kaspersky

Kaspersky Endpoint Security for Mac

© 2026 AO Kaspersky Lab

Sommario

Panoramica su Kaspersky Endpoint Security

Novità di questa versione

Confronto tra le funzioni di Kaspersky Endpoint Security in base allo strumento di gestione di Kaspersky Security Center

Installare e disinstallare l'applicazione

- Kit di distribuzione
- Requisiti hardware e software
- Preparare l'installazione
- Installare Kaspersky Endpoint Security
- Preparare l'applicazione per l'utilizzo
- Disinstallare Kaspersky Endpoint Security

Avviare l'applicazione per la prima volta

Interfaccia dell'applicazione Kaspersky Endpoint Security

- Finestra principale dell'applicazione
- Icona di Kaspersky Endpoint Security
- Finestra delle impostazioni dell'applicazione

Informazioni sulle notifiche

Licensing dell'applicazione Kaspersky Endpoint Security

- Informazioni sul Contratto di licenza con l'utente finale
- Informazioni sulla licenza
- Informazioni sull'abbonamento
- Informazioni sul certificato di licenza
- Informazioni sulla chiave
- Informazioni sul codice di attivazione
- Informazioni sul file chiave
- Informazioni sulla trasmissione dei dati
- Attivare Kaspersky Endpoint Security
- Visualizzare le informazioni sulla licenza
- Gestire licenze e abbonamenti
- Confronto tra le funzionalità dell'applicazione a seconda del tipo di licenza per le workstation

Esecuzione delle attività più comuni

- Aprire e chiudere l'applicazione
- Visualizzare lo stato di protezione del computer
- Visualizzare lo stato operativo dei componenti installati
- Disabilitare e ripristinare la protezione del computer
- Utilizzare Centro protezione
- Eseguire attività di scansione
- Configurare l'avvio automatico di un'attività di scansione pianificata
- Aggiornare i database dell'applicazione
- Come procedere se l'accesso al file è bloccato
- Ripristino di un file eliminato o disinfettato dall'applicazione
- Visualizzare il rapporto sul funzionamento dell'applicazione
- Come procedere se vengono visualizzate finestre di notifica

Configurazione avanzata dell'applicazione
- Ambito di protezione del computer
- Protezione Minacce File
- Protezione Minacce Web
- Protezione minacce di posta
- Protezione Minacce di Rete
- Firewall
- Rilevamento del Comportamento
- Scansione
- Attività di aggiornamento
- Attività locali
  - Attività di scansione dei dischi esterni
- Backup
- Rapporti
- Managed Detection and Response
- Endpoint Detection and Response Expert (on premises)
- Endpoint Detection and Response Optimum
  - Integrazione con Endpoint Detection and Response Optimum
  - Scansione per indicatori di compromissione
  - Sposta file in Quarantena
  - Ottieni file
  - Elimina file
  - Avvia processo
  - Termina processo
  - Prevenzione dell'esecuzione
  - Isolamento di rete del computer
  - Cloud Sandbox
- Criptaggio disco FileVault
- Protezione tramite password
- Prevenzione Exploit
- Motore di Remediation
- Controllo Web
- Controllo dispositivi

Partecipa a Kaspersky Security Network

Verificare l'integrità dei componenti dell'applicazione

Gestire l'applicazione tramite Kaspersky Security Center Administration Console
- Distribuire Kaspersky Endpoint Security in una rete aziendale
- Aggiornare Kaspersky Endpoint Security 11.1 o versione successiva alla versione 12.2.1
- Prepararsi all'installazione remota di Kaspersky Endpoint Security
  - Installare il plug-in di amministrazione di Kaspersky Endpoint Security
  - Installare Network Agent in locale
  - Installare Network Agent tramite Apple Remote Desktop
  - Installare Network Agent tramite Kaspersky Security Center
  - Installare Network Agent tramite il protocollo SSH
  - Disinstallare Network Agent in locale

- Gestire Network Agent dalla riga di comando
  - Avviare/interrompere Network Agent in un computer remoto
  - Controllare manualmente la connessione tra un computer client e Administration Server. Utilità klnagchk
  - Connettere manualmente un computer remoto ad Administration Server. Utilità klmover
  - Disinstallare Network Agent
- Installare e disinstallare Kaspersky Endpoint Security
  - Installare l'applicazione tramite il protocollo SSH
  - Installare l'applicazione tramite Kaspersky Security Center
  - Creare pacchetto di installazione
  - Disinstallare l'applicazione tramite Kaspersky Security Center
- Avviare e interrompere l'applicazione tramite Kaspersky Security Center
- Creare e gestire le attività
  - Creare le attività
  - Avviare e interrompere manualmente le attività
  - Importare ed esportare le attività
  - Visualizzare le attività
  - Gestire impostazioni specifiche delle attività
- Creare e gestire i criteri
  - Creare un criterio
  - Visualizzare l'elenco dei criteri
  - Configurare le impostazioni dei criteri
  - Modificare lo stato del criterio
  - Esportare un criterio in un file KLP
  - Importare un criterio da un file KLP
- Creare e gestire i profili criterio
- Generare un rapporto sugli oggetti rilevati
- Ottenere una chiave di ripristino per un'unità criptata

Amministrazione remota dell'applicazione tramite Kaspersky Security Center Web Console e Cloud Console

- Installare il plug-in Web di Kaspersky Endpoint Security
- Creare un criterio
  - Protezione minacce host
    - Configurare il componente Protezione minacce file
    - Configurare la Scansione unità rimovibili
    - Configurare Rilevamento del Comportamento
    - Configurare Anti-Cryptor
    - Configurazione del componente Prevenzione exploit
    - Configurazione del componente Motore di Remediation
  - Protezione Web e comunicazione
    - Configurare Protezione minacce di posta
    - Configurazione del componente Protezione minacce Web
    - Configurare Protezione Minacce di Rete
    - Configura il componente Firewal
  - Controlli di sicurezza
    - Configurazione del componente Controllo dispositivi
    - Configurazione del componente Controllo Web
  - Criptaggio dei dati

- Impostazioni generali
  - Impostazioni di rilevamento
  - Kaspersky Security Network
  - Interazione utente
  - Auto-difesa
  - Prestazioni
  - Rapporti e archivi
  - Impostazioni di Rete
  - Impostazioni di telemetria
  - Impostazioni degli eventi
  - Impostazioni di aggiornamento
- Agenti integrati
  - Configurare Managed Detection and Response
  - Configurare Endpoint Detection and Response
  - Configurare Endpoint Detection and Response Expert (on-premise)
- Creare le attività
  - Configurare le impostazioni dell'attività Scansione
  - Configurare le impostazioni dell'attività Aggiungi chiave
  - Configurare l'attività Aggiornamento
- Ottenere una chiave di ripristino per un'unità criptata

Gestire l'applicazione dalla riga di comando

- Visualizzare la guida della riga di comando
- Eseguire una scansione anti-malware
- Aggiornare l'applicazione
- Eseguire il rollback dell'ultimo aggiornamento
- Avviare/interrompere un'attività o un componente
- Visualizzare lo stato e le statistiche di un componente o un'attività
- Esportare le impostazioni di protezione
- Attivare l'applicazione
- Installazione dell'estensione di sistema
- Configurare le connessioni di rete
- Rimuovere le chiavi di licenza
- Codici restituiti della riga di comando
- Chiudere l'applicazione
- Disinstallare l'applicazione
- Comandi di gestione Detection and Response
  - Gestire Prevenzione dell'esecuzione
  - Gestire Isolamento di rete

Contattare l'Assistenza tecnica

- Come ottenere assistenza tecnica
- Assistenza tecnica tramite il Kaspersky CompanyAccount
- Acquisire informazioni per l'Assistenza tecnica
- Utilizzare un file di traccia
- Creare un file di traccia

Fonti di informazioni sull'applicazione

Appendici
Problemi noti e limitazioni
Problemi risolti
Elenco di oggetti esaminati in base all'estensione
Maschere nei percorsi di file e cartelle
Requisiti del file IOC
Interpreti di script supportati per Prevenzione dell'esecuzione
Come aggiungere il certificato Kaspersky Endpoint Security all'archivio dei certificati di Mozilla Firefox
Impostazioni di rete per l'interazione con servizi esterni
Informazioni sul codice di terze parti
Note relative ai marchi

Panoramica su Kaspersky Endpoint Security

L'applicazione Kaspersky Endpoint Security protegge i computer che eseguono macOS in presenza di malware e altre minacce per la protezione del computer.

Protezione Minacce File

Protezione Minacce File protegge il file system del computer in tempo reale, intercettando e analizzando i tentativi di accedere ai file. Ulteriori informazioni.

Protezione Minacce Web

Protezione Minacce Web protegge le informazioni inviate e ricevute dal computer tramite i protocolli HTTP e HTTPS in Safari, Google Chrome™ e Firefox™. Ulteriori informazioni.

Protezione minacce di posta

Protezione minacce di posta esamina gli allegati dei messaggi e-mail in entrata e in uscita alla ricerca di malware e altre minacce. Il componente garantisce la protezione del computer mediante database anti-malware, il servizio cloud Kaspersky Security Network e l'analisi euristica. Ulteriori informazioni.

Protezione Minacce di Rete

Protezione Minacce di Rete impedisce le intrusioni nel sistema operativo. Questo componente garantisce protezione dagli autori di attacchi informatici (che utilizzano la scansione delle porte e gli attacchi brute force) e dal malware installato da questi ultimi (compreso malware per i tentativi di invio dei dati personali ai criminali). Ulteriori informazioni.

Firewall

Firewall blocca le connessioni non autorizzate al computer durante l'utilizzo di Internet o della rete locale. Questo consente di proteggere la LAN aziendale da furto di identità e altri attacchi. Il componente garantisce la protezione del computer mediante database anti-malware, il servizio cloud Kaspersky Security Network e le regole di rete predefinite. Ulteriori informazioni.

Rilevamento del Comportamento

Il componente Rilevamento del Comportamento riceve informazioni sulle azioni delle applicazioni nel computer e le fornisce ad altri componenti della protezione per migliorarne le prestazioni. Esegue inoltre l'azione selezionata in risposta all'attività del malware. Ulteriori informazioni.

Prevenzione Exploit

Il componente Prevenzione Exploit rileva codice di programma che sfrutta le vulnerabilità del computer per sfruttare i privilegi di amministratore o per eseguire attività dannose. Ulteriori informazioni.

Motore di Remediation

Motore di Remediation consente a Kaspersky Endpoint Security di eseguire il rollback delle azioni eseguite dal malware nel sistema operativo. Ulteriori informazioni.

Scansione

L'applicazione Kaspersky Endpoint Security rileva e neutralizza su richiesta malware e altre minacce per la sicurezza del computer nell'ambito di scansione specificato. Kaspersky Endpoint Security può eseguire una scansione completa del computer, una scansione rapida delle aree critiche e una scansione dell'ambito specificato. Ulteriori informazioni.

Aggiornamento

Kaspersky Endpoint Security aggiorna i database e i moduli dell'applicazione dai server degli aggiornamenti Kaspersky, dai punti di distribuzione o da altre origini specificate dall'amministratore di sistema e crea copie di backup di tutti i file aggiornati per consentire un rollback dell'ultimo aggiornamento. Ulteriori informazioni.

Backup

Kaspersky Endpoint Security crea una copia di backup di file infetti prima di qualsiasi tentativo di disinfettarli o eliminarli, rendendo possibile il ripristino. Ulteriori informazioni.

Rapporti

Kaspersky Endpoint Security genera i rapporti sugli eventi e sulle azioni che interessano i componenti dell'applicazione. Ulteriori informazioni.

Notifiche

Kaspersky Endpoint Security utilizza le notifiche per informare in merito a determinati eventi nell'esecuzione di Kaspersky Endpoint Security. Le notifiche possono essere accompagnate da segnali acustici. Ulteriori informazioni.

Centro protezione

Kaspersky Endpoint Security visualizza messaggi sullo stato della protezione in Centro protezione. Centro protezione mostra informazioni sullo stato della protezione del computer e su come eliminare problemi e minacce per la sicurezza. Ulteriori informazioni.

Gestione remota dell'applicazione tramite Kaspersky Security Center

È possibile gestire in remoto la protezione dei computer in cui è installato Kaspersky Endpoint Security: ricevere informazioni sullo stato corrente della protezione del computer, risolvere i problemi in remoto, rispondere alle minacce per la protezione del computer, abilitare o disabilitare i componenti della protezione (Protezione Minacce File, Protezione Minacce Web, Protezione Minacce di Rete, Rilevamento del Comportamento), abilitare o disabilitare Controllo Web, Managed Detection and Response, Endpoint Detection and Response, Endpoint Detection and Reponse Expert (on-premise), eseguire attività di scansione, aggiornare i database dell'applicazione, eseguire il criptaggio del disco di avvio e gestire le licenze e gli abbonamenti di Kaspersky Endpoint Security. È possibile utilizzare i seguenti strumenti per gestire Kaspersky Endpoint Security:

- Kaspersky Security Center Administration Console. Ulteriori informazioni.
- Kaspersky Security Center Web Console e Cloud Console. Ulteriori informazioni.

