il passaggio precedente, selezionare l'applicazione nell'elenco delle applicazioni installate nel computer e fare clic su **OK** nella finestra **Seleziona applicazione**.

   - Se è stato selezionato **Sfoglia** durante il passaggio precedente, specificare il percorso del file eseguibile dell'applicazione e fare clic sul pulsante **Apri** nella finestra standard **Apri** di Microsoft Windows.

   Queste azioni determinano l'apertura della finestra **Esclusioni dalla scansione per l'applicazione**.

   a. Selezionare le caselle di controllo accanto alle regole dell'area attendibile appropriate per l'applicazione selezionata:

   - **Non esaminare i file aperti**.
   - **Non monitorare l'attività dell'applicazione**.
   - **Non ereditare restrizioni del processo principale (applicazione)**.
   - **Non monitorare l'attività dell'applicazione figlia**.
   - **Non bloccare l'interazione con l'interfaccia dell'applicazione**.
   - **Non esaminare il traffico di rete**.

   b. Nella finestra **Esclusioni dalla scansione per l'applicazione** fare clic su **OK**.

   Le applicazioni attendibili che sono state aggiunte vengono visualizzate nell'elenco delle applicazioni attendibili.

6. Per modificare le impostazioni di un'applicazione attendibile:

   a. Selezionare l'applicazione attendibile nell'elenco delle applicazioni attendibili.

   b. Fare clic sul pulsante **Modifica**.

   c. Verrà visualizzata la finestra **Esclusioni dalla scansione per l'applicazione**.

   d. Selezionare o deselezionare le caselle di controllo accanto alle regole dell'area attendibile appropriate per l'applicazione selezionata:

Se non è selezionata alcuna regola dell'area attendibile nella finestra **Esclusioni dalla scansione per l'applicazione**, l'applicazione attendibile viene inclusa nella scansione. In questo caso, l'applicazione attendibile non viene rimossa dall'elenco delle applicazioni attendibili ma la casella di controllo è deselezionata.

e. Nella finestra **Esclusioni dalla scansione per l'applicazione** fare clic su **OK**.

7. Per rimuovere un'applicazione attendibile dall'elenco delle applicazioni attendibili:

   a. Selezionare l'applicazione attendibile nell'elenco delle applicazioni attendibili.

   b. Fare clic sul pulsante **Rimuovi**.

8. Nella finestra **Area attendibile** fare clic su **OK**.

9. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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. Aprire la finestra delle impostazioni dell'applicazione.

2. Selezionare la sezione **Protezione anti-virus** a sinistra.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.

3. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Area attendibile**.

4. Nella finestra **Area attendibile** selezionare la scheda **Applicazioni attendibili**.

5. Nell'elenco delle applicazioni attendibili selezionare l'applicazione attendibile desiderata.

6. Eseguire una delle seguenti operazioni:

   - Per escludere un'applicazione attendibile dalla scansione da parte di Kaspersky Endpoint Security, selezionare la casella di controllo accanto al nome dell'applicazione.

   - Per includere un'applicazione attendibile nella scansione da parte di Kaspersky Endpoint Security, deselezionare la casella di controllo accanto al nome dell'applicazione.

7. Fare clic su **OK**.

8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Protezione anti-virus** a sinistra.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Area attendibile**.
4. Nella finestra **Area attendibile** selezionare la scheda **Archivio di certificati di sistema attendibili**.
5. Selezionare la casella di controllo **Usa archivio di certificati di sistema attendibili**.
6. Nell'elenco a discesa **Archivio di certificati di sistema attendibili** selezionare l'archivio di sistema di Kaspersky Endpoint Security da considerare attendibile.
7. Nella finestra **Area attendibile** fare clic su **OK**.
8. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Auto-Difesa di Kaspersky Endpoint Security

In questa sezione vengono descritti i meccanismi Auto-Difesa e Difesa controllo remoto di Kaspersky Endpoint Security e vengono fornite istruzioni sulla configurazione delle relative impostazioni.

## Informazioni sulla funzionalità Auto-Difesa di Kaspersky Endpoint Security

Kaspersky Endpoint Security protegge il computer dai programmi dannosi, incluso il malware che tenta di bloccare le operazioni di Kaspersky Endpoint Security o perfino di eliminarlo dal computer.

La stabilità del sistema di protezione del computer è assicurata dalle funzionalità Auto-Difesa e Difesa controllo remoto 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.

*Difesa controllo remoto* blocca tutti i tentativi di controllare i servizi dell'applicazione da un computer remoto.

Nei computer con sistemi operativi a 64 bit è disponibile solo la funzionalità Auto-Difesa di Kaspersky Endpoint Security, che impedisce la modifica e l'eliminazione dei file dell'applicazione sul disco rigido e delle voci del Registro di sistema.

## Abilitazione o disabilitazione di Auto-Difesa

Il meccanismo Auto-Difesa di Kaspersky Endpoint Security è abilitato per impostazione predefinita. Se necessario, è possibile disabilitare Auto-Difesa.

*Per abilitare o disabilitare Auto-Difesa:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni avanzate dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Eseguire una delle seguenti operazioni:
   - Per abilitare il meccanismo Auto-Difesa, selezionare la casella di controllo **Abilita l'Auto-Difesa**.
   - Per disabilitare il meccanismo Auto-Difesa, deselezionare la casella di controllo **Abilita l'Auto-Difesa**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Abilitazione o disabilitazione di Difesa controllo remoto

Il meccanismo Difesa controllo remoto è abilitato per impostazione predefinita. Se necessario, è possibile disabilitare il meccanismo Difesa controllo remoto.

*Per abilitare o disabilitare il meccanismo Difesa controllo remoto:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni avanzate dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Eseguire una delle seguenti operazioni:
   - Per abilitare il meccanismo Difesa controllo remoto, selezionare la casella di controllo **Disabilita gestione esterna del servizio di sistema**.
   - Per disabilitare il meccanismo Difesa controllo remoto, deselezionare la casella di controllo **Disabilita gestione esterna del servizio di sistema**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Supporto delle applicazioni di amministrazione remota

Talvolta può essere necessario utilizzare un'applicazione di amministrazione remota mentre il controllo della protezione esterna è abilitato.

*Per consentire l'esecuzione di applicazioni di amministrazione remota:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Protezione anti-virus** a sinistra.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Esclusioni dalla scansione e applicazioni attendibili** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Area attendibile**.
4. Nella finestra **Area attendibile** selezionare la scheda **Applicazioni attendibili**.
5. Fare clic sul pulsante **Aggiungi**.
6. Nel menu di scelta rapida visualizzato eseguire una delle seguenti operazioni:

   - Per trovare l'applicazione di amministrazione remota nell'elenco delle applicazioni installate nel computer, selezionare **Applicazioni**.

     Verrà visualizzata la finestra **Seleziona applicazione**.
   - Per specificare il percorso del file eseguibile dell'applicazione di amministrazione remota, selezionare **Sfoglia**.

     Verrà visualizzata la finestra standard di Microsoft Windows **Apri file**.
7. Selezionare l'applicazione in uno dei seguenti modi:

   - Se è stato selezionato **Applicazioni** durante il passaggio precedente, selezionare l'applicazione nell'elenco delle applicazioni installate nel computer e fare clic su **OK** nella finestra **Seleziona applicazione**.
   - Se è stato selezionato **Sfoglia** durante il passaggio precedente, specificare il percorso del file eseguibile dell'applicazione e fare clic sul pulsante **Apri** nella finestra standard **Apri** di Microsoft Windows.

   Queste azioni determinano l'apertura della finestra **Esclusioni dalla scansione per l'applicazione**.
8. Selezionare la casella di controllo **Non monitorare l'attività dell'applicazione**.
9. Nella finestra **Esclusioni dalla scansione per l'applicazione** fare clic su **OK**.

   Le applicazioni attendibili che sono state aggiunte vengono visualizzate nell'elenco delle applicazioni attendibili.
10. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Prestazioni di Kaspersky Endpoint Security e compatibilità con altre applicazioni

Questa sezione contiene informazioni sulle prestazioni di Kaspersky Endpoint Security e sulla compatibilità con altre applicazioni, oltre a indicazioni per la selezione dei tipi di oggetti rilevabili e della modalità di esecuzione di Kaspersky Endpoint Security.

# Informazioni sulle prestazioni di Kaspersky Endpoint Security e sulla compatibilità con altre applicazioni

## Prestazioni di Kaspersky Endpoint Security

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 Scansione Vulnerabilità
- 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

L'utilizzo delle risorse del computer da parte di Kaspersky Endpoint Security può influire sulle 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 è in grado di sospendere le attività pianificate e concedere risorse ad altre applicazioni.

Diverse applicazioni, tuttavia, vengono avviate immediatamente dopo il rilascio delle risorse della CPU e sono eseguite in background. Per evitare che la scansione dipenda dalle prestazioni di altre applicazioni, è consigliabile non concedere loro le risorse del sistema operativo.

È possibile avviare tali attività manualmente, se necessario.

### Utilizzo della tecnologia avanzata di disinfezione.

Gli attuali programmi dannosi 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 i programmi dannosi 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 file server a causa delle specifiche di Kaspersky Endpoint Security per i file server. 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 un'infezione attiva di un file server, abilitare la tecnologia avanzata di disinfezione per i file server e avviare un'attività di gruppo *Scansione virus* in un momento appropriato per gli utenti del file server.

## Selezione dei tipi di oggetti rilevabili

*Per selezionare i tipi di oggetti rilevabili:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Protezione anti-virus**.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Oggetti** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Oggetti per il rilevamento**.
4. Selezionare le caselle di controllo accanto agli oggetti che si desidera che vengano rilevati da Kaspersky Endpoint Security:

   - **Strumenti dannosi**
   - **Adware**
   - **Auto-Dialer**

- **Altro**
- **File compressi potenzialmente pericolosi**
- **File con compressione multipla**

5. Fare clic su **OK**.

   La finestra **Oggetti per il rilevamento** verrà chiusa. Nella sezione **Oggetti** i tipi di oggetti selezionati vengono elencati in **Rilevamento dei seguenti tipi di oggetti abilitato**.

6. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Abilitazione o disabilitazione della tecnologia avanzata di disinfezione per le workstation

*Per abilitare o disabilitare la tecnologia avanzata di disinfezione per le workstation:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Protezione anti-virus**.

   Le impostazioni della protezione anti-virus vengono visualizzate nella parte destra della finestra.

3. Nella parte destra della finestra eseguire una delle seguenti operazioni:
   - Selezionare **Attiva tecnologia Disinfezione avanzata** per abilitare la tecnologia avanzata di disinfezione.
   - Deselezionare **Attiva tecnologia Disinfezione avanzata** per disabilitare la tecnologia avanzata di disinfezione.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

Quando l'attività Disinfezione avanzata è avviata tramite Kaspersky Security Center, la maggior parte delle funzioni del sistema operativo non è disponibile per l'utente. La workstation viene riavviata dopo il completamento dell'attività.

## Abilitazione o disabilitazione della tecnologia avanzata di disinfezione per i file server

*Per abilitare la tecnologia avanzata di disinfezione per i file server, eseguire una delle seguenti operazioni:*

- Abilitare la tecnologia avanzata di disinfezione nelle proprietà del criterio di Kaspersky Security Center attivo. A tale scopo:
  a. Aprire la sezione **Impostazioni di protezione generali** nella finestra delle proprietà del criterio.
  b. Selezionare la casella di controllo **Attiva tecnologia Disinfezione avanzata**.
  c. Per salvare le modifiche, fare clic su **OK** nella finestra delle proprietà del criterio.

- Nelle proprietà dell'attività di gruppo Scansione virus di Kaspersky Security Center, selezionare la casella di controllo **Esegui immediatamente Disinfezione avanzata**.

*Per disabilitare la tecnologia avanzata di disinfezione per i file server, eseguire una delle seguenti operazioni:*

- Abilitare la tecnologia avanzata di disinfezione nelle proprietà del criterio di Kaspersky Security Center. A tale scopo:

  a. Aprire la sezione **Impostazioni di protezione generali** nella finestra delle proprietà del criterio.

  b. Deselezionare la casella di controllo **Attiva tecnologia Disinfezione avanzata**.

  c. Per salvare le modifiche, fare clic su **OK** nella finestra delle proprietà del criterio.

- Nelle proprietà dell'attività di gruppo Scansione virus di Kaspersky Security Center, deselezionare la casella di controllo **Esegui immediatamente Disinfezione avanzata**.

## Abilitazione o disabilitazione della modalità di risparmio energetico

*Per abilitare o disabilitare la modalità di risparmio energetico:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni avanzate dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Modalità operativa** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Modalità operativa**.
4. Nella finestra **Modalità operativa** eseguire le seguenti operazioni:

   - Per abilitare la modalità di risparmio energetico, selezionare la casella di controllo **Rimanda attività pianificate durante l'alimentazione a 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 Scansione Vulnerabilità
     - Attività Controllo integrità

   - Per disabilitare la modalità di risparmio energetico, deselezionare la casella di controllo **Rimanda attività pianificate durante l'alimentazione a batteria**. In questo caso, Kaspersky Endpoint Security esegue le attività pianificate indipendentemente dalla fonte di alimentazione del computer.
5. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Abilitazione o disabilitazione della concessione di risorse ad altre applicazioni

*Per abilitare o disabilitare la concessione di risorse ad altre applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni avanzate dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Modalità operativa** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Modalità operativa**.
4. Nella finestra **Modalità operativa** eseguire le seguenti operazioni:

   - Per abilitare la modalità in cui vengono concesse risorse ad altre applicazioni, selezionare la casella di controllo **Concedi risorse alle altre applicazioni**.

     Quando è configurato per la concessione di risorse ad altre applicazioni, Kaspersky Endpoint Security rimanda le attività pianificate che rallentano le altre applicazioni:

     - Attività di aggiornamento
     - Attività Scansione Completa
     - Attività Scansione delle aree critiche
     - Attività Scansione Personalizzata
     - Attività Scansione Vulnerabilità
     - Attività Controllo integrità
   - Per disabilitare la modalità in cui vengono concesse risorse ad altre applicazioni, deselezionare la casella di controllo **Concedi risorse alle altre applicazioni**. In questo caso, Kaspersky Endpoint Security esegue le attività pianificate indipendentemente dall'esecuzione di altre applicazioni.

   Per impostazione predefinita, l'applicazione è configurata in modo da concedere risorse ad altre applicazioni.
5. Per salvare le modifiche, fare clic sul pulsante **Salva**.

# Protezione tramite password

Questa sezione contiene informazioni sulla limitazione dell'accesso a Kaspersky Endpoint Security tramite una password.

## Informazioni sulla limitazione dell'accesso a Kaspersky Endpoint Security

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.

È possibile limitare l'accesso a Kaspersky Endpoint Security impostando nome utente e password e specificando le operazioni per cui vengono richieste tali credenziali all'utente:

Quando si esegue l'upgrade di una versione precedente dell'applicazione a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, la password viene mantenuta (se impostata). Per modificare le impostazioni di protezione tramite password per la prima volta, utilizzare il nome utente predefinito KLAdmin.

## Abilitazione e disabilitazione della protezione tramite password

È consigliabile prestare attenzione quando si utilizza una password per limitare l'accesso all'applicazione. Se si dimentica la password, contattare l'Assistenza tecnica di Kaspersky per informazioni sulla disabilitazione della protezione tramite password.

*Per abilitare la protezione tramite password:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Protezione tramite password** fare clic sul pulsante **Impostazioni**.

   Verrà aperta la finestra **Protezione tramite password**.
4. Selezionare la casella di controllo **Abilita la protezione tramite password**.
5. Nel campo **Nome utente** immettere il nome utente che deve essere specificato nella finestra **Controllo password** quando vengono eseguite le successive operazioni protette da password.
6. Nel campo **Nuova password** digitare una password per l'accesso all'applicazione.
7. Confermare la password nel campo **Conferma password**.
8. Se si desidera limitare l'accesso per tutte le operazioni con l'applicazione, nella sezione **Ambito della password** fare clic sul pulsante **Seleziona tutto**.
9. Se si desidera limitare l'accesso degli utenti in modo selettivo, nella sezione **Ambito della password** selezionare le caselle di controllo accanto ai nomi delle operazioni corrispondenti:
   - **Configura le impostazioni dell'applicazione**.
   - **Chiudi l'applicazione**.
   - **Disabilita componenti diprotezione**.
   - **Disabilita componenti di controllo**.

- **Rimuovi chiave**.
- **Rimuovi / modifica / ripristina applicazione**.
- **Ripristina l'accesso ai dati nelle unità criptate**.
- **Visualizza rapporti**.

10. Fare clic sul pulsante **OK**.

    L'applicazione verifica le password immesse. Se le password corrispondono, l'applicazione applica la password. Se le password non corrispondono, l'applicazione richiede di confermare nuovamente la password nel campo **Conferma password**.

Dopo avere abilitato la protezione tramite password, l'applicazione richiederà una password ogni volta che viene eseguita un'operazione inclusa nell'ambito della password. Se non si desidera che l'applicazione richieda la password ogni volta che si tenta di eseguire un'operazione protetta tramite password durante la sessione corrente, è possibile selezionare la casella di controllo **Salva la password per la sessione corrente** nella finestra **Controllo password**.

Quando la casella di controllo **Salva la password per la sessione corrente** è deselezionata, l'applicazione richiede la password ogni volta che si tenta di eseguire un'operazione protetta tramite password.

*Per disabilitare la protezione tramite password:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Protezione tramite password** fare clic sul pulsante **Impostazioni**.

   Verrà aperta la finestra **Protezione tramite password**.
4. Deselezionare la casella di controllo **Abilita la protezione tramite password**.

   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.
5. Fare clic sul pulsante **OK**.

Dopo avere disabilitato la protezione tramite password, le restrizioni di accesso all'applicazione saranno annullate al successivo avvio di Kaspersky Endpoint Security.

## Modifica della password di accesso a Kaspersky Endpoint Security

*Per modificare la password di accesso per Kaspersky Endpoint Security:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.
3. Nella sezione **Protezione tramite password** fare clic sul pulsante **Impostazioni**.

Verrà aperta la finestra **Protezione tramite password**.

4. Immettere il nome utente nel campo **Nome utente**.
5. Nel campo **Nuova password** immettere una nuova password per l'accesso all'applicazione.
6. Nel campo **Conferma password** immettere nuovamente la nuova password.
7. Fare clic su **OK**.

   L'applicazione verifica le password immesse. Se le password corrispondono, l'applicazione applica la nuova password e chiude la finestra **Protezione tramite password**. Se le password non corrispondono, l'applicazione richiede di confermare nuovamente la password nel campo **Conferma password**.

8. Per salvare le modifiche, nella finestra delle impostazioni dell'applicazione fare clic sul pulsante **Salva**.

## Informazioni sull'utilizzo di una password provvisoria

Mentre utilizzano i computer client gestiti da un criterio di Kaspersky Security Center, gli utenti potrebbero avere l'esigenza di eseguire operazioni con Kaspersky Endpoint Security che sono protette tramite password a livello di criterio. Quando la protezione tramite password è abilitata, solo l'amministratore di Kaspersky Security Center può eseguire le operazioni specificate nell'ambito della password. Tuttavia, se la connessione con Kaspersky Security Center non è disponibile (ad esempio, quando l'utente è all'esterno della rete aziendale), le funzioni per l'utilizzo dell'interfaccia locale di Kaspersky Security Center sono limitate.

Per offrire a un utente la possibilità di eseguire le operazioni necessarie senza fornirgli la password specificata nelle impostazioni del criterio, l'amministratore di Kaspersky Security Center può creare una password provvisoria. Una password provvisoria è valida solo per un determinato periodo e ha un ambito di applicazione limitato. Dopo che l'utente immette la password provvisoria nell'interfaccia locale dell'applicazione, le operazioni consentite dall'amministratore di Kaspersky Security Center diventano disponibili.

Alla scadenza della password provvisoria, Kaspersky Endpoint Security continua a funzionare in base alle impostazioni del criterio di Kaspersky Security Center. Le operazioni protette tramite password a livello di criterio diventano non disponibili per l'utente.

## Creazione di una password provvisoria tramite Kaspersky Security Center Administration Console

*Per creare una password provvisoria e inviarla a un utente:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione che include il computer dell'utente che ha richiesto la password provvisoria.
3. Nell'area di lavoro selezionare la scheda **Dispositivi**.
4. Dal menu di scelta rapida del computer che appartiene all'utente che ha richiesto la password provvisoria selezionare **Proprietà**.

   Verrà visualizzata la finestra **Proprietà: <Nome computer>**.

5. Nella finestra **Proprietà: <Nome computer>** selezionare la sezione **Applicazioni**.

6. Selezionare Kaspersky Endpoint Security Service Pack 2 for Windows e aprire la finestra delle proprietà dell'applicazione utilizzando uno dei seguenti metodi:

   - Fare clic sul pulsante **Proprietà** nella parte inferiore dello schermo.
   - Dal menu di scelta rapida dell'applicazione selezionare **Proprietà**.

   Verrà visualizzata la finestra **Impostazioni applicazione "<Nome applicazione>"**.

7. Nella finestra **Impostazioni applicazione "<Nome applicazione>"**, nella sezione **Impostazioni avanzate**, selezionare la sottosezione **Impostazioni applicazione**.

8. Nella sezione **Protezione tramite password** fare clic sul pulsante **Impostazioni**.

   Verrà aperta la finestra **Protezione tramite password**.

9. Nella finestra **Protezione tramite password**, nella sezione **Password provvisoria**, fare clic sul pulsante **Impostazioni**.

   Questo pulsante è disponibile se la protezione tramite password è abilitata per Kaspersky Security Center nel criterio di Kaspersky Security Center in esecuzione nel computer.

   Verrà visualizzata la finestra **Crea password provvisoria**.

10. Nel campo **Data di scadenza** specificare la data a partire dalla quale l'utente non più potrà utilizzare la password provvisoria.

    In questa data, la password provvisoria diventerà non valida. È necessario creare una nuova password provvisoria per fornire l'accesso per l'esecuzione di operazioni nell'interfaccia locale di Kaspersky Endpoint Security.

11. Nella tabella **Ambito della password provvisoria** selezionare le caselle di controllo accanto alle operazioni che devono essere disponibili per l'utente durante il periodo di validità della password provvisoria.

12. Fare clic sul pulsante **Crea**.

    Verrà visualizzata la finestra **Password provvisoria**, che contiene una password criptata.

13. Copiare la password e le istruzioni per la relativa applicazione e inviarle all'utente.

## Applicazione di una password provvisoria nell'interfaccia di Kaspersky Endpoint Security

Queste istruzioni sono destinate agli utenti di computer client in cui è installato Kaspersky Endpoint Security.

*Per applicare una password provvisoria:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni dell'applicazione vengono visualizzate nella parte destra della finestra.

3. Nella sezione **Protezione tramite password** fare clic sul pulsante **Password provvisoria**.

   Verrà visualizzata la finestra **Password provvisoria**.

4. Selezionare la casella di controllo **Abilita password provvisoria**.

5. Nel campo di immissione specificare la password che è stata ottenuta dall'amministratore di Kaspersky Security Center.

6. Fare clic su **OK** per salvare le modifiche.

Una volta applicata la password provvisoria, le operazioni specificate dall'amministratore di Kaspersky Security Center diventeranno disponibili. Nella finestra **Password provvisoria** sono visualizzate la data di scadenza della password provvisoria e le operazioni consentite.

# Amministrazione remota dell'applicazione tramite Kaspersky Security Center

Questa sezione descrive l'amministrazione di Kaspersky Endpoint Security tramite Kaspersky Security Center.

## Informazioni sulla gestione dell'applicazione tramite Kaspersky Security Center

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

Per ulteriori informazioni sulla gestione dell'applicazione tramite Kaspersky Security Center rispetto a quelle fornite nel presente documento, consultare la *Guida dell'amministratore di Kaspersky Security Center*.

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

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

## Considerazioni speciali in caso di utilizzo di versioni diverse dei plug-in di amministrazione

È possibile utilizzare un plug-in di amministrazione per modificare i seguenti elementi:

- Criteri
- Profili criterio
- Attività di gruppo
- Attività locali
- Impostazioni locali di Kaspersky Endpoint Security

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

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

### Modifica delle impostazioni definite in precedenza utilizzando una versione successiva del plug-in di amministrazione

È possibile utilizzare una versione successiva del plug-in di amministrazione per modificare tutte le impostazioni definite in precedenza e configurare nuove impostazioni che non erano presenti nella versione precedentemente in uso del plug-in di amministrazione.

Per le nuove impostazioni, una versione successiva del plug-in di amministrazione assegna i valori predefiniti quando si salva per la prima volta un criterio, un profilo criterio o un'attività.

Dopo aver modificato le impostazioni di un criterio, un profilo criterio o un'attività di gruppo utilizzando una versione successiva del plug-in di amministrazione, questi componenti diventeranno non disponibili per le versioni precedenti del plug-in di amministrazione. Le impostazioni locali di Kaspersky Endpoint Security e le impostazioni delle attività locali sono ancora disponibili per i plug-in di amministrazione di versioni precedenti.

## Avvio e arresto di Kaspersky Endpoint Security in un computer client

*Per avviare e arrestare l'applicazione in un computer client:*

1. Aprire Administration Console di Kaspersky Security Center.
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**.

   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 10 for Windows.
8. Eseguire le seguenti operazioni:

   - Per avviare l'applicazione, fare clic sul pulsante a destra dell'elenco delle applicazioni Kaspersky o eseguire le seguenti operazioni:

     a. Selezionare **Proprietà** nel menu di scelta rapida di Kaspersky Endpoint Security o fare clic sul pulsante **Proprietà** sotto l'elenco delle applicazioni Kaspersky.

     Verrà visualizzata la finestra delle **impostazioni dell'applicazione Kaspersky Endpoint Security 10 for Windows**.

     b. Nella sezione **Generale** fare clic sul pulsante **Esegui** nella parte destra della finestra.

   - Per arrestare l'applicazione, fare clic sul pulsante a destra dell'elenco delle applicazioni Kaspersky o eseguire le seguenti operazioni:

a. Selezionare **Proprietà** nel menu di scelta rapida di Kaspersky Endpoint Security o fare clic sul pulsante **Proprietà** sotto l'elenco delle applicazioni Kaspersky.

Verrà visualizzata la finestra delle **impostazioni dell'applicazione Kaspersky Endpoint Security 10 for Windows**.

b. Nella sezione **Generale** fare clic sul pulsante **Arresta** nella parte destra della finestra.

## Configurazione delle impostazioni di Kaspersky Endpoint Security

*Per configurare le impostazioni di Kaspersky Endpoint Security:*

1. Aprire Administration Console di Kaspersky Security Center.
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 l'applicazione Kaspersky Endpoint Security 10 for Windows.
8. Eseguire una delle seguenti operazioni:

   - Selezionare **Proprietà** dal menu di scelta rapida di Kaspersky Endpoint Security 10 for Windows.
   - Fare clic sul pulsante **Proprietà** sotto l'elenco delle applicazioni Kaspersky.

   Verrà visualizzata la finestra delle **impostazioni dell'applicazione Kaspersky Endpoint Security 10 for Windows**.
9. Nella sezione **Impostazioni avanzate** configurare le impostazioni per Kaspersky Endpoint Security e le impostazioni per i rapporti e l'archiviazione.

   Le altre sezioni della finestra delle **impostazioni dell'applicazione Kaspersky Endpoint Security 10 for Windows** sono identiche alle sezioni standard per l'applicazione di Kaspersky Security Center. Una descrizione di queste sezioni è disponibile nella *Guida dell'amministratore 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 avanzate**.
10. Per salvare le modifiche, nella finestra delle **impostazioni dell'applicazione Kaspersky Endpoint Security 10** fare clic su **OK**.

# Gestione delle attività

In questa sezione viene descritto come gestire le attività per Kaspersky Endpoint Security. Per informazioni dettagliate sulla gestione delle attività tramite Kaspersky Security Center, consultare la *Guida dell'amministratore di Kaspersky Security Center*.

## Informazioni sulle attività per Kaspersky Endpoint Security

Kaspersky Security Center controlla l'attività delle applicazioni Kaspersky nei computer client attraverso le attività. Le attività implementano le funzioni di amministrazione principali, come l'installazione della chiave, la scansione del computer e gli aggiornamenti dei database e dei moduli software dell'applicazione.

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 un set di computer che non appartengono a gruppi di amministrazione.

  Le attività per i set di computer non inclusi nei gruppi di amministrazione si applicano solo ai computer client specificati nelle impostazioni dell'attività. Se si aggiungono nuovi computer client a un set di computer per cui è stata configurata un'attività, l'attività non viene applicata ai nuovi computer. Per applicare l'attività ai nuovi computer, creare una nuova attività o modificare le impostazioni dell'attività esistente.

Per gestire in remoto Kaspersky Endpoint Security, è possibile utilizzare le seguenti attività di qualsiasi dei tipi elencati:

- **Aggiungi chiave**. Kaspersky Endpoint Security aggiunge una chiave per l'attivazione dell'applicazione ed eventualmente una chiave di riserva.
- **Modifica i componenti dell'applicazione**. Kaspersky Endpoint Security installa o rimuove i componenti nei computer client in base all'elenco di componenti specificati nelle impostazioni dell'attività.
- **Inventario**. Kaspersky Endpoint Security raccoglie informazioni su tutti i file eseguibili delle applicazioni installate nei computer.