Nota: la funzionalità supportata da Kaspersky Endpoint Security dipende dallo strumento di gestione utilizzato.

Criptaggio disco FileVault

Kaspersky Endpoint Security consente la gestione remota del criptaggio FileVault. Il criptaggio impedisce agli utenti non autorizzati di accedere ai dati sensibili archiviati nel disco di avvio del computer dell'utente.

Controllo Web

È possibile gestire in remoto l'accesso ai siti Web visitati dagli utenti. È possibile consentire o bloccare l'accesso a specifici indirizzi Web o gruppi di indirizzi Web. È inoltre possibile consentire o bloccare l'accesso a determinate categorie di siti Web in base al relativo contenuto. Ulteriori informazioni.

Controllo dispositivi

Controllo dispositivi gestisce l'accesso degli utenti ai dispositivi installati o connessi al computer. Ciò consente di proteggere il computer dalle infezioni quando vengono collegati tali dispositivi e impedire perdite o fughe di dati. Ulteriori informazioni.

Managed Detection and Response

Il componente Managed Detection and Response garantisce l'interazione con il servizio Kaspersky Managed Detection and Response che rileva ed elimina costantemente le minacce per la sicurezza rivolte all'organizzazione. Ulteriori informazioni.

Endpoint Detection and Response

Il componente Endpoint Detection and Response facilita l'interazione con la soluzione Kaspersky Endpoint Detection and Response. Questa funzionalità della soluzione combina il rilevamento automatico delle minacce con la capacità di reagire a queste minacce per contrastare gli attacchi avanzati, inclusi nuovi exploit, ransomware, attacchi senza file, nonché metodi che utilizzano strumenti di sistema legittimi. Ulteriori informazioni.

Endpoint Detection and Response Expert (on premises)

Il componente Endpoint Detection and Response Expert (on-premise) facilita l'interazione con la soluzione Kaspersky Anti Targeted Attack Platform. Questa soluzione rileva prontamente le minacce avanzate, come attacchi mirati, minacce persistenti avanzate, attacchi zero-day e altro. Ulteriori informazioni.

Novità di questa versione

Questa Guida si applica a Kaspersky Endpoint Security for Mac versione 12.2.1.

Kaspersky Endpoint Security offre le seguenti nuove funzionalità e i seguenti miglioramenti:

- Adesso è supportato il nuovo sistema operativo macOS 27 Golden Gate.
- L'interfaccia di gestione dei criteri in Web Console è stata aggiornata. La struttura delle sezioni nel criterio è stata modificata per garantire la coerenza con le interfacce del plug-in di Kaspersky Endpoint Security for Windows e Linux.
- Adesso è possibile visualizzare quali modifiche sono state apportate a un criterio in un determinato periodo, nonché salvare le informazioni su tali modifiche in un file.
- Sono stati aggiunti i nuovi componenti Protezione Minacce di Posta, Controllo dispositivi, Firewall, Motore di Remediation e Prevenzione Exploit.
- Adesso è possibile attivare il componente Managed Detection and Response dall'applicazione Kaspersky Endpoint Security.
- È stata migliorata la visibilità delle azioni di reazione per i dettagli degli avvisi.
- Adesso è possibile gestire il componente Rilevamento del comportamento in Web Console.
- Sono stati aggiunti i riepiloghi degli avvisi.
- Adesso gli utenti riceveranno una notifica se un oggetto è un oggetto critico di sistema prima che venga eseguita qualsiasi azione di reazione.
- Adesso è possibile modificare i file IOC direttamente in Web Console durante la creazione o la modifica delle impostazioni delle attività di Scansione IOC.
- Adesso è possibile spostare gli oggetti rilevati in Quarantena dai dettagli degli avvisi.
- Sono stati aggiunti avvisi per azioni limitate per l'attività di Isolamento di rete.
- Correzioni di bug generali e miglioramenti.

Confronto tra le funzioni di Kaspersky Endpoint Security in base allo strumento di gestione di Kaspersky Security Center

La funzionalità supportata da Kaspersky Endpoint Security dipende dallo strumento di gestione utilizzato (vedere la tabella di seguito).

È possibile utilizzare i seguenti strumenti per gestire Kaspersky Endpoint Security:

- Kaspersky Security Center Administration Console. Uno snap-in per Microsoft Management Console (MMC) installato nella workstation dell'amministratore di Kaspersky Security Center.
- Kaspersky Security Center Web Console. Un componente di Kaspersky Security Center installato in Administration Server. È possibile utilizzare Web Console tramite un browser in qualsiasi computer che abbia accesso ad Administration Server.
- Kaspersky Security Center Cloud Console. La versione cloud di Kaspersky Security Center.

Confronto tra le funzionalità di Kaspersky Endpoint Security

Funzionalità	Kaspersky Security Center		
	Administration Console	Web Console	Cloud Console
Protezione Minacce Avanzata			
Kaspersky Security Network	✓	✓	✓
Rilevamento del Comportamento	✓	✓	
Prevenzione Exploit	✓	✓	
Motore di Remediation	✓	✓	
Protezione Minacce Essenziale			
Protezione Minacce File	✓	✓	✓
Protezione Minacce Web	✓	✓	✓
Protezione Minacce di Rete	✓	✓	✓
Protezione minacce di posta	✓	✓	
Firewall	✓	✓	
Controlli di sicurezza			
Controllo Web	✓	✓	✓
Controllo dispositivi	✓	✓	
Criptaggio dei dati			
Criptaggio disco FileVault	✓	✓	✓
Chiave di ripristino	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Endpoint Detection and Response		✓	
Endpoint Detection and Response Expert (on premises)	✓	✓	✓
Attività			

Funzionalità	Kaspersky Security Center		
	Administration Console	Web Console	Cloud Console
Aggiungi chiave	✓	✓	✓
Aggiornamento	✓	✓	✓
Scansione rapida	✓	✓	
Rollback	✓	✓	✓
Scansione	✓	✓	✓

Installare e disinstallare l'applicazione

Kit di distribuzione

Il kit di distribuzione include il pacchetto di installazione di Kaspersky Endpoint Security, che contiene i seguenti file:

- File necessari per l'installazione dell'applicazione in uno dei modi disponibili.
- Il file license_<loc>.txt con il Contratto di licenza con l'utente finale.
  Il Contratto di licenza con l'utente finale specifica le condizioni di utilizzo dell'applicazione.

Decomprimere il pacchetto di installazione compresso per accedere ai relativi file.

Requisiti hardware e software

Kaspersky Endpoint Security presenta i seguenti requisiti hardware e software:

- Tipo di processore: Intel, Apple Silicon
- 4 GB di memoria (RAM)
- 5 GB di spazio su disco disponibile
- macOS 14, 15, 26, 27
- Connessione Internet

Browser supportati:

- Safari
- Chrome
- Firefox

Kaspersky Endpoint Security è compatibile con i seguenti strumenti di virtualizzazione:

- Parallels Desktop 16 for Mac Business Edition o versione successiva
- VMware Fusion™ 11.5 Professional
- VMware Fusion 12 Professional
- VMware Fusion 13 Pro

È possibile distribuire i profili MDM con i server Jamf e Apple. Se si utilizzano altri server, consultare l'articolo nel sito Web dell'Assistenza tecnica (Knowledge Base).

È possibile gestire Kaspersky Endpoint Security in remoto tramite Kaspersky Security Center. È richiesto Kaspersky Security Center 14.2 o versione successiva per la gestione di Kaspersky Endpoint Security utilizzando il plug-in di amministrazione per Kaspersky Security Center Administration Console e il plug-in Web per Kaspersky Security Center Web Console.

Nota: per gestire Kaspersky Endpoint Security for Mac 12.2.1 tramite Kaspersky Security Center, è necessario installare Network Agent versione 15 nei computer remoti.

Preparare l'installazione

Prima di installare l'applicazione nel computer, è consigliabile eseguire le seguenti operazioni:

- Verificare che il computer soddisfi i requisiti hardware e software.
- Rimuovere Kaspersky Internet Security for Mac o eventuali altre applicazioni anti-malware per evitare conflitti di sistema e ottimizzare le prestazioni del sistema.

Nota: prima di installare Kaspersky Endpoint Security in remoto, è consigliabile scaricare l'archivio KES_for_macOS11_and_later.zip dal sito Web dell'Assistenza tecnica di Kaspersky e applicare il profilo di configurazione KES_for_macOS11_and_later_profile.mobileconfig nel computer client utilizzando gli strumenti di gestione remota Apple. Questo consentirà a Kaspersky Endpoint Security di ottenere quanto segue: autorizzazioni per installare l'estensione Kernel e l'estensione di sistema, accesso completo al disco e autorizzazioni per configurare le connessioni di rete. Per ulteriori informazioni sul profilo di configurazione e altre opzioni, visitare il sito Web dell'Assistenza tecnica.

Installare Kaspersky Endpoint Security

Importante: gli esperti di Kaspersky consigliano di installare Kaspersky Endpoint Security solo con le modalità descritte nella presente guida.

È possibile installare Kaspersky Endpoint Security in uno dei modi seguenti:

- In locale, dal kit di distribuzione scaricato dal sito Web di Kaspersky.
- Utilizzo in remoto di Apple Remote Desktop
- In remoto tramite Kaspersky Security Center Administration Console.
- In remoto tramite Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console.

  Per informazioni dettagliate sulla distribuzione delle applicazioni Kaspersky con l'utilizzo di Kaspersky Security Center Web Console, consultare la Guida di Kaspersky Security Center. Per informazioni dettagliate sulla distribuzione delle applicazioni Kaspersky con l'utilizzo di Kaspersky Security Center Cloud Console, consultare la Guida di Kaspersky Security Center Cloud Console.

Eseguire un'installazione standard di Kaspersky Endpoint Security

1. Decomprimere l'archivio ZIP dal kit di distribuzione.
2. Aprire il file DMG dai contenuti dell'archivio decompresso.
3. Nella finestra visualizzata fare doppio clic su **Installa Kaspersky Endpoint Security**.

   Verrà visualizzato l'assistente all'installazione di Kaspersky Endpoint Security.
4. Fare clic su **Installa**.
5. Seguire i passaggi dell'assistente all'installazione per completare l'installazione.

   Al termine dell'installazione, Kaspersky Endpoint Security viene avviato automaticamente. Non è necessario riavviare il computer.

Nota: se viene utilizzato questo metodo di installazione, i componenti Endpoint Detection and Response Expert (on-premise), Endpoint Detection and Response (Optimum) e Cloud Sandbox non vengono installati.

Eseguire un'installazione personalizzata di Kaspersky Endpoint Security

1. Decomprimere l'archivio ZIP dal kit di distribuzione.
2. Aprire il file DMG dai contenuti dell'archivio decompresso.
3. Nella finestra visualizzata fare doppio clic su **Installa Kaspersky Endpoint Security**.

   Verrà visualizzato l'assistente all'installazione di Kaspersky Endpoint Security.
4. Fare clic su **Personalizza**, selezionare o deselezionare le caselle di controllo accanto ai componenti che non si desidera installare e fare clic su **Continua**.
5. Seguire i passaggi dell'assistente all'installazione per completare l'installazione.

   Al termine dell'installazione, Kaspersky Endpoint Security viene avviato automaticamente. Non è necessario riavviare il computer.

Installare Kaspersky Endpoint Security in remoto utilizzando Apple Remote Desktop

1. Nel Mac scegliere **menu Apple** > **Impostazioni di Sistema** > **Generale** > **Condivisione**.
2. Selezionare la casella di controllo **Gestione remota**.
3. In un altro Mac che si desidera impostare come server, installare Apple Remote Desktop. Per ulteriori informazioni su Apple Remote Desktop, fare riferimento al Supporto Apple.
4. Aprire Apple Remote Desktop.
5. Nella finestra **Desktop remoto** fare clic su **Scanner** a sinistra e selezionare i dispositivi in cui si desidera installare Kaspersky Endpoint Security.
6. Fare clic su **Installa**.
7. Nella richiesta delle credenziali di amministratore immettere un nome e una password amministratore e fare clic su **Aggiungi**.

8. Fare clic su + e selezionare il file DMG con il pacchetto di installazione di Kaspersky Endpoint Security.
9. Fare clic su **Installa**.

L'installazione di Kaspersky Endpoint Security viene avviata nei dispositivi selezionati.