  È possibile abilitare l'inventario di moduli DLL e file di script. In questo caso, Kaspersky Security Center riceverà informazioni sui moduli DLL caricati in un computer in cui è installato Kaspersky Endpoint Security e sui file che contengono script.

  L'abilitazione dell'inventario dei moduli DLL e dei file di script aumenta notevolmente la durata dell'attività di inventario e le dimensioni del database.
- **Aggiornamento**. Kaspersky Endpoint Security aggiorna i database e i moduli dell'applicazione in base alle impostazioni di aggiornamento configurate.

- **Rollback**. Kaspersky Endpoint Security esegue il rollback dell'ultimo aggiornamento di database e moduli.
- **Scansione virus**. Kaspersky Endpoint Security esamina le aree del computer specificate nelle impostazioni dell'attività alla ricerca di virus e altre minacce.
- **Verifica della connessione con KSN**. Kaspersky Endpoint Security invia una query sulla disponibilità dei server KSN e aggiorna lo stato della connessione KSN.
- **Controllo integrità**. Kaspersky Endpoint Security riceve dati sul set di moduli dell'applicazione installati nel computer client ed esamina la firma digitale di ogni modulo.
- **Gestisci account per l'Agente di Autenticazione**. Durante l'esecuzione di questa attività, Kaspersky Endpoint Security genera comandi per la rimozione, l'aggiunta o la modifica di account per l'Agente di Autenticazione.

È possibile eseguire le seguenti azioni sulle attività:

- Avviare, arrestare, sospendere e riprendere attività.
- Creare nuove attività.
- Modificare le impostazioni delle attività.

I diritti di accesso alle impostazioni delle attività di Kaspersky Endpoint Security (lettura, scrittura, esecuzione) sono definiti per ogni utente che ha accesso all'Administration Server di Kaspersky Security Center, 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 **Protezione** della finestra delle proprietà dell'Administration Server di Kaspersky Security Center.

## Configurazione della modalità di gestione delle attività

*Per configurare la modalità di gestione delle attività nell'interfaccia locale di Kaspersky Endpoint Security:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera configurare la modalità di gestione delle attività nell'interfaccia locale di Kaspersky Endpoint Security.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella sezione **Impostazioni avanzate** selezionare la sottosezione **Impostazioni applicazione**.
7. Nella sezione **Modalità operativa**:
   - Se si desidera consentire agli utenti di utilizzare le attività locali nell'interfaccia e nella riga di comando di Kaspersky Endpoint Security, selezionare la casella di controllo **Consenti utilizzo delle attività locali**.

Se la casella di controllo è deselezionata, le funzioni delle attività locali sono arrestate. In questa modalità, le attività locali non vengono eseguite in base alla pianificazione. Le attività locali risultano anche non disponibili per l'avvio e la modifica nell'interfaccia locale di Kaspersky Endpoint Security e durante l'utilizzo della riga di comando.

- Se si desidera consentire agli utenti di visualizzare l'elenco delle attività di gruppo, selezionare la casella di controllo **Consenti la visualizzazione delle attività di gruppo**.
- Se si desidera consentire agli utenti di modificare le impostazioni delle attività di gruppo, selezionare la casella di controllo **Consenti la gestione delle attività di gruppo**.

8. Fare clic su **OK** per salvare le modifiche.
9. Applicare il criterio.

   Per informazioni sull'applicazione del criterio di Kaspersky Security Center, vedere la *Guida dell'amministratore di Kaspersky Security Center*.

## Creazione di un'attività locale

*Per creare un'attività locale:*

1. Aprire Administration Console di Kaspersky Security Center.
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 creare un'attività locale.
5. Eseguire una delle seguenti operazioni:
   - Nel menu di scelta rapida del computer client selezionare l'opzione **Tutte le attività** Crea attività.
   - Nel menu di scelta rapida del computer client selezionare **Proprietà**. Nella finestra **Proprietà: <Nome computer>** visualizzata, nella scheda **Attività**, fare clic sul pulsante **Aggiungi**.
   - Nell'elenco a discesa **Esegui azione** selezionare **Crea attività**.

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

## Creazione di un'attività di gruppo

*Per creare un'attività di gruppo:*

1. Aprire Administration Console di Kaspersky Security Center.

2. Eseguire una delle seguenti operazioni:

   - Nella struttura di Administration Console selezionare la cartella **Dispositivi gestiti** per creare un'attività di gruppo per tutti i computer gestiti da Kaspersky Security Center.
   - 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 **Attività**.
4. Fare clic sul pulsante **Crea attività**.

   Verrà avviata la Creazione guidata attività.

5. Attenersi alle istruzioni della Creazione guidata attività.

## Creazione di un'attività per una selezione di dispositivi

*Per creare un'attività per una selezione di dispositivi, procedere come segue:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Selezionare la cartella **Attività** nella struttura di Administration Console.
3. Fare clic sul pulsante **Crea attività**.

   Verrà avviata la Creazione guidata attività.

4. Attenersi alle istruzioni della Creazione guidata attività.
5. Nella finestra **Selezionare i dispositivi a cui assegnare l'attività** della procedura guidata fare clic sul pulsante **Assegna attività a una selezione di dispositivi**.
6. Nella finestra successiva della procedura guidata fare clic sul pulsante **Seleziona**.

   Verrà visualizzata la finestra **Selezione dispositivi**.

7. Selezionare i dispositivi desiderati.
8. Fare clic su **OK** nella finestra **Selezione dispositivi**.
9. Attenersi alle istruzioni della Creazione guidata attività.

## Avvio, arresto, sospensione e ripresa di un'attività

Se l'applicazione Kaspersky Endpoint Security è in esecuzione in un computer client, è possibile avviare, arrestare, sospendere e riprendere un'attività nel computer client tramite Kaspersky Security Center. Quando Kaspersky Endpoint Security è sospeso, le attività in esecuzione vengono sospese e diventa impossibile avviare, arrestare, sospendere o riprendere un'attività tramite Kaspersky Security Center.

*Per avviare, arrestare, sospendere o riprendere un'attività locale:*

1. Aprire Administration Console di Kaspersky Security Center.
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, arrestare, sospendere o riprendere un'attività locale.
5. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida del computer client, quindi selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del computer client.
6. Selezionare la sezione **Attività**.

   Nella parte destra della finestra verrà visualizzato un elenco di attività locali.
7. Selezionare l'attività locale che si desidera avviare, arrestare, sospendere o riprendere.
8. Eseguire l'azione desiderata sull'attività utilizzando uno dei seguenti metodi:

   - Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida dell'attività locale, quindi selezionare **Esegui** / **Arresta** / **Sospendi** / **Riprendi**.
   - Per avviare o interrompere un'attività locale, fare clic sul pulsante / a destra dell'elenco delle attività locali.
   - Eseguire le seguenti operazioni:

     a. Fare clic sul pulsante **Proprietà** sotto l'elenco delle attività locali o selezionare **Proprietà** nel menu di scelta rapida dell'attività.

     Verrà visualizzata la finestra **Proprietà: <Nome attività>**.

     b. Nella scheda **Generale** fare clic sul pulsante **Esegui** / **Arresta** / **Sospendi** / **Riprendi**.

*Per avviare, arrestare, sospendere o riprendere un'attività di gruppo:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera avviare, arrestare, sospendere o riprendere un'attività di gruppo.
3. Nell'area di lavoro selezionare la scheda **Attività**.

   Le attività di gruppo vengono visualizzate nella parte destra della finestra.
4. Selezionare l'attività di gruppo che si desidera avviare, arrestare, sospendere o riprendere.
5. Eseguire l'azione desiderata sull'attività utilizzando uno dei seguenti metodi:

   - Nel menu di scelta rapida dell'attività di gruppo selezionare **Esegui** / **Arresta** / **Sospendi** / **Riprendi**.
   - Fare clic sul pulsante / nella parte destra della finestra per avviare o arrestare un'attività di gruppo.
   - Eseguire le seguenti operazioni:

a. Fare clic sul collegamento **Impostazioni attività** nella parte destra dell'area di lavoro di Administration Console o selezionare **Proprietà** dal menu di scelta rapida dell'attività.

Verrà visualizzata la finestra **Proprietà: <Nome attività>**.

b. Nella scheda **Generale** fare clic sul pulsante **Esegui** / **Arresta** / **Sospendi** / **Riprendi**.

*Per avviare, arrestare, sospendere o riprendere un'attività per una selezione di computer:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Attività** della struttura di Administration Console selezionare l'attività per la selezione di computer da avviare, arrestare, sospendere o riprendere.
3. Eseguire una delle seguenti operazioni:
   - Nel menu di scelta rapida selezionare **Esegui** / **Arresta** / **Sospendi** / **Riprendi**.
   - Fare clic sul pulsante / nella parte destra della finestra per avviare o arrestare l'attività per computer specifici.
   - Eseguire le seguenti operazioni:
     a. Fare clic sul collegamento **Impostazioni attività** nella parte destra dell'area di lavoro di Administration Console o selezionare **Proprietà** dal menu di scelta rapida dell'attività.

     Verrà visualizzata la finestra **Proprietà: <Nome attività>**.

     b. Nella scheda **Generale** fare clic sul pulsante **Esegui** / **Arresta** / **Sospendi** / **Riprendi**.

## Modifica delle impostazioni delle attività

*Per modificare le impostazioni di un'attività locale:*

1. Aprire Administration Console di Kaspersky Security Center.
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 dell'applicazione.
5. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida del computer client, quindi selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del computer client.
6. Selezionare la sezione **Attività**.