Preparare l'applicazione per l'utilizzo

Dopo l'installazione di Kaspersky Endpoint Security, è possibile eseguire le seguenti operazioni:

- Attivare Kaspersky Endpoint Security. In seguito all'attivazione dell'applicazione, Kaspersky Endpoint Security avvia la protezione del computer e sarà possibile aggiornare regolarmente i database e i moduli dell'applicazione, eseguire attività di scansione anti-malware e inviare richieste all'Assistenza tecnica.

  Il componente Managed Detection and Response viene attivato separatamente in Kaspersky Security Center Administration Console o Web Console.

  Se il componente Endpoint Detection and Response non è supportato dalla licenza corrente, è necessario attivare separatamente Kaspersky Endpoint Detection and Response.

- Valutare lo stato di protezione del computer.
- Aggiornare Kaspersky Endpoint Security.
- Esaminare il computer per rilevare la presenza di malware.

Disinstallare Kaspersky Endpoint Security

1. Aprire il file DMG del kit di distribuzione dell'applicazione.
2. Nella finestra con il contenuto del kit di distribuzione fare doppio clic su **Disinstalla Kaspersky Endpoint Security**.

   Il programma di disinstallazione di Kaspersky Endpoint Security viene avviato.
3. Nella finestra del programma di disinstallazione fare clic su **Disinstalla**.
4. Quando vengono richieste le credenziali di amministratore, immettere il nome e la password dell'amministratore e confermare che si desidera disinstallare Kaspersky Endpoint Security.

   Verrà avviata la disinstallazione di Kaspersky Endpoint Security.
5. Leggere le informazioni sul completamento della disinstallazione e fare clic su **Esci** per chiudere il programma di disinstallazione.

Kaspersky Endpoint Security è stato disinstallato dal computer. Non è necessario riavviare il computer dopo la disinstallazione dell'applicazione.

Avviare l'applicazione per la prima volta

Kaspersky Endpoint Security viene avviato nel computer subito dopo l'installazione. Per proteggere subito il Mac, l'applicazione richiede di eseguire la configurazione di base:

- Concedere le autorizzazioni necessarie a Kaspersky Endpoint Security per proteggere il Mac da malware, attacchi di rete e minacce Internet.

  Per ulteriori informazioni sulle autorizzazioni da concedere, fare clic su ?.

- Attivare Kaspersky Endpoint Security.

Nota: per la configurazione di base di Kaspersky Endpoint Security è necessaria una connessione Internet.

Avviare Kaspersky Endpoint Security per la prima volta

1. Nella finestra **Protezione essenziale** eseguire le seguenti azioni per assicurarsi che Protezione Minacce File e Protezione Minacce Web funzionino correttamente:

   - Per far funzionare correttamente l'applicazione Kaspersky Endpoint Security, consentire all'applicazione di esaminare ogni file presente nel Mac. A tale scopo, fare clic su **Consenti** accanto all'elemento **Accesso completo al disco** e seguire le istruzioni visualizzate.

   - Se si desidera che Kaspersky Endpoint Security ispezioni URL e pacchetti di rete prima che possano danneggiare il Mac, installare l'estensione di sistema. A tale scopo, fare clic su **Installa** accanto all'elemento **Estensione di sistema** e seguire le istruzioni visualizzate.

   - Se si desidera che l'estensione di sistema funzioni correttamente, consentire il filtro dei contenuti di rete. A tale scopo, fare clic su **Consenti** accanto all'elemento **Filtro dei contenuti di rete** e seguire le istruzioni visualizzate.

   - Se si desidera che Kaspersky Endpoint Security esegua la ricerca di malware e minacce Internet nel traffico HTTPS criptato, installare il certificato attendibile. A tale scopo, fare clic su **Installa** accanto all'elemento **Certificato attendibile** e seguire le istruzioni visualizzate.

   Importante: l'applicazione Kaspersky Endpoint Security non funzionerà correttamente senza queste autorizzazioni. È necessario concedere tutte le autorizzazioni nella finestra **Protezione essenziale**.

2. Fare clic su **Continua**.

Verrà visualizzata la finestra principale dell'applicazione.

Interfaccia dell'applicazione Kaspersky Endpoint Security

Finestra principale dell'applicazione

Aprire la finestra principale dell'applicazione

Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Kaspersky Endpoint Security**.

La finestra principale dell'applicazione di Kaspersky Endpoint Security contiene elementi dell'interfaccia che forniscono l'accesso alle funzioni principali dell'applicazione.

La finestra principale dell'applicazione è divisa in due parti:

- La parte sinistra contiene la barra laterale, che consente di navigare nell'applicazione e di accedere rapidamente alle funzioni principali.
- La parte centrale visualizza il contenuto della sezione selezionata nella barra laterale e consente di gestire i dati.

Barra laterale

La barra laterale della finestra principale dell'applicazione presenta le seguenti opzioni:

Monitoraggio	Fare clic per aprire la pagina **Monitoraggio**, che fornisce informazioni su cosa sta facendo Kaspersky Endpoint Security per proteggere il computer.
Centro protezione	Fare clic per visualizzare lo stato di protezione del computer. Ulteriori informazioni.
Sicurezza	Fare clic per visualizzare lo stato operativo dei componenti installati. Ulteriori informazioni.
Scansione	Fare clic per gestire le attività di scansione. Ulteriori informazioni.
Aggiornamento	Fare clic per gestire le attività di aggiornamento. Ulteriori informazioni.
Licenza	Fare clic per attivare l'applicazione o visualizzare le informazioni sulla licenza. Ulteriori informazioni.

Controlli della pagina **Monitoraggio**

La pagina **Monitoraggio** visualizza l'indicatore dello stato della protezione, fornisce informazioni su cosa sta facendo Kaspersky Endpoint Security per proteggere il computer e contiene i seguenti controlli.

Centro protezione	Informa sui problemi di protezione del computer. Ulteriori informazioni.
Rapporti	Consente di visualizzare gli eventi che si sono verificati durante il funzionamento dell'applicazione, dei singoli componenti e delle attività. Ulteriori informazioni.
Backup	Consente di visualizzare un elenco di copie salvate dei file infetti eliminati dall'applicazione. Ulteriori informazioni. Ulteriori informazioni.

Rilevamento delle minacce	Consente di visualizzare le informazioni sulle tecnologie di rilevamento delle minacce applicate da Kaspersky Endpoint Security e sul numero di minacce rilevate da queste tecnologie.
Kaspersky Security Network	Visualizza lo stato della connessione tra Kaspersky Endpoint Security e Kaspersky Security Network, nonché le statistiche globali di Kaspersky Security Network.

Icona di Kaspersky Endpoint Security

Al termine dell'installazione di Kaspersky Endpoint Security, l'icona di Kaspersky Endpoint Security appare nella barra dei menu. Quando l'applicazione è attivata, l'icona dell'applicazione visualizza lo stato dell'applicazione. Se l'icona dell'applicazione è attiva ( ), tutti o alcuni componenti della protezione sono abilitati. Se l'icona dell'applicazione non è attiva ( ), tutti o alcuni componenti della protezione sono disabilitati.

Aprire il menu dell'icona dell'applicazione

Nella barra dei menu fare clic sull'icona dell'applicazione.

Per impostazione predefinita, l'icona dell'applicazione è sempre visualizzata nella barra dei menu. È possibile rimuovere l'icona dell'applicazione dalla barra dei menu.

Rimuovere l'icona dell'applicazione dalla barra dei menu

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Interfaccia** della sezione **Icona dell'applicazione** deselezionare la casella **Mostra nella barra dei menu**.

Quando si apre la finestra dell'applicazione, l'icona dell'applicazione compare anche nel **Dock**.

Dal menu dell'icona dell'applicazione è possibile accedere alla finestra principale dell'applicazione ed eseguire le seguenti azioni:

- Disabilitare la protezione del computer.
- Ripristinare la protezione del computer.
- Aprire Centro protezione.
- Avvia scansione rapida.
- Eseguire un aggiornamento.
- Aprire la finestra delle impostazioni dell'applicazione.
- Chiudere Kaspersky Endpoint Security.

Finestra delle impostazioni dell'applicazione

Aprire la finestra delle impostazioni dell'applicazione

Eseguire una delle seguenti operazioni:

- Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.
- Nella barra dei menu fare clic su **Kaspersky Endpoint Security** > **Impostazioni**.
- Se Kaspersky Endpoint Security è in esecuzione, fare clic sull'icona dell'applicazione nel **Dock** e scegliere **Impostazioni**.

È possibile accedere velocemente alle impostazioni dell'applicazione utilizzando le seguenti schede nella parte superiore della finestra delle impostazioni:

- **Essenziale**. In questa scheda è possibile abilitare o disabilitare la protezione del computer e configurare le impostazioni di Protezione Minacce File, Protezione Minacce Web e Protezione Minacce di Rete.
- **Scansione**. In questa scheda è possibile configurare le impostazioni per le attività di scansione e l'avvio pianificato di tali attività.
- **Minacce**. In questa scheda è possibile selezionare le categorie di oggetti da rilevare, creare l'Area attendibile e configurare le impostazioni di Backup.
- **Avanzate**. In questa scheda è possibile iscriversi a o disiscriversi da Kaspersky Security Network.
- **Aggiornamento**. In questa scheda è possibile configurare le impostazioni degli aggiornamenti dell'applicazione o eseguire il rollback alla versione precedente dei database dell'applicazione.
- **Interfaccia**. In questa scheda è possibile configurare le impostazioni relative ai rapporti, alle notifiche e all'icona di Kaspersky Endpoint Security, nonché abilitare o disabilitare la registrazione delle informazioni di debug in un file di traccia.

Utilizzando il pulsante  è possibile impedire agli utenti che non dispongono dei diritti di amministratore di modificare le impostazioni di Kaspersky Endpoint Security. Il pulsante è disponibile nella parte inferiore della finestra delle impostazioni dell'applicazione. Per modificare le impostazioni, è necessario immettere le credenziali dell'amministratore.

Il pulsante ? consente di aprire la Guida di Kaspersky Endpoint Security, in cui vengono descritte tutte le impostazioni della finestra dell'applicazione corrente. È inoltre possibile aprire l'argomento della Guida per la finestra dell'applicazione attiva selezionando **Apri la Guida per questa finestra** nel menu della **Guida**.

Informazioni sulle notifiche

Kaspersky Endpoint Security visualizza notifiche per informare in merito agli eventi dell'applicazione. A seconda della versione del sistema operativo installato nel computer, le notifiche vengono visualizzate nel Centro Notifiche del sistema operativo. La visualizzazione delle notifiche dipende dalle opzioni impostate nelle impostazioni di notifica del sistema operativo.

Gli eventi di Kaspersky Endpoint Security si suddividono in tre tipi, in base all'importanza:

- *Critici* - eventi che rappresentano una minaccia per la protezione del computer (rilevamento di oggetti dannosi, vulnerabilità, problemi relativi a Kaspersky Endpoint Security). Gli eventi critici richiedono attenzione immediata da parte dell'utente. È consigliabile non disabilitare le notifiche sugli eventi critici.

- *Importanti* - eventi che non richiedono attenzione immediata da parte dell'utente, ma possono rappresentare una minaccia futura per la protezione del computer.

- *Informativi* - gli eventi segnalati a scopo informativo.

Disabilitazione delle notifiche

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Interfaccia**, nella sezione **Notifiche**, deselezionare la casella di controllo **Abilita notifiche per eventi**.

Abilitare la registrazione degli eventi non critici

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Interfaccia**, nella sezione **Rapporti**, selezionare la casella di controllo **Registra eventi non critici** per ricevere le notifiche sugli eventi informativi di Kaspersky Endpoint Security.

Indipendentemente dal fatto che le notifiche siano abilitate o disabilitate, i rapporti di applicazione includono informazioni sugli eventi che si verificano durante l'esecuzione di Kaspersky Endpoint Security.

Le notifiche possono essere accompagnate da segnali acustici (ad esempio le notifiche su un malware rilevato). È possibile disabilitare l'avviso sonoro.

La registrazione di eventi non critici determina un aumento significativo delle dimensioni totali del file del rapporto. Tenere presente che questa impostazione si applica solo a Protezione Minacce File.

Disabilitazione dei segnali acustici che accompagnano le notifiche

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Interfaccia**, nella sezione **Notifiche**, deselezionare la casella di controllo **Attiva le notifiche acustiche al rilevamento del malware**.

Se è necessaria un'azione in risposta a un evento, Kaspersky Endpoint Security visualizza una finestra di notifica. Ad esempio, quando l'applicazione rileva un oggetto dannoso, richiede di eliminare o disinfettare l'oggetto. La finestra di notifica scompare solo dopo la selezione di una delle azioni.