   Nella parte destra della finestra verrà visualizzato un elenco di attività locali.
7. Selezionare l'attività locale desiderata nell'elenco delle attività locali.
8. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:

- Dal menu di scelta rapida del criterio selezionare **Proprietà**.
- Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

9. Nella finestra **Proprietà: <Nome attività locale>** selezionare la sezione **Impostazioni**.
10. Modificare le impostazioni dell'attività locale.
11. Per salvare le modifiche, nella finestra **Proprietà: <Nome attività locale>** fare clic su **OK**.
12. Per salvare le modifiche, nella finestra **Proprietà: <Nome computer>** fare clic su **OK**.

*Per modificare le impostazioni di un'attività di gruppo:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** aprire la cartella con il nome del gruppo di amministrazione desiderato.
3. Nell'area di lavoro selezionare la scheda **Attività**.
   Le attività di gruppo sono visualizzate nell'area di lavoro di Administration Console.
4. Selezionare l'attività di gruppo desiderata.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
6. Nella finestra **Proprietà: <Nome attività di gruppo>** selezionare la sezione **Impostazioni**.
7. Modificare le impostazioni dell'attività di gruppo.
8. Per salvare le modifiche, nella finestra **Proprietà: <Nome attività di gruppo>** fare clic su **OK**.

*Per modificare le impostazioni di un'attività per una selezione di computer:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Attività** della struttura di Administration Console selezionare l'attività per la selezione di computer di cui si desidera modificare le impostazioni.
3. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.
4. Nella finestra **Proprietà: <Nome dell'attività per la selezione di computer>** selezionare la sezione **Impostazioni**.
5. Modificare le impostazioni dell'attività per la selezione di computer.
6. Per salvare le modifiche, nella finestra **Proprietà: <Nome dell'attività per la selezione di computer>** fare clic su **OK**.

Ad eccezione della scheda **Impostazioni**, tutte le schede nella finestra delle proprietà dell'attività sono identiche a quelle utilizzate in Kaspersky Security Center. Per una descrizione dettagliata di queste schede, fare riferimento alla *Guida dell'amministratore di Kaspersky Security Center*. La sezione **Impostazioni** contiene le impostazioni specifiche per Kaspersky Endpoint Security 10 for Windows. Il contenuto della sezione dipende dall'attività selezionata o dal tipo di attività.

## Gestione dei criteri

In questa sezione sono descritte la creazione e la configurazione dei criteri per Kaspersky Endpoint Security. Per informazioni più dettagliate sulla gestione di Kaspersky Endpoint Security tramite i criteri di Kaspersky Security Center, fare riferimento alla *Guida dell'amministratore di Kaspersky Security Center*.

## Informazioni sui criteri

È possibile utilizzare i criteri per applicare le stesse impostazioni di Kaspersky Endpoint Security a tutti i computer client in un gruppo di amministrazione.

È possibile modificare in locale i valori delle impostazioni specificate da un criterio per singoli computer in un gruppo di amministrazione utilizzando Kaspersky Endpoint Security. Possono essere modificate in locale solo quelle impostazioni di cui il criterio non impedisce la modifica.

Il fatto che un'impostazione di un'applicazione possa essere modificata o meno in un computer client dipende dallo stato di "blocco" per l'impostazione all'interno di un criterio:

- Se un'impostazione è "bloccata" (), non è possibile modificare il valore di questa impostazione in locale. Il valore dell'impostazione specificato dal criterio viene utilizzato per tutti i computer client del gruppo di amministrazione.
- Quando un'impostazione è "sbloccata" (), è possibile modificarla in locale. Un'impostazione configurata in locale viene applicata a tutti i computer client del gruppo di amministrazione. L'impostazione configurata tramite criteri non viene applicata.

Dopo la prima applicazione del criterio, le impostazioni locali dell'applicazione vengono modificate in base alle impostazioni del criterio.

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 **Protezione** della finestra delle proprietà dell'Administration Server di Kaspersky Security Center.

Sono disponibili i seguenti ambiti funzionali di Kaspersky Endpoint Security:

- Protezione anti-virus. L'ambito funzionale include Anti-Virus File, Anti-Virus Posta, Anti-Virus Web, Anti-Virus IM, Scansione Vulnerabilità e le attività di scansione.
- Controllo avvio applicazioni. L'ambito funzionale include il componente Controllo avvio applicazioni.
- Controllo dispositivi. L'ambito funzionale include il componente Controllo dispositivi.
- Criptaggio. L'ambito funzionale include i componenti di criptaggio di dischi rigidi, file e cartelle.
- Area attendibile. L'ambito funzionale include l'area attendibile.

- Controllo Web. L'ambito funzionale include il componente Controllo Web.
- Prevenzione Intrusioni. L'ambito funzionale include Monitor attività applicazioni, Monitor vulnerabilità, Firewall, Prevenzione attacchi di rete e Controllo privilegi applicazioni.
- Funzioni di base. Questo ambito funzionale include le impostazioni generali dell'applicazione non specificate per altri ambiti funzionali, tra cui: gestione delle licenze, impostazioni di KSN, attività di inventario, attività di aggiornamento di database e moduli dell'applicazione, Auto-Difesa, impostazioni avanzate dell'applicazione, rapporti e backup, impostazioni di protezione tramite password e impostazioni dell'interfaccia dell'applicazione.

È possibile eseguire le seguenti operazioni all'interno di un criterio:

- Creare un criterio.
- Modificare le impostazioni dei criteri.

  Se l'account utente con cui è stato eseguito l'accesso all'Administration Server non dispone dei diritti per la modifica delle impostazioni di determinati ambiti funzionali, le impostazioni di tali ambiti funzionali non sono disponibili per la modifica.

- Eliminare un criterio.
- Modificare lo stato dei criteri.

Per informazioni sull'utilizzo dei criteri che non sono correlati all'interazione con Kaspersky Endpoint Security, fare riferimento alla *Guida dell'amministratore di Kaspersky Security Center*.

## Creazione di un criterio

*Per creare un criterio:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Eseguire una delle seguenti operazioni:
   - Nella struttura di Administration Console selezionare la cartella **Dispositivi gestiti** per creare un criterio per tutti i computer gestiti da Kaspersky Security Center.
   - 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. Eseguire una delle seguenti operazioni:
   - Fare clic sul pulsante **Crea criterio**.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida, quindi selezionare **Crea** Criterio.

   Verrà avviata la Creazione guidata nuovo criterio.
5. Attenersi alle istruzioni della Creazione guidata nuovo criterio.

## Modifica delle impostazioni dei criteri

*Per modificare le impostazioni dei criteri:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nella cartella **Dispositivi gestiti** della struttura di Administration Console aprire la cartella con il nome del gruppo di amministrazione per cui si desidera modificare le impostazioni del criterio.
3. Nell'area di lavoro selezionare la scheda **Criteri**.
4. Selezionare il criterio desiderato.
5. Aprire la finestra **Proprietà: <Nome criterio>** utilizzando uno dei seguenti metodi:
   - Dal menu di scelta rapida del criterio selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura criterio** nella parte destra dell'area di lavoro di Administration Console.

   Le impostazioni dei criteri di Kaspersky Endpoint Security 10 for Windows includono le impostazioni dei componenti e le impostazioni dell'applicazione. Le sezioni **Protezione anti-virus** e **Controllo endpoint** della finestra **Proprietà: <Nome criterio>** visualizzano le impostazioni dei componenti della protezione e controllo, la sezione **Criptaggio dei dati** visualizza le impostazioni di criptaggio per file e cartelle e la sezione **Impostazioni avanzate** visualizza le impostazioni dell'applicazione.

   Per abilitare la visualizzazione delle impostazioni di criptaggio dei dati e delle impostazioni dei componenti di controllo nelle impostazioni del criterio, è necessario selezionare le caselle di controllo corrispondenti nella finestra **Impostazioni interfaccia** di Kaspersky Security Center.
6. Modificare le impostazioni del criterio.
7. Per salvare le modifiche, nella finestra **Proprietà: <Nome criterio>** fare clic su **OK**.

## Selezione delle impostazioni da visualizzare nel criterio di Kaspersky Security Center

*Per selezionare le impostazioni da visualizzare nel criterio di Kaspersky Security Center:*

1. Aprire Administration Console di Kaspersky Security Center.
2. Nel menu di scelta rapida del nodo **Administration Server – <Nome computer>** della struttura di Administration Console selezionare Visualizza → **Impostazioni interfaccia**.

   Verrà visualizzata la finestra **Impostazioni interfaccia**.
3. Nella finestra **Impostazioni interfaccia** selezionare le caselle di controllo accanto alle impostazioni che devono essere visualizzate nelle impostazioni di creazione del criterio di Kaspersky Security Center e nelle proprietà del criterio:
   - Selezionare la casella di controllo **Visualizza componenti di controllo endpoint** per abilitare la visualizzazione delle impostazioni dei componenti di controllo nella finestra della Creazione guidata nuovo criterio di Kaspersky Security Center e nelle proprietà del criterio.

- Selezionare la casella di controllo **Visualizza criptaggio e protezione dati** per abilitare la visualizzazione delle impostazioni di criptaggio dei dati nella Creazione guidata nuovo criterio di Kaspersky Security Center e nelle proprietà del criterio.

4. Fare clic su **OK**.

## Invio dei messaggi degli utenti al server di Kaspersky Security Center

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 avvio applicazioni ha bloccato l'avvio di un'applicazione.

  Il modello del messaggio per una richiesta di consentire l'avvio di un'applicazione bloccata è disponibile nell'interfaccia di Kaspersky Endpoint Security, nella sezione Controllo avvio 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 Endpoint Security non è in esecuzione un criterio di Kaspersky Security Center, 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 Endpoint Security è in esecuzione un criterio di Kaspersky Security Center, 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. Nel campo del messaggio vengono inseriti i valori dei campi del modello definito nel criterio di Kaspersky Security Center.

- Se nel computer in cui è installato Kaspersky Endpoint Security è in esecuzione un criterio fuori sede di Kaspersky Security Center, il metodo utilizzato per inviare i messaggi dipende dal fatto che sia presente o meno una connessione con Kaspersky Security Center.

  - Se viene stabilita una connessione con Kaspersky Security Center, Kaspersky Endpoint Security invia il messaggio standard a Kaspersky Security Center Administration Server.

  - Se la connessione con Kaspersky Security Center è assente, il messaggio dell'utente viene inviato all'amministratore della rete locale tramite e-mail.

  In entrambi casi, nel campo del messaggio vengono inseriti i valori dei campi del modello definito nel criterio di Kaspersky Security Center.

# Visualizzazione dei messaggi degli utenti nell'archivio di eventi di Kaspersky Security Center

I componenti Controllo avvio applicazioni, Controllo dispositivi e Controllo Web consentono agli utenti della rete LAN che utilizzano computer in cui è installato Kaspersky Endpoint Security di inviare messaggi all'amministratore.

Un utente può inviare messaggi all'amministratore in due modi:

- Come eventi nell'archivio di eventi di Kaspersky Security Center.

  L'evento dell'utente viene inviato all'archivio di eventi di Kaspersky Security Center se l'applicazione Kaspersky Endpoint Security installata nel computer dell'utente viene eseguita in base a un criterio attivo.

- Come messaggi e-mail.

  Le informazioni sull'utente vengono inviate tramite e-mail se l'applicazione Kaspersky Endpoint Security installata nel computer dell'utente non esegue un criterio o esegue un criterio fuori sede.

*Per visualizzare il messaggio di un utente nell'archivio di eventi di Kaspersky Security Center:*

1. Aprire Administration Console di Kaspersky Security Center.
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 **Eventi selezionati** selezionare **Richieste utente**.
4. Selezionare il messaggio da inviare all'amministratore.
5. Aprire la finestra **Impostazioni evento** in uno dei seguenti modi:

   - Fare clic con il pulsante destro del mouse sull'evento. Dal menu di scelta rapida visualizzato selezionare **Proprietà**.
   - Fare clic sul pulsante **Apri la finestra delle proprietà dell'evento** nella parte destra dell'area di lavoro di Administration Console.

# Partecipazione a Kaspersky Security Network

Questa sezione contiene informazioni sulla partecipazione a Kaspersky Security Network e istruzioni su come abilitare o disabilitare l'utilizzo di Kaspersky Security Network.

## Informazioni sulla partecipazione a Kaspersky Security Network

Per proteggere il computer in modo più efficace, Kaspersky Endpoint Security utilizza dati raccolti dagli utenti di tutto il mondo. La raccolta 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.

A seconda della posizione dell'infrastruttura, sono disponibili un servizio KSN globale (l'infrastruttura è ospitata dai server di Kaspersky) e un servizio KSN privato (l'infrastruttura è ospitata da server di terze parti, ad esempio nella rete del provider di servizi Internet).

Dopo la modifica della licenza, inviare i dettagli della nuova chiave al provider di servizi allo scopo di utilizzare il servizio KSN privato. In caso contrario, lo scambio di dati con KSN non sarà possibile.

Grazie agli utenti che partecipano a KSN, Kaspersky è in grado di ricevere tempestivamente informazioni sui tipi e sulle origini delle minacce, sviluppare soluzioni per la loro neutralizzazione e ridurre al minimo il numero di falsi allarmi visualizzati dai componenti dell'applicazione.

Durante la partecipazione a KSN, l'applicazione invia automaticamente a KSN le statistiche generate durante l'esecuzione dell'applicazione. L'applicazione può anche inviare a Kaspersky per una scansione aggiuntiva determinati file (o parti di file) che gli hacker potrebbero utilizzare per danneggiare il computer o i dati.

Non vengono raccolti, elaborati o memorizzati dati personali. 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 di KSN, Kaspersky può rilasciare database anti-virus dell'applicazione che disabilitano temporaneamente o limitano parzialmente le richieste a Kaspersky Security Network. In questo caso, per lo stato della connessione a KSN viene visualizzato *Abilitato con restrizioni*.

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.
- Proxy KSN memorizza nella cache i dati elaborati, riducendo il carico sulla connessione di rete esterna e velocizzando la ricezione delle informazioni richieste dal computer dell'utente.

Per ulteriori informazioni sul servizio proxy KSN, consultare la *Guida dell'amministratore di Kaspersky Security Center*.

Le impostazioni del servizio proxy KSN possono essere configurate nelle proprietà del criterio di *Kaspersky Security Center*.

La partecipazione al programma Kaspersky Security Network è facoltativa. L'utente viene invitato a partecipare a KSN durante la configurazione iniziale dell'applicazione. Gli utenti possono aderire al servizio o interrompere la partecipazione a KSN in qualsiasi momento.

## Abilitazione e disabilitazione dell'utilizzo di Kaspersky Security Network

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

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sottosezione **Impostazioni KSN**.

   Le impostazioni di Kaspersky Security Network sono visualizzate nella parte destra della finestra.
3. Eseguire una delle seguenti operazioni:
   - Per abilitare l'utilizzo di Kaspersky Security Network, selezionare la casella di controllo **Accetto l'informativa e le condizioni per l'adesione al programma KSN**.
   - Per disabilitare l'utilizzo di Kaspersky Security Network, deselezionare la casella di controllo **Accetto l'informativa e le condizioni per l'adesione al programma KSN**.
4. Per salvare le modifiche, fare clic sul pulsante **Salva**.

## Verifica della connessione a Kaspersky Security Network

*Per verificare la connessione a Kaspersky Security Network:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra fare clic sul pulsante **Kaspersky Security Network**.

   Verrà visualizzata la finestra **Kaspersky Security Network**.

   Nella parte sinistra della finestra **Kaspersky Security Network** la modalità di connessione a Kaspersky Security Network viene visualizzata sotto forma di pulsante rotondo con la scritta **KSN**:
   - Se Kaspersky Endpoint Security non è connesso a Kaspersky Security Network, il pulsante **KSN** è grigio. Lo stato visualizzato sotto il pulsante **KSN** è *Disabilitato*.

- Se Kaspersky Endpoint Security è connesso a Kaspersky Security Network e i server KSN sono disponibili, il pulsante **KSN** è verde. Sotto il pulsante **KSN** vengono visualizzate le seguenti informazioni: stato *Abilitato*, tipo di servizio KSN in uso (**KSN privato** o **KSN globale**) e data e ora dell'ultima sincronizzazione con i server KSN. Nella parte destra della finestra vengono visualizzate statistiche sulla reputazione di file, risorse Web e software.

Kaspersky Endpoint Security raccoglie dati statistici sull'utilizzo di KSN al momento dell'apertura della finestra **Kaspersky Security Network**. Le statistiche non vengono aggiornate in tempo reale.

- Se Kaspersky Endpoint Security è connesso a Kaspersky Security Network ma i server KSN non sono disponibili, il pulsante **KSN** è rosso. Lo stato visualizzato sotto il pulsante **KSN** è *Abilitato.*

  Se l'ora dell'ultima sincronizzazione con i server di KSN è superiore a 15 minuti o presenta lo stato *Sconosciuto*, i server KSN non sono disponibili. In tal caso, è consigliabile contattare l'Assistenza tecnica o il fornitore del servizio.

  La connessione ai server Kaspersky Security Network potrebbe essere assente per i seguenti motivi:

  - Il computer non è connesso a Internet.
  - L'applicazione non è stata attivata o la licenza è scaduta.
  - Sono stati rilevati problemi correlati alla chiave (ad esempio, la chiave è stata inserita nella blacklist).

## Controllo della reputazione di un file in Kaspersky Security Network

Il servizio KSN consente di recuperare informazioni sulle applicazioni che sono incluse nei database di reputazione di Kaspersky. Questo permette di gestire in modo flessibile i criteri di avvio delle applicazioni a livello di azienda, impedendo l'avvio di adware e altri programmi che possono essere utilizzati da utenti malintenzionati per danneggiare il computer o i dati personali dell'utente.

*Per controllare la reputazione di un file in Kaspersky Security Network:*

1. Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida del file di cui si desidera verificare la reputazione.
2. Selezionare l'opzione **Controlla reputazione in KSN**.

   Questa opzione è disponibile se sono state accettate le condizioni dell'Informativa di Kaspersky Security Network.

   Verrà visualizzata la finestra **<Nome file> - Reputazione in KSN**. La finestra **<Nome file> - Reputazione in KSN** contiene le seguenti informazioni sul file:

   - **Percorso**. Percorso del file sul disco.
   - **Versione**. Versione dell'applicazione (questa informazione è visualizzata solo per i file eseguibili).
   - **Firma digitale**. Presenza di una firma digitale nel file.

- **Firmato**. Data in cui il certificato è stato firmato con una firma digitale.
- **Data creazione**. Data di creazione del file.
- **Data modifica**. Data dell'ultima modifica del file.
- **Dimensioni**. Spazio su disco occupato dal file.
- Informazioni su quanti utenti considerano attendibile o bloccano il file.

## Protezione avanzata con Kaspersky Security Network

Kaspersky offre agli utenti un livello di protezione aggiuntivo mediante Kaspersky Security Network. Questo metodo di protezione è progettato per contrastare le minacce persistenti di livello avanzato e gli attacchi zero-day. Le tecnologie cloud integrate e l'esperienza degli analisti anti-virus di Kaspersky rendono Kaspersky Endpoint Security la soluzione migliore in assoluto per la protezione dalle minacce di rete più complesse.

Informazioni dettagliate sulla protezione avanzata in Kaspersky Endpoint Security sono disponibili nel sito Web di Kaspersky.

# 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 nel forum

Se la domanda non richiede una risposta urgente, è possibile sottoporla agli esperti di Kaspersky e ad altri utenti nel forum.

In questo forum è possibile visualizzare gli argomenti esistenti, lasciare i propri commenti e creare nuovi argomenti di discussione.

# Come contattare l'assistenza tecnica

Questa sezione descrive i modi e le condizioni per ottenere assistenza tecnica.