Licensing dell'applicazione Kaspersky Endpoint Security

Informazioni sul Contratto di licenza con l'utente finale

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

Importante: leggere attentamente il Contratto di licenza prima di iniziare a utilizzare l'applicazione.

È possibile consultare i termini del Contratto di licenza con l'utente finale utilizzando i metodi seguenti:

- Durante l'installazione di Kaspersky Endpoint Security
- Leggendo il documento license.txt nella cartella di installazione dell'applicazione

Installando Kaspersky Endpoint Security, l'utente conferma di avere compreso e accettato le condizioni del Contratto di licenza con l'utente finale. Se non si accettano le condizioni del Contratto di licenza con l'utente finale, annullare l'installazione di Kaspersky Endpoint Security ed evitare di utilizzare l'applicazione.

Informazioni sulla licenza

Per *licenza* si intende un diritto limitato nel tempo di utilizzare Kaspersky Endpoint Security, concesso conformemente alle condizioni del Contratto di licenza firmato (Contratto di licenza con l'utente finale).

L'ambito dei servizi e il periodo di validità dipendono dalla licenza con cui viene utilizzata l'applicazione.

Sono disponibili i seguenti tipi di licenza:

- *Di prova*. Una licenza gratuita che consente di acquisire familiarità con l'applicazione.

  Una licenza di prova ha in genere un periodo di validità breve. Alla scadenza di una 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 utilizzare l'applicazione con una licenza di prova per un solo periodo di prova.

- *Commerciale*. Una licenza a pagamento.

  Quando una licenza commerciale scade, le funzionalità chiave dell'applicazione vengono disabilitate. Per continuare a utilizzare Kaspersky Endpoint Security, è necessario rinnovare la licenza commerciale. Dopo la scadenza della licenza commerciale, non sarà possibile continuare a utilizzare l'applicazione e bisognerà rimuoverla dal dispositivo.

  È consigliabile rinnovare la licenza prima della scadenza per garantire la protezione ininterrotta da tutte le minacce per la protezione.

Informazioni sull'abbonamento

L'*abbonamento a Kaspersky Endpoint Security* consiste in un ordine di acquisto dell'applicazione con parametri specifici (data di scadenza, numero di dispositivi protetti). È possibile ordinare l'abbonamento a Kaspersky Endpoint Security dal provider di servizi, ad esempio il provider di servizi Internet. È possibile gestire l'abbonamento nell'area riservata presente nel sito Web del provider di servizi. Ad esempio, è possibile rinnovare o annullare l'abbonamento, ridurre il periodo di validità o modificare il numero di dispositivi protetti con l'abbonamento.

Un abbonamento può essere limitato (ad esempio per un anno) o illimitato (senza data di scadenza). Per continuare a utilizzare Kaspersky Endpoint Security dopo la scadenza del periodo di validità di un abbonamento limitato, è necessario provvedere manualmente al rinnovo. Un abbonamento illimitato viene rinnovato automaticamente previo pagamento anticipato al provider di servizi.

Se si utilizza l'applicazione con un abbonamento limitato, allo scadere dell'abbonamento verrà concesso un periodo di tolleranza per il rinnovo dell'abbonamento. L'applicazione rimane funzionante durante il periodo di tolleranza.

Allo scadere dell'abbonamento per gli aggiornamenti e al termine del periodo di tolleranza per il rinnovo dell'abbonamento, Kaspersky Endpoint Security continua a funzionare ma interrompe l'aggiornamento dei database dell'applicazione.

Allo scadere dell'abbonamento per gli aggiornamenti e la protezione e al termine del periodo di tolleranza per il rinnovo dell'abbonamento, Kaspersky Endpoint Security interrompe la protezione del computer.

Per utilizzare Kaspersky Endpoint Security con un abbonamento, è necessario aggiungere il codice di attivazione ricevuto dal provider di servizi. Nel caso di utilizzo dell'applicazione con abbonamento, non è possibile utilizzare un codice di attivazione diverso per il rinnovo dell'abbonamento. È possibile applicare un codice di attivazione diverso solo se l'abbonamento scade o se si annulla l'abbonamento. Per annullare l'abbonamento, contattare il provider di servizi da cui è stato acquistato Kaspersky Endpoint Security.

Nota: è possibile applicare un codice di attivazione dell'abbonamento diverso solo quando la chiave attiva viene eliminata. L'abbonamento non dispone di un file chiave. Non è possibile aggiungere l'abbonamento come chiave di riserva. Non è possibile aggiungere una chiave di riserva quando l'abbonamento è in uso.

Se si utilizza già Kaspersky Endpoint Security con una licenza valida ma si desidera utilizzare l'applicazione con l'abbonamento, rimuovere la chiave attiva corrente per poter attivare l'applicazione tramite una chiave con abbonamento. Il codice di attivazione precedentemente utilizzato per l'attivazione dell'applicazione nel computer corrente può essere utilizzato in un altro computer.

Nota: le opzioni di abbonamento possibili possono variare in base al provider di servizi. Alcuni provider di servizi possono inoltre scegliere di non concedere un periodo di tolleranza per il rinnovo degli abbonamenti.

Informazioni sul certificato di licenza

Un *certificato di licenza* è un documento che si riceve insieme a un file chiave o a un codice di attivazione.

Un certificato di licenza contiene le seguenti informazioni sulla licenza fornita:

- Chiave di licenza o numero d'ordine
- Informazioni sull'utente a cui è stata concessa la licenza
- Informazioni sull'applicazione che può essere attivata con la licenza fornita
- Limite relativo al numero di unità di licenza (ad esempio i dispositivi in cui l'applicazione può essere utilizzata con la licenza fornita)
- Data di inizio validità della licenza
- Data di scadenza della licenza o durata della licenza
- Tipo di licenza

Informazioni sulla chiave

La *chiave* è una sequenza di bit con cui è possibile attivare e quindi utilizzare l'applicazione in conformità alle condizioni del Contratto di licenza con l'utente finale. Le chiavi sono generate dagli specialisti di Kaspersky.

È possibile aggiungere una chiave all'applicazione tramite uno dei seguenti metodi: applicando un *file chiave* o immettendo un *codice di attivazione*. La chiave viene visualizzata nell'interfaccia dell'applicazione come una sequenza alfanumerica univoca dopo che viene aggiunta all'applicazione.

La chiave può essere bloccata da Kaspersky in caso di violazione delle condizioni del Contratto di licenza. Se la chiave è stata bloccata, è necessario aggiungere un'altra chiave se si desidera utilizzare l'applicazione.

Una chiave può essere attiva o di riserva.

Una *chiave attiva* è una chiave attualmente utilizzata dall'applicazione. Una chiave attiva può essere aggiunta per una licenza di prova o commerciale o per un abbonamento. L'applicazione non può avere più di una chiave attiva.

Una *chiave di riserva* è una chiave che consente l'utilizzo dell'applicazione da parte dell'utente, ma non è attualmente in uso. Una chiave di riserva diventa automaticamente attiva alla scadenza della licenza associata alla chiave attiva. È possibile aggiungere una chiave di riserva solo se è già stata aggiunta una chiave attiva.

Una chiave per una licenza di prova può essere aggiunta come chiave attiva. Non è possibile aggiungere una chiave per una licenza di prova come chiave di riserva. Una chiave di riserva non può essere aggiunta quando è attiva la chiave per una licenza di prova.

Informazioni sul codice di attivazione

Un *codice di attivazione* è una sequenza univoca di 20 lettere e numeri. È necessario immettere un codice di attivazione per aggiungere una chiave di licenza per l'attivazione di Kaspersky Endpoint Security. Il codice di attivazione viene inviato all'indirizzo e-mail fornito al momento dell'acquisto di Kaspersky Endpoint Security o della richiesta della versione di prova di Kaspersky Endpoint Security.

Per attivare l'applicazione utilizzando il codice di attivazione, è necessario l'accesso a Internet per connettersi ai server di attivazione di Kaspersky.

In caso di smarrimento del codice di attivazione dopo l'installazione dell'applicazione, contattare il partner Kaspersky da cui è stata acquistata la licenza.

Informazioni sul file chiave

Un *file chiave* è un file con estensione key fornito all'utente da Kaspersky. I file chiave vengono utilizzati per attivare l'applicazione aggiungendo una chiave di licenza.

Il file chiave viene inviato all'indirizzo e-mail fornito al momento dell'acquisto di Kaspersky Endpoint Security o dell'ordine della versione di prova di Kaspersky Endpoint Security.

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

È possibile ripristinare un file chiave se è stato eliminato accidentalmente. Un file chiave può ad esempio essere necessario per la registrazione di un Kaspersky CompanyAccount.

Per ripristinare il file chiave, eseguire una delle seguenti azioni:

- Contattare il venditore della licenza.
- Ricevere un file chiave tramite il sito Web di Kaspersky utilizzando il codice di attivazione disponibile.

Informazioni sulla trasmissione dei dati

Contratto di licenza con l'utente finale

Quando si attiva Kaspersky Endpoint Security con il codice di attivazione, allo scopo di verificare la legittimità dell'utilizzo dell'applicazione e di fornire le informazioni statistiche di distribuzione e utilizzo dei prodotti Kaspersky, si accetta di fornire automaticamente le seguenti informazioni durante l'utilizzo di Kaspersky Endpoint Security:

- Tipo, versione e localizzazione del software installato.
- Le versioni degli aggiornamenti installati.
- Identificatore del computer e identificatore dell'installazione del software nel computer.
- Il codice di attivazione e l'identificatore univoco dell'attivazione per la licenza corrente.
- Tipo, versione e dimensione delle parole del sistema operativo.
- Nome dell'ambiente virtuale quando il software è installato in un ambiente virtuale.
- Identificatori dei componenti software attivi al momento dell'invio delle informazioni.
- La sorgente dei dati supportata.
- Timeout.
- Data e ora sul computer dell'utente.

- Versione del protocollo.
- Tipo di contenuti del protocollo.
- Lunghezza dei contenuti del protocollo.
- Il tipo di compressione dei dati utilizzato.
- Il tipo di firma nel ticket di attivazione.
- Identificatore del Centro di attivazione regionale.
- Hash del codice di attivazione calcolato utilizzando l'algoritmo SHA1.
- Hash del corpo del ticket calcolato utilizzando l'algoritmo SHA1.
- Data e ora di creazione del ticket della licenza.
- Identificatore dell'attivazione della licenza.
- Identificatore del ticket della licenza corrente.
- Identificatore della sequenza di ticket della licenza.
- Data e ora dell'attivazione della licenza.
- Data e ora della scadenza della licenza.
- Stato della licenza.
- La versione della licenza.
- L'identificatore univoco del computer dell'utente.
- Versione dell'intestazione del ticket della licenza.
- Nome applicazione.
- Tipo di dati trasferiti.
- Versione dello scherma dei dati trasferiti.
- La versione completa del sistema operativo.
- Descrizione della macchina virtuale utilizzata.
- Elenco di ID per le applicazioni compatibili.

Quando si utilizzano i server degli aggiornamenti Kaspersky per scaricare gli aggiornamenti, per aumentare l'efficienza della procedura di aggiornamento, si accetta di inviare periodicamente le seguenti informazioni per l'identificazione dell'applicazione durante gli aggiornamenti dei moduli e del database:

- ID Software (AppID).
- ID licenza attiva.

- ID installazione software univoco (InstallationID).
- ID avvio attività di aggiornamento univoco (SessionID).
- Versione dell'applicazione (BuildInfo).

Informativa su Kaspersky Security Network (KSN)

L'uso di KSN può aumentare la velocità di risposta del Software in caso di minacce alla sicurezza della rete. Lo scopo dichiarato viene conseguito mediante le seguenti azioni:

- Determinando la reputazione degli oggetti esaminati.
- Identificando le minacce per la protezione delle informazioni nuove e difficili da rilevare e le relative origini.
- Adozione di misure tempestive per aumentare la protezione dei dati archiviati ed elaborati dall'Utente finale con il computer.
- Riducendo la probabilità di falsi positivi.
- Aumentando l'efficienza dei componenti dell'applicazione.
- Analisi dell'infezione del computer di un utente.
- Migliorando le prestazioni dei prodotti Kaspersky.
- Ricevendo le informazioni di riferimento sul numero di oggetti con reputazione nota.
- Identificando e correggendo tempestivamente gli errori relativi all'installazione, alla rimozione e all'aggiornamento del prodotto.

Durante l'utilizzo di KSN, Kaspersky riceverà ed elaborerà automaticamente i dati. I dati trasmessi dall'utente dipendono dal tipo di licenza installata e dalle impostazioni di utilizzo di Kaspersky Security Network specificate.

Se si utilizza una licenza per 1-4 nodi, durante l'uso di Kaspersky Security Network Kaspersky riceve ed elabora automaticamente i seguenti dati:

- Informazioni sulla licenza utilizzata: tipo di licenza e relativo periodo di validità, numero di giorni restanti prima della scadenza della licenza, identificatore del partner dal quale la licenza è stata acquistata, identificatore del Centro regionale di attivazione, checksum del codice di attivazione, hash del corpo del ticket calcolato tramite l'algoritmo SHA1, data e ora di creazione del ticket di licenza, identificatore dei dati della licenza, identificatore del ticket della licenza, identificatore di sequenza del ticket della licenza, identificatore univoco del computer dell'utente, data di inizio validità del ticket della licenza, data di fine validità del ticket della licenza, stato corrente del ticket della licenza, versione intestazione ticket, versione della licenza, identificatore certificato di firma intestazione ticket, checksum del file chiave, numero di serie firmatario intestazione ticket, token di autenticazione.

- Versione completa del Software installato; tipo di software installato; ID aggiornamento Software; ID del servizio di reputazione; ID del tipo di protocollo; ID di un centro di attivazione regionale; versione dell'elenco delle decisioni del servizio Software revocato; ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record dei database anti-virus del Software attivati; ID univoco dell'istanza di installazione dell'applicazione nel computer; data di attivazione della licenza; data di scadenza della licenza; identificatore della licenza; stato della licenza utilizzata dal software; tipo di checksum per l'oggetto elaborato; nome del malware rilevato o del software legittimo che può essere utilizzato per danneggiare i dati o il dispositivo dell'utente; checksum dell'oggetto elaborato; checksum del codice di attivazione del Software; versione completa del software; ID dispositivo univoco; ID Software; checksum del file chiave del Software; ID del modello di informazioni utilizzato per fornire la licenza Software; identificatore del certificato utilizzato per accedere all'intestazione del ticket della licenza Software; data e ora di creazione del ticket di licenza Software; checksum del ticket di licenza Software; versione del ticket di licenza Software; versione del codice di attivazione del Software; formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; ID ticket licenza corrente; ID componente Software; risultato dell'azione del Software; codice errore; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); numero di porta; indirizzo Web dell'origine della richiesta del servizio Web (Referrer); chiave pubblica del certificato; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash.

Se si utilizza una licenza per 5 o più nodi, durante l'uso di Kaspersky Security Network Kaspersky riceve ed elabora automaticamente i seguenti dati:

- Informazioni sulla versione del sistema operativo (OS) e dei service pack installati sul computer, sulla versione e sui checksum (MD5, SHA2-256, SHA1) del file kernel del sistema operativo e sui parametri della modalità di esecuzione del sistema operativo; versione del sistema operativo, numero build del sistema operativo, numero di aggiornamento del sistema operativo, edizione del sistema operativo, informazioni estese sull'edizione del sistema operativo; versione Service Pack del sistema operativo; data e ora di avvio del sistema operativo; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di analisi comportamentale; numero di eventi azione del sistema operativo del tipo corrente ritardati; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di difesa proattiva; numero di eventi azione del sistema operativo elaborati; numero di eventi azione del sistema operativo sincroni elaborati; ritardo totale di tutti gli eventi azione del sistema operativo del tipo corrente; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di archiviazione degli eventi persistenti; ritardo totale di tutti gli eventi azione del sistema operativo; numero di eventi azione del sistema operativo sincroni in attesa; data e ora dell'evento ricevuto di un'azione nel sistema operativo.

- Informazioni sull'ultimo riavvio non riuscito del sistema operativo: numero di riavvii non riusciti.

- Informazioni sull'applicazione installata dal Titolare dei diritti e sullo stato della protezione anti-virus: ID installazione Software (PCID); versione del record del database del Software; identificativo univoco dell'istanza di installazione dell'applicazione sul computer, tipo di applicazione, ID del tipo di applicazione, versione completa dell'applicazione installata, identificativo della versione delle impostazioni dell'applicazione, identificativo del tipo di computer, identificativo univoco del computer su cui è installata l'applicazione, identificativo univoco dell'Utente nei servizi del Titolare dei diritti, lingua locale e stato operativo, versione dei componenti del Software installato e relativo stato operativo, versione del protocollo utilizzato per connettersi ai servizi del Titolare dei diritti. versione completa del Software installato; tipo di software installato; ID aggiornamento Software; ID del servizio di reputazione; ID del tipo di protocollo; ID di un centro di attivazione regionale; versione dell'elenco delle decisioni del servizio Software revocato; ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record dei database anti-virus del Software attivati; ID univoco dell'istanza di installazione dell'applicazione nel computer; data di attivazione della licenza; data di scadenza della licenza; identificatore della licenza; stato della licenza utilizzata dal software; tipo di checksum per l'oggetto elaborato; nome del malware rilevato o del software legittimo che può essere utilizzato per danneggiare i dati o il dispositivo dell'utente; checksum dell'oggetto elaborato; checksum del codice di attivazione del Software; versione completa del software; ID Software; checksum del file chiave del Software; ID del modello di informazioni utilizzato per fornire la licenza Software; identificatore del certificato utilizzato per accedere all'intestazione del ticket della licenza Software; data e ora di creazione del ticket di licenza Software; checksum del ticket di licenza Software; versione del ticket di licenza Software; versione del codice di attivazione del Software; formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; ID ticket licenza corrente; ID componente Software; risultato dell'azione del Software; codice errore; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); numero di porta; indirizzo Web dell'origine della richiesta del servizio Web (Referrer); numero di cicli di applicazione degli aggiornamenti per i database anti-virus; data e ora dell'ultimo aggiornamento e dell'applicazione dei database anti-virus; data e ora di rilascio dei database del Software; versione del componente del Software; ID aggiornamento Software; tipo di software installato; data e ora di avvio di Controllo sistema; data e ora di installazione del Software; probabilità di invio statistiche da parte di Controllo sistema; codice dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; tempo di elaborazione del database dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; tempo massimo consentito per l'elaborazione di un evento da parte di Controllo sistema; tempo di elaborazione dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; numero totale di eventi che hanno richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema.

- Informazioni su tutti gli oggetti elaborati e sulle operazioni: verdetto del Software sull'oggetto elaborato; codice directory; dimensioni dell'oggetto elaborato; checksum (SHA256) dell'oggetto elaborato; numero del software rilevato nel contesto Controllo sistema; data e ora di rilevamento del software da parte di Controllo sistema; caratteristiche di rilevamento; ID del record attivato nei database anti-virus del Software; motivo del rilevamento del software da parte di Controllo sistema; checksum (MD5) dell'oggetto elaborato; risultato del controllo dell'integrità del modulo; nome dell'oggetto elaborato; tipo di record dei database anti-virus del Software attivati; percorso dell'oggetto elaborato; nome dell'oggetto esaminato; data e ora della scansione; URL e indirizzi Referrer da cui è stato scaricato; dimensioni dei file esaminati e dei relativi percorsi; segno dell'archivio; data e ora di creazione del file; nome, dimensioni e checksum (MD5, SHA2-256) dello strumento di creazione dei pacchetti (se il file è stato compresso); l'entropia del file; tipo di file; codice del tipo di file; formato, ID e segno del file eseguibile; checksum dell'oggetto (MD5, SHA2-256); tipo e il valore del checksum supplementare dell'oggetto; dati relativi alla firma digitale dell'oggetto (certificato): dati sull'entità di pubblicazione del certificato, numero di avvii dell'oggetto dall'ultimo invio di dati statistici, ID dell'attività di scansione dell'applicazione, modalità di ricezione delle informazioni sulla reputazione dell'oggetto, valore del filtro di destinazione, parametri tecnici delle tecnologie di rilevamento applicabili; percorso dell'oggetto elaborato; codice directory.

- Per i file eseguibili: entropia delle sezioni dei file, flag di verifica della reputazione o flag di firma del file, nome, tipo, ID, checksum (MD5) e dimensione dell'applicazione caricata dall'oggetto in fase di convalida, percorso dell'applicazione e percorsi del template, attributo indicante la presenza nell'elenco di esecuzione automatica, data di inserimento, elenco di attributi, nome dello strumento di creazione dei pacchetti, informazioni sulla firma digitale dell'applicazione: certificato dell'autore, nome del file caricato nel formato MIME, data e ora di compilazione del file.

- Informazioni sulle applicazioni avviate e sui rispettivi moduli: checksum (MD5, SHA2-256) dei file in esecuzione, dimensioni, attributi, data di creazione, nome dello strumento di creazione dei pacchetti (se il file è stato inserito in un pacchetto), nomi dei file, informazioni sui processi in esecuzione nel sistema (ID processo (PID), nome processo, informazioni sull'account da cui è stato avviato il processo, l'applicazione e il comando che hanno avviato il processo, percorso completo dei file del processo e riga di comando iniziale, descrizione dell'applicazione alla quale appartiene il processo (nome dell'applicazione e informazioni sull'autore), certificati digitali utilizzati e informazioni necessarie per verificarne l'autenticità o informazioni sull'assenza della firma digitale di un file), nonché informazioni sui moduli caricati nei processi: nome, dimensione, tipo, data di creazione, attributi, checksum (MD5, SHA2-256, SHA1), percorsi, informazioni sull'intestazione dei file PE, nomi degli strumenti di creazione dei pacchetti (se il file è stato inserito in un pacchetto), informazioni sulla disponibilità e la validità di queste statistiche e ID della modalità utilizzata per generare le statistiche inviate.

- Se vengono identificate minacce o vulnerabilità, oltre alle informazioni sull'oggetto rilevato verranno fornite informazioni sull'identificatore, sulla versione e sul tipo di record nel database anti-virus, il nome della minaccia in base alla classificazione Kaspersky, la data e l'ora dell'ultimo aggiornamento del database anti-virus, il nome del file eseguibile, il checksum (MD5) del file dell'applicazione che ha richiesto l'URL in cui è stata rilevata la minaccia, l'indirizzo IP (IPv4 o IPv6) della minaccia rilevata, l'identificatore della vulnerabilità e il livello della minaccia, l'URL e il Referrer della pagina Web in cui è stata rilevata la vulnerabilità.

- Se viene rilevato un oggetto potenzialmente dannoso, le relative informazioni sui dati vengono trasmesse nella memoria dei processi.

- Informazioni sugli attacchi di rete: indirizzo IP del computer da cui proviene l'attacco e numero della porta nel computer dell'utente interessata dall'attacco di rete, ID del protocollo di attacco, nome e tipo di attacco.

- Informazioni sulle connessioni di rete: la versione e i checksum (MD5, SHA2-256, SHA1) del file da cui il processo è stato avviato che ha aperto la porta, il percorso del file del processo e la sua firma digitale, gli indirizzi IP locale e remoto, i numeri delle porte di connessione locali e remote, lo stato di connessione, il timestamp dell'apertura della porta.

- L'URL e l'indirizzo IP della pagina web su cui è stato rilevato il contenuto dannoso o sospetto, il nome, la dimensione e il checksum del file che ha richiesto l'URL, il codice identificativo, il peso e il grado della regola impiegata per raggiungere il verdetto, l'oggetto dell'attacco.

- Informazioni sugli aggiornamenti dell'applicazione installata e dei database anti-virus: stato di completamento dell'attività di aggiornamento, tipo di errore che potrebbe essersi verificato durante il processo di aggiornamento, numero di aggiornamenti non riusciti e identificatore del componente dell'applicazione che esegue gli aggiornamenti.

- Informazioni sull'utilizzo di Kaspersky Security Network (KSN): identificatore KSN, identificatore dell'applicazione, versione completa dell'applicazione, indirizzo IP depersonalizzato del dispositivo dell'Utente, indicatori della qualità di adempimento delle richieste KSN, indicatori della qualità di elaborazione dei pacchetti KSN, indicatori del numero di richieste KSN e informazioni sui tipi di richieste KSN, data e ora di inizio e fine dell'invio delle statistiche; Informazioni sugli aggiornamenti della configurazione KSN: identificatore della configurazione attiva, identificatore della configurazione ricevuta, codice di errore dell'aggiornamento della configurazione.

- Informazioni sugli eventi del registro di sistema: ora dell'evento, nome del registro in cui è stato rilevato l'evento, tipo e categoria dell'evento, nome dell'origine dell'evento e descrizione dell'evento.

- Informazioni per determinare la reputazione dei file e gli indirizzi URL: l'indirizzo URL a cui si chiede la reputazione e il Referrer, il tipo di protocollo della connessione, l'ID interno del tipo di applicazione, il numero della porta in uso, l'ID Utente, il checksum del file analizzato (MD5), il tipo di minaccia rilevata e le informazioni sul registro utilizzato per rilevare una minaccia (l'identificatore del registro per il database anti-virus, il tipo e la marca temporale); chiave pubblica del certificato; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash.