# Come ottenere assistenza tecnica

Se non è possibile trovare una soluzione per il proprio problema nella documentazione dell'applicazione o in una delle fonti di informazioni sull'applicazione, è consigliabile contattare l'Assistenza tecnica. Gli specialisti dell'Assistenza tecnica rispondono ai quesiti in merito all'installazione e all'utilizzo dell'applicazione.

L'Assistenza tecnica è disponibile solo per gli utenti che hanno acquistato una licenza commerciale. Gli utenti che hanno ricevuto una licenza di prova non hanno diritto all'Assistenza tecnica.

Prima di contattare l'Assistenza tecnica, consultare le regole dell'assistenza.

È possibile contattare l'Assistenza tecnica in uno dei seguenti modi:

- Contattando telefonicamente l'Assistenza tecnica
- Inviando una richiesta all'Assistenza tecnica di Kaspersky attraverso il portale Kaspersky CompanyAccount

# Assistenza tecnica telefonica

È possibile contattare telefonicamente il personale dell'Assistenza tecnica dalla maggior parte delle aree geografiche in tutto il mondo. Le informazioni sui modi per ricevere assistenza tecnica nella propria area geografica e i contatti dell'Assistenza tecnica sono disponibili nel sito Web dell'Assistenza tecnica di Kaspersky.

Prima di contattare l'Assistenza tecnica, consultare le regole dell'assistenza.

# Assistenza tecnica tramite Kaspersky CompanyAccount

Kaspersky CompanyAccount è un portale per le aziende che utilizzano le applicazioni Kaspersky. Il portale Kaspersky CompanyAccount è progettato per agevolare l'interazione tra utenti ed esperti di Kaspersky tramite richieste in formato elettronico. È possibile utilizzare il portale Kaspersky CompanyAccount per tenere traccia dello stato delle richieste in formato elettronico e memorizzare una cronologia di tali richieste.

È possibile registrare tutti i dipendenti dell'organizzazione con un unico account in Kaspersky CompanyAccount. Un unico account consente di gestire a livello centralizzato le richieste elettroniche dei dipendenti registrati a Kaspersky, nonché di gestire i privilegi di questi dipendenti tramite Kaspersky CompanyAccount.

Il portale Kaspersky CompanyAccount è disponibile nelle seguenti lingue:

- Inglese
- Spagnolo

- Italiano
- Tedesco
- Polacco
- Portoghese
- Russo
- Francese
- Giapponese

Per ulteriori informazioni su Kaspersky CompanyAccount, visitare il sito Web dell'Assistenza tecnica.

## Raccolta di informazioni per l'assistenza tecnica

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 all'utente di registrare 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 e dump degli arresti anomali dell'applicazione.

È possibile raccogliere tutte le informazioni necessarie grazie a Kaspersky Endpoint Security. Le informazioni raccolte possono essere salvate sul disco rigido e caricate in un secondo momento.

Durante l'esecuzione della diagnostica, gli esperti dell'Assistenza tecnica possono richiedere di modificare le impostazioni dell'applicazione:

- Attivazione della funzionalità di raccolta delle informazioni di diagnostica estese.
- Ottimizzazione delle impostazioni dei singoli componenti dell'applicazione, non disponibili tramite gli elementi dell'interfaccia utente standard.
- Modifica delle impostazioni per l'archiviazione e la trasmissione delle informazioni di diagnostica raccolte.
- 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 raccolti per le operazioni di debug. Le informazioni di diagnostica estese raccolte vengono salvate nel computer dell'utente. I dati raccolti non vengono trasmessi automaticamente a Kaspersky.

Le impostazioni utilizzate per determinare l'indirizzo del server di dump per l'invio dei file di dump a Kaspersky sono memorizzate nel computer dell'utente. Se necessario, i valori di queste impostazioni possono essere modificati nella chiave del Registro di sistema del sistema operativo `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`.

Le operazioni elencate vanno eseguite solo dietro supervisione degli specialisti dell'Assistenza tecnica, in base alle relative istruzioni. Le modifiche non supervisionate alle impostazioni dell'applicazione eseguite con modalità non previste nella Guida dell'amministratore o non conformi alle istruzioni degli specialisti dell'Assistenza tecnica possono rallentare o provocare l'arresto anomalo del sistema operativo, compromettere la protezione del computer o la disponibilità e l'integrità dei dati elaborati.

## Creazione di un file di traccia

*Per creare il file di traccia:*

1. Aprire la finestra principale dell'applicazione.
2. Nella finestra principale dell'applicazione fare clic sul pulsante .

   Verrà visualizzata la finestra **Assistenza**.
3. Nella finestra **Assistenza** fare clic sul pulsante **Tracciamento del sistema**.

   Verrà visualizzata la finestra **Informazioni per l'assistenza tecnica**.
4. Per abilitare il processo di tracciamento, selezionare la casella di controllo **Abilita tracciamento**.
5. Nell'elenco a discesa **Livello** selezionare il livello di traccia.

   È consigliabile richiedere il livello di traccia necessario a uno specialista del servizio di Assistenza tecnica. In mancanza di indicazioni da parte dell'Assistenza tecnica, impostare il livello di traccia su **Normale (500)**.
6. Riprodurre la situazione in cui si è verificato il problema.
7. Per interrompere il processo di tracciamento, tornare alla finestra **Informazioni per l'assistenza tecnica** e deselezionare la casella di controllo **Abilita tracciamento**.

Dopo aver creato il file di traccia, è possibile caricare i risultati della traccia sul server di Kaspersky.

## Contenuto e archiviazione dei file di traccia

L'utente è personalmente responsabile di garantire la sicurezza dei dati raccolti, in particolare del monitoraggio e della limitazione dell'accesso ai dati raccolti archiviati nel computer fino all'invio a Kaspersky.

I file di traccia sono memorizzati nel computer in un formato modificato di cui è impossibile eseguire la lettura finché l'applicazione è in uso e vengono eliminati definitivamente quando l'applicazione viene rimossa.

I file di traccia sono archiviati nella cartella ProgramData\Kaspersky Lab.

Il file di traccia presenta il seguente formato di nome: `KES<numero versione_dataXX.XX_oraXX.XX_pidXXX.> <tipo di file di traccia> .log.enc1`.

Il file di traccia dell'Agente di Autenticazione è archiviato nella cartella System Volume Information e ha il seguente nome: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

È possibile visualizzare i dati salvati nei file di traccia. Contattare l'Assistenza tecnica di Kaspersky per indicazioni su come visualizzare i dati.

Tutti i file di traccia contengono i seguenti dati comuni:

- Ora dell'evento.
- Numero del thread di esecuzione.

  Il file di traccia dell'Agente di Autenticazione non contiene questa informazione.

- Componente dell'applicazione che ha causato l'evento.
- Livello di gravità di evento (evento informativo, avviso, evento critico, errore).
- Descrizione dell'evento, inclusi l'esecuzione di un comando da parte di un componente dell'applicazione e il risultato dell'esecuzione di questo comando.

## Contenuto dei file di traccia SRV.log, GUI.log e ALL.log

I file di traccia SRV.log, GUI.log e ALL.log possono archiviare le seguenti informazioni, in aggiunta 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.
- 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 traffico è registrato nei file di traccia solo da trafmon2.ppl.
- 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.

## Contenuto dei file di traccia HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

In aggiunta 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.

In aggiunta 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.

In aggiunta 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.

In aggiunta 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.

In aggiunta 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.

### Contenuto dei file di traccia dei plug-in dell'applicazione

I file di traccia dei plug-in dell'applicazione contengono le seguenti informazioni, in aggiunta ai dati generali:

- Il file di traccia shellex.dll.log del plug-in che avvia l'attività di scansione dal menu di scelta rapida contiene le informazioni sull'esecuzione dell'attività di scansione e i dati necessari per il debug del plug-in.
- Il file di traccia mcou.OUTLOOK.EXE del plug-in di Anti-Virus Posta può contenere parti di messaggi e-mail, inclusi indirizzi e-mail.

### Contenuto del file di traccia dell'Agente di Autenticazione

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.

## Abilitazione o disabilitazione della trasmissione a Kaspersky dei file di dump e di traccia

*Per abilitare o disabilitare la trasmissione a Kaspersky dei file di dump e di traccia:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra selezionare la sezione **Impostazioni avanzate**.

   Le impostazioni avanzate dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Modalità operativa** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Modalità operativa**.
4. Nella finestra **Modalità operativa** selezionare la casella di controllo **Abilita scrittura di dump** per consentire la scrittura dei file di dump dell'applicazione.
5. Eseguire una delle seguenti operazioni:

   - Selezionare la casella di controllo **Invia file di traccia e di dump a Kaspersky** se si desidera che l'applicazione visualizzi una richiesta nella finestra **Carica informazioni sul server per l'assistenza tecnica** per l'invio dei file di dump e di traccia a Kaspersky per l'analisi delle cause dei problemi dell'applicazione al successivo avvio del sistema operativo.

- In caso contrario, deselezionare la casella di controllo **Invia file di traccia e di dump a Kaspersky**.

6. Fare clic su **OK** nella finestra **Modalità operativa**.

7. Per salvare le modifiche, fare clic sul pulsante **Salva** nella finestra principale dell'applicazione.

## Invio di file al server dell'assistenza tecnica

I file che contengono informazioni sul sistema operativo, i file di traccia e i file di dump devono essere inviati agli esperti dell'Assistenza tecnica di Kaspersky.

*Per inviare i file al server dell'assistenza tecnica:*

1. Riavviare Kaspersky Endpoint Security dopo qualsiasi malfunzionamento durante l'esecuzione.

   Verrà visualizzata la finestra **Avvio dell'applicazione precedente non riuscito**.

   La finestra **Avvio dell'applicazione precedente non riuscito** verrà visualizzata a ogni avvio di Kaspersky Endpoint Security (anche dopo il riavvio del computer) finché non si inviano i file di dump e di traccia all'Assistenza tecnica o finché non si fa clic sul pulsante **Non inviare**.