- Dati sulla distribuzione territoriale dell'applicazione: data di installazione e attivazione dell'applicazione, ID del partner che fornisce la licenza per l'attivazione dell'applicazione, ID dell'applicazione, ID localizzazione lingua applicazione, numero di serie della licenza di attivazione dell'applicazione, indicazione di partecipazione a KSN.

- Informazioni sulla licenza utilizzata: tipo di licenza e relativo periodo di validità, numero di giorni restanti prima della scadenza della licenza, identificatore del partner dal quale la licenza è stata acquistata, identificatore del Centro regionale di attivazione, checksum del codice di attivazione, hash del corpo del ticket calcolato tramite l'algoritmo SHA1, data e ora di creazione del ticket di licenza, identificatore dei dati della licenza, identificatore del ticket della licenza, identificatore di sequenza del ticket della licenza, identificatore univoco del computer dell'utente, data di inizio validità del ticket della licenza, data di fine validità del ticket della licenza, stato corrente del ticket della licenza, versione intestazione ticket, versione della licenza, identificatore certificato di firma intestazione ticket, checksum del file chiave, numero di serie firmatario intestazione ticket, token di autenticazione.

- - Informazioni sull'hardware installato nel computer; tipo, nome, nome del modello, versione firmware, parametri dei dispositivi integrati e collegati.

- Informazioni su dispositivo: ID dispositivo.

- Informazioni sul funzionamento del componente Controllo Web: versione del componente, motivo della categorizzazione, informazioni aggiuntive sul motivo della categorizzazione, URL categorizzato, indirizzo IP host dell'oggetto bloccato/categorizzato.

Inoltre, al fine di raggiungere lo scopo dichiarato di aumentare l'efficacia della protezione fornita dall'applicazione, Kaspersky può ricevere oggetti utilizzabili da utenti malintenzionati per danneggiare il computer e creare minacce per la protezione delle informazioni. Questi oggetti sono:

- File eseguibili e non eseguibili o loro componenti

- Aree della memoria RAM del computer

- Settori interessati dal processo di avvio del sistema operativo

- Pacchetti di dati del traffico di rete

- Pagine Web ed e-mail contenenti oggetti dannosi o sospetti

- Descrizione delle classi e delle relative istanze per l'archiviazione WMI

- Rapporti sull'attività dell'applicazione

I rapporti sulle attività dell'applicazione contengono le seguenti informazioni su file e processi:

- Nome, dimensioni e versione del file inviato, relativa descrizione e checksum (MD5, SHA2-256, SHA1), ID formato, nome del produttore, nome dell'applicazione a cui appartiene il file, percorso completo del file nel computer e codice del modello di percorso, data e ora di creazione e aggiornamento del file.

- Data e ora di inizio e fine validità del certificato se il file inviato dispone di una firma digitale, data e ora in cui è stato firmato il certificato, nome dell'autorità di emissione del certificato, informazioni sul titolare del certificato, impressione e chiave pubblica del certificato e algoritmi utilizzati per calcolarli, numero di serie del certificato.

- Nome dell'account che aveva eseguito il processo.

- Checksum (MD5, SHA2-256, SHA1) relativi al nome del computer che esegue il processo.

- Intestazioni delle finestre del processo.

- ID per i database anti-virus, nome della minaccia identificata secondo la classificazione di Kaspersky.
- Informazioni sulla licenza utilizzata per l'applicazione, ID licenza, tipo e data di scadenza.
- Ora locale del computer al momento dell'invio delle informazioni.
- I nomi e i percorsi dei file a cui il processo ha avuto accesso.
- URL e indirizzi IP a cui il processo ha avuto accesso.
- URL e indirizzi IP da cui è stato scaricato il file in esecuzione.

Inoltre, per conseguire lo scopo dichiarato in merito alla prevenzione di falsi positivi, il Titolare dei diritti può ricevere file eseguibili o non eseguibili attendibili o relative parti.

Leggere l'Informativa sulla raccolta dei dati di KSN

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Avanzate** fare clic su **Mostra Informativa KSN**.

Kaspersky Endpoint Security salva le seguenti informazioni in un file di Traccia:

- Informazioni sul dispositivo e sul sistema operativo (ID univoco dispositivo, tipo di dispositivo, indirizzi MAC dei dispositivi di rete, tipo di sistema operativo, versione del sistema operativo).
- Informazioni sul funzionamento dell'applicazione e dei relativi moduli.
- Informazioni sull'abbonamento (tipo di abbonamento, area geografica).
- Informazioni sulle impostazioni locali della lingua, ID applicazione, personalizzazione applicazione, versione applicazione, ID installazione univoco dell'applicazione, ID univoco computer.
- Informazioni sullo stato della protezione anti-malware del computer, nonché su tutti gli oggetti rilevati ed elaborati (nome dell'oggetto rilevato, data e ora del rilevamento, indirizzo Web da cui è stato eseguito il download, nomi e dimensioni dei file infetti e relativi percorsi, indirizzo IP del computer che ha originato l'attacco e numero della porta del computer interessata dall'attacco di rete, elenco delle attività malware e indirizzi Web indesiderati) e le relative decisioni e azioni intraprese dall'applicazione e dall'utente.
- Informazioni sulle applicazioni scaricate dall'utente (indirizzo Web, attributi, dimensioni dei file e informazioni sul processo che ha scaricato il file).
- Informazioni sulle applicazioni avviate e sui moduli delle applicazioni (dimensioni, attributi, data di creazione, dettagli dell'intestazione PE, area geografica, nome, percorso e programmi di compressione).
- Informazioni sugli errori dell'interfaccia e sull'utilizzo dell'interfaccia dell'applicazione Kaspersky installata.
- Informazioni sulle connessioni di rete: l'indirizzo IP del computer remoto e del computer dell'utente, i numeri delle porte utilizzate per stabilire la connessione e il protocollo di rete della connessione.
- Informazioni sui pacchetti di rete ricevuti e inviati dal computer tramite le reti IT e di telecomunicazione.
- Informazioni sui messaggi e-mail e i messaggi istantanei inviati e ricevuti.

- Informazioni sugli indirizzi Web visitati: l'orario in cui è stata stabilita la connessione utilizzando un protocollo aperto, dati sul nome utente e la password per il sito Web e contenuto dei cookie.
- Certificato pubblico del server.

I file di traccia contengono solo le informazioni necessarie per risolvere gli errori dell'applicazione. Kaspersky utilizza i file di traccia per analizzare gli incidenti associati agli errori durante l'esecuzione dell'applicazione Kaspersky Endpoint Security.

Per impostazione predefinita, la creazione dei file di traccia è disabilitata. È possibile abilitare la generazione dei file di traccia nelle impostazioni dell'applicazione.

I file di traccia possono essere inviati solo manualmente a Kaspersky. L'applicazione non invia automaticamente i file di traccia a Kaspersky.

È possibile scegliere la modalità di invio dei file di traccia a Kaspersky.

Prima di inviare i file di traccia a Kaspersky, rivedere i dati che contengono.

Importante: i file di traccia possono contenere informazioni personali o sensibili. Inviando i file di traccia a Kaspersky, l'utente accetta di fornire a Kaspersky tutti i dati contenuti nei file di traccia inviati e accetta il metodo utilizzato per l'invio.

È inoltre possibile inviare a Kaspersky file o parti di file utilizzabili dagli intrusi per danneggiare il computer o i dati per un'ulteriore analisi.

Kaspersky protegge le informazioni ricevute in conformità alle leggi e alle regole applicabili di Kaspersky. I dati vengono trasmessi tramite un canale sicuro.

La partecipazione al programma Kaspersky Security Network è facoltativa. La decisione di partecipare viene presa dall'utente durante l'installazione dell'applicazione. Tuttavia, è possibile rivedere tale decisione in qualsiasi momento.

Attivare Kaspersky Endpoint Security

Importante: prima di attivare Kaspersky Endpoint Security, accertarsi che la data e l'ora impostate nel computer corrispondano alla data e ora effettive.

L'attivazione dell'applicazione implica l'aggiunta di una chiave all'applicazione.

Nota: per attivare l'applicazione è necessaria una connessione a Internet.

Attivare la versione di prova

1. Aprire la finestra principale dell'applicazione.
2. Nella barra laterale della finestra principale dell'applicazione fare clic su **Licenza**.

   Verrà visualizzata la finestra **Licenza**.
3. Nella finestra **Licenza** fare clic su **Attiva**.

Kaspersky Endpoint Security si connette ai server di attivazione di Kaspersky e invia i dati per la verifica. Se la verifica ha esito positivo, l'applicazione riceve e aggiunge una chiave per la versione di prova gratuita.

Importante: è possibile attivare una versione di prova di Kaspersky Endpoint Security solo se l'applicazione non è stata attivata in precedenza nel computer.

Attivare l'applicazione mediante il codice di attivazione

1. Aprire la finestra principale dell'applicazione.
2. Nella barra laterale della finestra principale dell'applicazione fare clic su **Licenza**.

   Verrà visualizzata la finestra **Licenza**.
3. Nella finestra **Licenza** inserire il codice di attivazione ricevuto al momento dell'acquisto di Kaspersky Endpoint Security.
4. Fare clic su **Attiva**.

   Nota: il codice di attivazione è una combinazione univoca di venti lettere e numeri dell'alfabeto latino nel formato xxxxx-xxxxx-xxxxx-xxxxx.

   L'applicazione si connette ai server di attivazione di Kaspersky e invia il codice di attivazione per verificarne l'autenticità. Se il codice di attivazione viene verificato correttamente, l'applicazione riceve e aggiunge automaticamente la chiave di licenza.

   Nota: a seconda del codice di attivazione ricevuto, può essere necessario compilare un modulo di registrazione.

   Se la verifica del codice di attivazione ha esito negativo, viene visualizzata una notifica. In questo caso, contattare il rivenditore del software che ha fornito il codice di attivazione.

In seguito all'attivazione dell'applicazione con il codice di attivazione, è possibile visualizzare le seguenti informazioni nella finestra **Licenza**:

- Stato della licenza o dell'abbonamento
- Chiavi attive
- Chiavi di riserva (se presenti)
- Tipo di licenza e numero di computer in cui è possibile utilizzare l'applicazione con la licenza corrente o con un abbonamento
- Funzionalità dell'applicazione disponibili con la licenza o l'abbonamento correnti
- Data e ora di scadenza della licenza
- Numero di giorni rimanenti prima della scadenza della licenza

Visualizzare le informazioni sulla licenza

Visualizzare le informazioni sulla licenza

1. Aprire la finestra principale dell'applicazione.
2. Nella barra laterale della finestra principale dell'applicazione fare clic su **Licenza**.

   Verrà visualizzata la finestra **Licenza**.

La finestra **Licenza** può contenere le seguenti informazioni:

- Stato della licenza o dell'abbonamento
- Chiavi attive
- Chiavi di riserva (se presenti)
- Tipo di licenza e numero di computer in cui è possibile utilizzare l'applicazione con la licenza corrente o con un abbonamento
- Funzionalità dell'applicazione disponibili con la licenza o l'abbonamento correnti
- Data e ora di scadenza della licenza
- Numero di giorni rimanenti prima della scadenza della licenza

Gestire licenze e abbonamenti

È necessario rinnovare la licenza se la licenza associata alla chiave attiva è scaduta e non è stata aggiunta una chiave di riserva. Allo scadere della licenza, l'applicazione continua a funzionare con funzionalità limitate (aggiornamenti, Kaspersky Security Network, Controllo Web e Criptaggio disco FileVault tramite Kaspersky Security Center diventano non disponibili). È ancora possibile utilizzare tutti i componenti dell'applicazione ed eseguire scansioni anti-malware, ma soltanto utilizzando i database anti-malware installati prima della scadenza della licenza.

Importante: se i database anti-malware sono obsoleti, il computer è soggetto a un rischio più elevato di infezioni.

Rinnovare una licenza

1. Nella barra laterale della finestra principale dell'applicazione, fare clic su **Centro protezione**.

   Viene aperta la finestra **Centro protezione**.
2. Nella finestra **Centro protezione** fare clic su **Rinnova**.

Verrà visualizzata una pagina Web con le informazioni sul rinnovo della licenza tramite il negozio online di Kaspersky o i partner Kaspersky. Quando si rinnova una licenza tramite un negozio online, un codice di attivazione per Kaspersky Endpoint Security viene inviato all'indirizzo e-mail specificato nel modulo d'ordine dopo l'esecuzione del pagamento.

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 rinnova l'abbonamento senza richiedere ulteriori azioni.

Se si utilizza l'applicazione con un abbonamento limitato e il periodo di tolleranza per rinnovare l'abbonamento è terminato, Kaspersky Endpoint Security invia una notifica all'utente e arresta i tentativi di rinnovo automatico dell'abbonamento e di aggiornamento dei database dell'applicazione.

È possibile rinnovare un abbonamento manualmente contattando il rivenditore presso il quale è stato acquistato Kaspersky Endpoint Security.

Rinnovare l'abbonamento

1. Aprire la finestra principale dell'applicazione.
2. Nella barra laterale della finestra principale dell'applicazione fare clic su **Licenza**.

   Verrà visualizzata la finestra **Licenza**.
3. Nella finestra **Licenza** visualizzata fare clic su **Visita il sito Web del provider del servizio**.

Si aprirà il sito web del provider di servizi.

Lo stato dell'abbonamento può diventare obsoleto. In questo caso, è necessario aggiornare manualmente lo stato dell'abbonamento. Se non si dispone di un abbonamento valido, Kaspersky Endpoint Security interrompe l'aggiornamento dei database dell'applicazione (se si dispone di un abbonamento per gli aggiornamenti) oppure interrompe la protezione del computer (se si dispone di un abbonamento per gli aggiornamenti e la protezione).

Aggiornare lo stato dell'abbonamento

1. Aprire la finestra principale dell'applicazione.
2. Nella barra laterale della finestra principale dell'applicazione fare clic su **Licenza**.

   Verrà visualizzata la finestra **Licenza**.
3. Nella finestra **Licenza** fare clic sul pulsante .

Confronto tra le funzionalità dell'applicazione a seconda del tipo di licenza per le workstation

Il set di funzionalità di Kaspersky Endpoint Security disponibili nelle workstation dipende dal tipo di licenza (vedere la tabella di seguito).

Funzionalità	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
Protezione Minacce Avanzata						
Kaspersky Security Network	✓	✓	✓	✓	✓	✓
Rilevamento del Comportamento	✓	✓	✓	✓	✓	✓
Prevenzione Exploit	✓	✓	✓	✓	✓	✓
Motore di Remediation	✓	✓	✓	✓	✓	✓
Protezione Minacce Essenziale						
Protezione Minacce File	✓	✓	✓	✓	✓	✓
Protezione Minacce Web	✓	✓	✓	✓	✓	✓
Protezione minacce di posta	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓
Protezione Minacce di Rete	✓	✓	✓	✓	✓	✓
Controlli di sicurezza						
Controllo dispositivi	✓	✓	✓	✓	✓	✓
Controllo Web	✓	✓	✓	✓	✓	✓
Criptaggio dei dati						
Criptaggio disco FileVault	–	✓	✓	✓	✓	✓
Detection and Response						
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓
Kaspersky Sandbox *(È necessario acquistare la licenza Kaspersky Sandbox separatamente)*	✓	✓	✓	✓	✓	✓

Esecuzione delle attività più comuni

Aprire e chiudere l'applicazione

Al termine dell'installazione, l'applicazione viene avviata automaticamente e l'icona dell'applicazione è visualizzata nella barra dei menu.

Aprire l'applicazione

Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Kaspersky Endpoint Security**.

Chiudere l'applicazione

Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Esci**.

Quando si chiude l'applicazione, il processo dell'applicazione viene rimosso dalla memoria del computer.

Importante: dopo la chiusura dell'applicazione Kaspersky Endpoint Security, il computer non sarà più protetto e potrebbe essere esposto a infezioni, comportando potenziali perdite di dati.

Visualizzare lo stato di protezione del computer

L'indicatore dello stato della protezione informa in merito a problemi con la protezione del computer. Questo indicatore ha la forma di uno scudo e si trova nella finestra principale dell'applicazione. Il colore dell'indicatore può cambiare a seconda dello stato della protezione del computer. Se Kaspersky Endpoint Security rileva minacce per la sicurezza, viene visualizzato un messaggio relativo alle minacce nella finestra principale dell'applicazione e cambia il colore dell'indicatore.

Il colore dell'indicatore può cambiare nei modi seguenti:

- **Verde**. Il computer è protetto in modo ottimale.

  L'indicatore di colore verde indica che i database anti-malware sono aggiornati e che tutti i componenti dell'applicazione sono stati configurati come consigliato da Kaspersky. Non sono stati rilevati oggetti dannosi oppure gli oggetti dannosi rilevati sono stati neutralizzati.

- **Giallo**. Il livello di protezione del computer è ridotto.

  L'indicatore giallo indica che Kaspersky Endpoint Security è al corrente dell'esistenza di un problema. Tali problemi includono lievi variazioni rispetto alle impostazioni di protezione consigliate o database dell'applicazione non aggiornati.

- **Rosso**. Il computer è a rischio di infezione.

  L'indicatore di colore rosso indica che sono presenti problemi pericolosi che possono provocare infezioni del computer o perdite di dati. Ad esempio, i database anti-malware dell'applicazione sono estremamente obsoleti, l'applicazione non è stata attivata oppure sono stati rilevati oggetti dannosi.

  È consigliabile correggere i problemi e gestire le minacce per la sicurezza il prima possibile.

Visualizzare lo stato operativo dei componenti installati

Kaspersky Endpoint Security consente di controllare lo stato dei componenti dell'applicazione installati nella finestra **Sicurezza**. L'indicatore accanto al nome di ogni componente ne riflette lo stato.

Visualizza lo stato del componente

1. Aprire la finestra principale dell'applicazione.
2. Nella barra laterale della finestra principale dell'applicazione fare clic su **Sicurezza**.

   Verrà visualizzata la finestra **Sicurezza**.

Possono essere visualizzati i seguenti indicatori di stato:

	Il componente è in esecuzione.
	Il componente è in esecuzione e gestito da un criterio di sicurezza.
	Il componente ha subito un malfunzionamento.
	Il componente ha subito un malfunzionamento ed è gestito da un criterio di sicurezza.
	Il componente è spento.
	Il componente viene disattivato e gestito da un criterio di sicurezza.
	Il componente è in pausa.
	Il componente non è supportato dalla licenza corrente.

Nota: per alcuni componenti è anche possibile utilizzare il menu con 3 puntini accanto al nome del componente per aprire un rapporto o configurare le impostazioni del componente.

Disabilitare e ripristinare la protezione del computer

Per impostazione predefinita, Kaspersky Endpoint Security viene avviato in seguito all'avvio del sistema operativo e protegge il computer fino allo spegnimento. Tutti i componenti di protezione (Protezione Minacce File, Protezione Minacce Web e Protezione Minacce di Rete) sono abilitati e in esecuzione.

È possibile disabilitare completamente la protezione o disabilitare componenti della protezione specifici.

Importante: Kaspersky consiglia vivamente di non disabilitare la protezione o i componenti di protezione in quanto questo potrebbe provocare infezioni del computer o perdite di dati.

Quando la protezione del computer è disabilitata:

- L'icona dell'applicazione nella barra dei menu è inattiva.
- L'indicatore dello stato della protezione nella finestra principale dell'applicazione è rosso.

Quando uno o più di componenti della protezione sono disabilitati, l'indicatore dello stato della protezione è rosso o giallo.

Nota: la disabilitazione o la sospensione di questi componenti di protezione non ha effetti sulle attività di scansione o sull'attività di aggiornamento.

È possibile disabilitare o ripristinare la protezione del computer in uno dei seguenti modi:

- Dall'icona dell'applicazione
- Dalla finestra delle impostazioni dell'applicazione
- Dal menu **Protezione**

Disabilitare o ripristinare la protezione del computer dall'icona dell'applicazione

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Disattiva protezione/Attiva protezione**.

   Quando si disattiva la protezione, viene visualizzata la richiesta delle credenziali di amministratore.

2. Quando vengono richieste le credenziali di amministratore, immettere il nome e la password dell'amministratore e confermare che si desidera disattivare la protezione.

Disabilitazione o ripristino della protezione del computer dalla finestra delle impostazioni dell'applicazione

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale**, nella sezione **Generale**, deselezionare o selezionare la casella di controllo **Abilita la protezione**.

Disabilitare o ripristinare la protezione del computer dalla barra dei menu

Nella barra dei menu fare clic su **Protezione** > **Disattiva protezione/Attiva protezione**.

Importante: se si disabilita la protezione del computer, non verrà riabilitata automaticamente al riavvio di Kaspersky Endpoint Security. È necessario riabilitare il componente di protezione manualmente.

Disabilitazione di un componente di protezione

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale**, nella sezione **<nome del componente>**, deselezionare la casella di controllo **Abilita <nome del componente>**.

Importante: se un componente di protezione è stato disabilitato, non verrà riabilitato automaticamente al riavvio di Kaspersky Endpoint Security. È necessario riabilitare il componente di protezione manualmente.

Abilitazione di un componente di protezione

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale**, nella sezione **<nome del componente>**, selezionare la casella di controllo **Abilita <nome del componente>**.

Per abilitare la protezione del computer o i componenti della protezione, è inoltre possibile utilizzare Centro protezione. Disabilitando la protezione del computer o i componenti di protezione, il computer è soggetto a un rischio molto più elevato di infezione. Per questo motivo Centro protezione informa l'utente quando la protezione del computer viene disabilitata.

Utilizzare Centro protezione

Centro protezione è una funzionalità di Kaspersky Endpoint Security che consente di analizzare e correggere i problemi e le minacce per la protezione del computer.

Aprire Centro protezione

Nella barra laterale della finestra principale dell'applicazione, fare clic su **Centro protezione**.

In Centro protezione è possibile trovare informazioni sulle minacce attive, visualizzare lo stato dei database dell'applicazione e verificare se la protezione di qualche componente è disabilitata.

Nota: se l'amministratore di sistema dell'organizzazione abilita Controllo Web per bloccare l'accesso alle risorse Web pericolose, Kaspersky Endpoint Security visualizza la notifica **Controllo Web abilitato** in Centro protezione.

Per ogni problema o minaccia Kaspersky Endpoint Security suggerisce le azioni che è possibile eseguire per risolvere il problema o la minaccia. Ad esempio, se Kaspersky Endpoint Security rileva file infetti nel computer, è possibile fare clic su **Disinfetta**. Se i database anti-malware sono obsoleti, è possibile fare clic su **Aggiorna**. È possibile correggere un problema o neutralizzare una minaccia immediatamente o in un secondo momento.

Correggere un problema o neutralizzare una minaccia immediatamente

Fare clic sul pulsante con il nome di un'azione consigliata per correggere il problema o neutralizzare la minaccia.

L'applicazione esegue l'azione selezionata.

Se si chiude Centro protezione senza neutralizzare le minacce pericolose, l'indicatore dello stato della protezione nella finestra principale dell'applicazione rimane rosso per ricordare la presenza di tali minacce.

Eseguire attività di scansione

L'attività Scansione completa predefinita è inclusa in Kaspersky Endpoint Security. Durante l'esecuzione dell'attività, l'applicazione esamina la memoria, gli oggetti di avvio e tutte le unità interne del computer per rilevare la presenza di virus e altro malware.

Eseguire una scansione completa del computer

1. Nella barra laterale della finestra principale dell'applicazione, fare clic su **Scansione**.

   Verrà visualizzata la finestra **Scansione**.

2. Fare clic sul pulsante **Scansione completa**.

Verrà avviata una scansione completa del computer.

L'attività Scansione rapida predefinita è inclusa in Kaspersky Endpoint Security. Durante l'esecuzione dell'attività, l'applicazione esamina le aree critiche del computer (la memoria, gli oggetti di avvio e le cartelle di sistema) per rilevare la presenza di virus e altro malware.

Eseguire una scansione rapida del computer

1. Nella barra laterale della finestra principale dell'applicazione, fare clic su **Scansione**.

   Verrà visualizzata la finestra **Scansione**.

2. Fare clic sul pulsante **Scansione rapida**.

Verrà avviata una scansione rapida del computer.

Per esaminare un singolo oggetto (come un disco interno, una cartella, un file o un disco rimovibile) per rilevare la presenza di virus e altro malware, è possibile eseguire l'attività Scansione personalizzata.

Esaminare un elemento selezionato

Eseguire una delle seguenti operazioni:

- Fare clic con il pulsante destro del mouse su un elemento selezionato e scegliere **Ricerca malware**.
- Trascinare un elemento selezionato sull'icona dell'applicazione nel Dock.
- Trascinare un elemento selezionato nella finestra **Scansione**.

È possibile visualizzare i risultati delle attività di scansione completate nella finestra **Rapporti**.

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Configurare l'avvio automatico di un'attività di scansione pianificata

È possibile creare una pianificazione per l'avvio delle attività di Scansione rapida e Scansione completa. Kaspersky Endpoint Security esamina automaticamente l'intero computer o le aree specificate del computer in conformità con la pianificazione configurata.

Pianificare un'attività di scansione dalla finestra Scansione

1. Nella barra laterale della finestra principale dell'applicazione, fare clic su **Scansione**.

   Verrà visualizzata la finestra **Scansione**.