2. Nella finestra **Avvio dell'applicazione precedente non riuscito** aprire l'elenco dei file generati facendo clic **qui**.

3. Selezionare le caselle di controllo accanto ai file che si desidera inviare all'assistenza tecnica.

4. Fare clic sul pulsante **Mostra testo informativa**.

   Verrà visualizzata la finestra **Informativa sulla trasmissione dei dati**.

5. Leggere il testo dell'Informativa sulla trasmissione dei dati e fare clic sul pulsante **Chiudi**.

6. Nella finestra **Avvio dell'applicazione precedente non riuscito** selezionare la casella di controllo **Accetto l'informativa sulla trasmissione dei dati**.

7. Fare clic sul pulsante **Invia**.

   Verrà visualizzata la finestra **Numero di richiesta**.

8. Nella finestra **Numero di richiesta** specificare il numero assegnato alla richiesta nel momento in cui è stata contattata l'Assistenza tecnica tramite Kaspersky CompanyAccount.

9. Fare clic su **OK**.

I file di dati selezionati verranno compressi e inviati al server del servizio di Assistenza tecnica.

## Abilitazione e disabilitazione della protezione dei file di dump e di traccia

I file di dump e di traccia contengono informazioni sul sistema operativo, oltre a dati riservati 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. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Impostazioni avanzate** a sinistra.

   Le impostazioni dell'applicazione vengono visualizzate nella parte destra della finestra.
3. Nella sezione **Modalità operativa** fare clic sul pulsante **Impostazioni**.

   Verrà visualizzata la finestra **Modalità operativa**.
4. Eseguire una delle seguenti operazioni:
   - Se si desidera abilitare la protezione, selezionare la casella di controllo **Abilita protezione dei file di dump e di traccia**.
   - Se si desidera disabilitare la protezione, deselezionare la casella di controllo **Abilita protezione dei file di dump e di traccia**.
5. Fare clic su **OK** nella finestra **Modalità operativa**.
6. Per salvare le modifiche, fare clic sul pulsante **Salva** nella finestra principale dell'applicazione.

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.

# Glossario

## Administration Server

Un componente di Kaspersky Security Center che archivia in modo centralizzato le informazioni su tutte le applicazioni Kaspersky installate nei computer della rete. Può essere utilizzato anche per gestire tali applicazioni.

## Agente di Autenticazione

Interfaccia per l'esecuzione del processo di autenticazione per l'accesso ai dischi rigidi criptati e il caricamento del sistema operativo dopo il criptaggio del disco rigido del sistema.

## Aggiornamento

Procedura di sostituzione o aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky.

## Ambito della scansione

Oggetti per i quali Kaspersky Endpoint Security esegue la scansione durante l'esecuzione di un'attività di scansione.

## Ambito di protezione

Oggetti per i quali viene eseguita costantemente la scansione da parte di Protezione anti-virus quando il componente è in esecuzione. Gli ambiti di protezione dei vari componenti dispongono di differenti proprietà.

## Analisi delle firme

Tecnologia di rilevamento delle minacce che utilizza i database di Kaspersky Endpoint Security, in cui sono contenute le descrizioni delle minacce conosciute, nonché i metodi per eliminarle. La protezione tramite analisi delle firme garantisce un livello di protezione minimo. In base alle raccomandazioni degli specialisti di Kaspersky, questo metodo è sempre abilitato.

## Analisi euristica

Questa tecnologia è stata progettata per il rilevamento delle minacce che non possono essere identificate utilizzando la versione corrente dei database dell'applicazione Kaspersky. Consente di rilevare i file che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante di un virus noto.

## 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.

## Backup

Uno speciale archivio per le copie di backup dei file create prima del tentativo di disinfezione o eliminazione.

## Blacklist di indirizzi

Elenco di indirizzi e-mail da cui l'applicazione Kaspersky blocca tutti i messaggi in arrivo, indipendentemente dal contenuto del messaggio.

## Certificato

Documento elettronico, contenente la chiave privata e le informazioni sul proprietario e l'ambito della chiave, che conferma che la chiave pubblica appartiene al proprietario. Il certificato deve essere firmato dal centro di certificazione che lo ha emesso.

## Certificato di licenza

Documento che Kaspersky trasferisce all'utente insieme al file chiave o al codice di attivazione. Contiene informazioni sulla licenza concessa all'utente.

## Chiave attiva

Chiave attualmente utilizzata dall'applicazione.

## Chiave di riserva

Chiave che certifica il diritto di utilizzare l'applicazione, ma che non è attualmente in uso.

## Connettore per Network Agent

Funzionalità dell'applicazione che connette l'applicazione a Network Agent. Network Agent consente l'amministrazione remota dell'applicazione tramite Kaspersky Security Center.

## 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.

## Exploit

Codice di programma che sfrutta una vulnerabilità nel sistema o nel software. Gli exploit vengono spesso utilizzati per installare malware nel computer a insaputa dell'utente.

## 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 potenzialmente infetto

Un file che contiene codice modificato di un virus noto oppure codice che ricorda quello di un virus, ma non ancora noto a Kaspersky. I file potenzialmente infetti vengono rilevati tramite l'analizzatore euristico.

## 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 HTTP, la password e la porta di connessione. L'indirizzo della risorsa Web viene inoltre modificato in caratteri minuscoli.

Nel contesto della protezione anti-virus, 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.Esempio.com\.

Forma normalizzata di un indirizzo: www.esempio.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.

## Identificazione personale certificato

Informazioni utilizzate per identificare la chiave di un certificato. Un'identificazione personale viene creata applicando una funzione hash di criptaggio al valore della chiave.

## Impostazioni dell'applicazione

Impostazioni dell'applicazione comuni a tutti i tipi di attività e che gestiscono l'esecuzione complessiva dell'applicazione, come le impostazioni per le prestazioni dell'applicazione, i rapporti e i backup.

## Impostazioni delle attività

Impostazioni dell'applicazione specifiche per ogni tipo di attività.

## Maschera file

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:

- ***** – Sostituisce zero o più caratteri.
- **?** – Sostituisce qualsiasi carattere singolo.

Si noti che il nome e l'estensione del file sono sempre separati da un punto.

## Moduli dell'applicazione

File inclusi nelle file di installazione dell'applicazione, che implementano le principali funzionalità dell'applicazione. Un modulo eseguibile distinto corrisponde a ogni tipo di attività eseguita dall'applicazione (Protezione in tempo reale, Scansione su richiesta e Aggiornamento). Quando si avvia una scansione completa del computer dalla finestra principale dell'applicazione, viene avviato il modulo di tale attività.

## 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 del certificato

Titolare di una chiave privata collegata a un certificato. Può essere un utente, un'applicazione, un oggetto virtuale, un computer o un servizio.

## 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.

## Patch

Piccolo componente aggiuntivo dell'applicazione che risolve bug individuati durante l'esecuzione dell'applicazione o installa aggiornamenti.

## Phishing

Tipo di frode Internet che consiste nell'invio di messaggi e-mail allo scopo di trafugare informazioni riservate, solitamente dati finanziari.

## 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 sul computer.

## Quarantena

Kaspersky Endpoint Security inserisce i file potenzialmente infetti in questa cartella. I file messi in quarantena vengono archiviati in formato criptato.

## Servizio di rete

Set di parametri che definiscono l'attività di rete. Per questa attività di rete, è possibile creare una regola di rete che gestisce l'esecuzione del componente Firewall.

## Spostamento dei file in Quarantena

Metodo di gestione di un file potenzialmente infetto, in cui l'accesso al file viene bloccato e il file viene spostato dalla posizione originale nella cartella Quarantena, dove è conservato in formato criptato per identificare la possibile infezione.

## Trusted Platform Module

Un microchip sviluppato per fornire funzioni di sicurezza di base (ad esempio, per l'archiviazione di chiavi di criptaggio). Un TPM in genere è installato nella scheda madre del computer e interagisce con tutti gli altri componenti del sistema tramite il bus hardware.

# 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 appartengono ai rispettivi proprietari.

Adobe, Acrobat e Shockwave sono marchi o marchi registrati di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi.

Mac e FireWire sono marchi registrati di Apple, Inc. negli Stati Uniti e in altri paesi.

AutoCAD è un marchio o un marchio registrato di Autodesk, Inc. e/o delle relative filiali/consociate negli Stati Uniti e in altri paesi.

Bluetooth e il relativo logo sono di proprietà di Bluetooth SIG, Inc.

Borland è un marchio o un marchio registrato di Borland Software Corporation negli Stati Uniti e in altri paesi.

Citrix e Citrix Provisioning Services sono marchi di Citrix Systems, Inc. e/o delle relative filiali registrati come brevetti negli Stati Uniti e in altri paesi.

dBase è un marchio di dataBased Intelligence, Inc.

EMC e SecurID sono marchi o marchi registrati di EMC Corporation negli Stati Uniti o in altri paesi.

ICQ è un marchio e/o un marchio di servizio di ICQ LLC.

Intel e Pentium sono marchi registrati di Intel Corporation negli Stati Uniti e in altri paesi.

Logitech è un marchio o un marchio registrato di Logitech Company negli Stati Uniti e in altri paesi.

Mail.ru è un marchio registrato di Mail.Ru, LLC.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell e Surface sono marchi registrati di Microsoft Corporation negli Stati Uniti e in altri paesi.

Mozilla e Thunderbird sono marchi di Mozilla Foundation.

Novell è un marchio di Novell Inc. registrato negli Stati Uniti e in altri paesi.

Java e JavaScript sono marchi registrati di Oracle Corporation e/o delle relative consociate.

SafeNet è un marchio registrato di SafeNet, Inc.

UNIX è un marchio registrato negli Stati Uniti e in altri paesi ed è utilizzato su licenza di X/Open Company Limited.