2. Fare clic su **Pianifica scansione**.

   Verrà visualizzata una finestra di dialogo in cui è possibile impostare la pianificazione.

3. Selezionare la casella di controllo **Scansione completa** o **Scansione rapida**.

4. Specificare la frequenza di scansione e l'ora di avvio della scansione.

5. Fare clic su **OK**.

Pianificare un'attività di scansione dalla finestra Impostazioni

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Scansione** fare clic su **Pianifica**.

3. Nella finestra visualizzata selezionare la casella di controllo accanto al nome dell'attività di scansione che si desidera avviare in base a una pianificazione.

4. Configurare l'ora e la frequenza dell'attività di scansione.

5. Fare clic su **OK** per salvare le modifiche apportate alla pianificazione dell'attività di scansione.

È possibile visualizzare i risultati dell'attività di scansione nella finestra **Rapporti**.

Aggiornare i database dell'applicazione

La principale sorgente degli aggiornamenti per Kaspersky Endpoint Security sono i server degli aggiornamenti dedicati di Kaspersky. Kaspersky Endpoint Security può inoltre utilizzare i punti di distribuzione, le cartelle locali o altri server Web come *sorgente degli aggiornamenti*.

Nota: per scaricare gli aggiornamenti disponibili dai server degli aggiornamenti è necessario disporre di una connessione Internet.

Per impostazione predefinita, Kaspersky Endpoint Security controlla periodicamente la presenza di aggiornamenti sui server degli aggiornamenti di Kaspersky. Se su un server sono disponibili nuovi aggiornamenti, Kaspersky Endpoint Security ne esegue il download in background e li installa nel computer.

Avviare un aggiornamento di Kaspersky Endpoint Security

1. Nella barra laterale della finestra principale dell'applicazione fare clic su **Aggiornamento**.

   Verrà visualizzata la finestra **Aggiornamento**.

2. Fare clic su **Aggiorna**.

L'applicazione verifica la disponibilità di aggiornamenti. Se sono disponibili aggiornamenti, l'applicazione li scarica e li installa nel computer.

È inoltre possibile avviare un'attività di aggiornamento in uno dei seguenti modi:

- Fare clic sull'icona dell'applicazione e scegliere **Aggiornamento**.
- Nella barra dei menu scegliere **Protezione** > **Aggiornamento**.

È possibile modificare il modo in cui Kaspersky Endpoint Security aggiorna i database delle applicazioni. Per impostazione predefinita, l'applicazione aggiorna automaticamente i database.

Abilitare/disabilitare i download automatici degli aggiornamenti dei database di Kaspersky Endpoint Security

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Aggiornamento**, nella sezione **Database**, selezionare o deselezionare la casella di controllo **Scarica gli aggiornamenti automaticamente**.

È possibile visualizzare i risultati delle attività di aggiornamento completate nella finestra **Rapporti**.

Nota: Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Come procedere se l'accesso al file è bloccato

L'applicazione Kaspersky Endpoint Security blocca l'accesso alle applicazioni e ai file infetti. Se un file è infetto, deve essere disinfettato prima di potervi accedere.

Disinfettare un oggetto rilevato

1. Nella barra dei menu scegliere **Protezione** > **Oggetti rilevati**.

   Verrà visualizzata la finestra **Oggetti rilevati**.

2. Nella sezione **Oggetti rilevati** fare clic su ••• accanto al file desiderato e scegliere **Disinfetta**.

   L'applicazione inizia a disinfettare l'oggetto selezionato. Durante la disinfezione, viene visualizzata una finestra di dialogo in cui è possibile selezionare l'azione da eseguire sull'oggetto.

Disinfettare tutti gli oggetti rilevati

1. Nella barra dei menu scegliere **Protezione** > **Oggetti rilevati**.

   Verrà visualizzata la finestra **Oggetti rilevati**.

2. Nella sezione **Oggetti rilevati** fare clic su **Disinfetta tutto**.

   L'applicazione inizia a disinfettare gli oggetti rilevati. Durante la disinfezione, viene visualizzata una finestra di dialogo in cui è possibile selezionare l'azione da eseguire sull'oggetto. Se si seleziona la casella di controllo **Applica a tutti** nella finestra di notifica dopo aver selezionato l'azione, tale azione verrà applicata a tutti i file del tipo specificato.

Se si è certi che i file bloccati da Protezione Minacce File sono sicuri, è possibile includerli nell'Area attendibile.

Ripristino di un file eliminato o disinfettato dall'applicazione

Talvolta non è possibile salvare i file nella loro interezza durante il processo di disinfezione. Se un file disinfettato conteneva informazioni importanti che risultano in parte o del tutto inaccessibili dopo la disinfezione, è possibile tentare di ripristinare il file originale dalla relativa copia di backup.

Ripristinare un file eliminato o modificato dall'applicazione durante la disinfezione

1. Nella barra dei menu scegliere **Protezione** > **Oggetti rilevati**.

   Verrà visualizzata la finestra **Oggetti rilevati**.

2. Nella sezione **Backup** fare clic su ••• accanto al file che si desidera ripristinare.

   Verrà visualizzato il menu pop-up.

3. Scegliere **Ripristina file**.

   Si aprirà una finestra in cui specificare il nome del file, il tag e la cartella in cui verrà ripristinato il file. Per impostazione predefinita, sono già specificati il nome del file e la posizione originali.

4. Specificare il nome del file e la cartella in cui verrà ripristinato il file.

5. Fare clic su **Salva**.

L'applicazione ripristina il file nel percorso specificato e con il nome specificato.

È necessario sottoporre il file a una scansione anti-malware subito dopo averlo ripristinato. È possibile che l'oggetto venga disinfettato utilizzando i database aggiornati senza essere danneggiato.

Importante: non è consigliabile ripristinare le copie di backup dei file a meno che non sia assolutamente necessario, poiché il ripristino potrebbe esporre il computer al rischio di infezione.

Visualizzare il rapporto sul funzionamento dell'applicazione

È possibile visualizzare un rapporto di Kaspersky Endpoint Security in cui sono elencati tutti gli oggetti rilevati nella scheda **Oggetti elaborati**. Gli eventi di sistema vengono visualizzati nella scheda **Eventi di sistema**. In aggiunta, viene creato un altro rapporto dettagliato distinto per ciascuno dei seguenti componenti dell'applicazione: Protezione Minacce File, Protezione Minacce Web, Protezione Minacce di Rete, Rilevamento del Comportamento e le attività di scansione e aggiornamento.

Aprire la finestra Rapporti

Nella barra dei menu scegliere **Protezione** > **Rapporti**.

Come procedere se vengono visualizzate finestre di notifica

Le notifiche dell'applicazione, sotto forma di finestre di notifica, informano di eventi dell'applicazione che richiedono l'attenzione dell'utente.

Se viene visualizzata una notifica, selezionare una delle opzioni suggerite. L'opzione ottimale è quella impostata come predefinita dagli specialisti di Kaspersky.

Configurazione avanzata dell'applicazione

Ambito di protezione del computer

Gli oggetti rilevati da Kaspersky Endpoint Security sono suddivisi in categorie in base a vari attributi. L'applicazione esegue sempre la ricerca di virus, worm, Trojan e strumenti dannosi. Questi programmi possono causare danni significativi al computer. Per migliorare l'affidabilità della protezione del computer, è possibile estendere l'elenco degli oggetti rilevabili consentendo all'applicazione di verificare la presenza di software legittimo utilizzabile da un utente malintenzionato per danneggiare il computer o i dati personali.

Gli oggetti contro cui Kaspersky Endpoint Security garantisce protezione sono raggruppati come segue:

- **Virus, worm, Trojan, strumenti dannosi, adware e auto-dialer**.

  Questa categoria include:

  - Tutti i tipi di malware.
  - Software che può disturbare mostrando pubblicità (ad esempio banner) nel computer o sostituendo i risultati di ricerca nel browser con siti Web pubblicitari.
  - Applicazioni che stabiliscono connessioni telefoniche nascoste tramite un modem del computer.

  La protezione da tutti i tipi di malware è il livello minimo di sicurezza necessario. In base alle raccomandazioni degli esperti di Kaspersky, Kaspersky Endpoint Security esegue sempre il monitoraggio degli oggetti appartenenti a questa categoria.

- **Software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali dell'utente**. Questa categoria include il software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali, ad esempio le applicazioni di amministrazione remota.

Selezionare le categorie di oggetti da rilevare

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Oggetti da rilevare** della scheda **Minacce** selezionare le caselle relative alle categorie di oggetti da rilevare.

   Nota: Kaspersky Endpoint Security protegge sempre il computer da virus, worm, Trojan, strumenti dannosi, adware e Auto-dialer. Di conseguenza, non è possibile deselezionare la casella di controllo per questa categoria.

A seconda delle categorie di oggetti da rilevare selezionate, Kaspersky Endpoint Security utilizzerà i database anti-malware in parte o per intero durante l'esecuzione di Protezione Minacce File, Protezione Minacce Web e delle attività di scansione.

Nota: se Kaspersky Endpoint Security classifica un'applicazione come malware ma l'utente la considera innocua, è possibile aggiungere questa applicazione all'Area attendibile.

L'*area attendibile* è un elenco di oggetti che Kaspersky Endpoint Security non sottopone a scansione o monitoraggio. Può essere necessario aggiungere oggetti all'area attendibile se, ad esempio, Kaspersky Endpoint Security blocca l'accesso a un file, a un'applicazione o a un sito Web, benché si abbia la certezza assoluta che l'oggetto, l'applicazione o l'indirizzo Web non ponga alcun problema di protezione.

Quando un'applicazione viene aggiunta all'area attendibile, il relativo file e le attività di rete (incluse quelle sospette) non vengono più monitorati. Tuttavia, Kaspersky Endpoint Security continua a esaminare il file eseguibile e l'elaborazione dell'applicazione attendibile.

Nota: Quando un amministratore configura il criterio per proibire la modifica dell'Area attendibile, gli utenti non possono accedere alle impostazioni dell'Area attendibile.

Aggiungere o rimuovere un file o una cartella a o da un elenco di file e cartelle attendibili

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Esclusioni** della scheda **Minacce** fare clic su **Area attendibile**.

   Verrà visualizzata la finestra delle impostazioni dell'area attendibile.

3. Nella scheda **File e cartelle** modificare l'elenco di file e cartelle attendibili:

   - Per aggiungere un file o una cartella all'elenco:

     a. Fare clic su +.

     Verrà visualizzata una finestra di dialogo in cui è possibile selezionare un file o una cartella.

     b. Selezionare un file o una cartella che si desidera aggiungere.

     c. Fare clic su **Apri**.

   - Per rimuovere un file o una cartella dall'elenco:

     a. Selezionare un file o una cartella che si desidera rimuovere dall'elenco di file e cartelle attendibili.

     b. Fare clic su –.

4. Fare clic su **OK**.

Aggiungere o rimuovere un indirizzo Web attendibile all'elenco o dall'elenco di indirizzi Web attendibili

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Esclusioni** della scheda **Minacce** fare clic su **Area attendibile**.

   Verrà visualizzata la finestra delle impostazioni dell'area attendibile.

   È inoltre possibile aprire questa finestra facendo clic sul pulsante **Area attendibile** nella sezione **Generale** della scheda **Essenziale**.

3. Nella scheda **Indirizzi Web** modificare l'elenco di indirizzi Web attendibili:

   - Per aggiungere un indirizzo Web all'elenco:

     a. Fare clic su +.

     b. Immettere l'indirizzo Web che si desidera aggiungere all'elenco.

     c. Fare clic su **OK**.

   - Per rimuovere un indirizzo Web dall'elenco:

     a. Selezionare un indirizzo Web che si desidera rimuovere.

     b. Fare clic su –.

4. Fare clic su **OK**.

Per impostazione predefinita, l'elenco degli indirizzi Web attendibili è vuoto.

Aggiungere o rimuovere un'applicazione attendibile all'elenco o dalle applicazioni attendibili

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Esclusioni** della scheda **Minacce** fare clic su **Area attendibile**.

   Verrà visualizzata la finestra delle impostazioni dell'area attendibile.

   È inoltre possibile aprire questa finestra facendo clic sul pulsante **Area attendibile** nella sezione **Generale** della scheda **Essenziale**.

3. Nella scheda **Applicazioni attendibili** modificare l'elenco delle applicazioni attendibili:

   - Per aggiungere un'applicazione all'elenco:

     a. Fare clic su +.

     Viene aperta una finestra in cui è possibile specificare i parametri dell'applicazione richiesta.

     b. Specificare i seguenti parametri dell'applicazione che si desidera aggiungere:

     - **Percorso**
     - **Requisito di firma del codice**

     Nota: è possibile immettere i valori di questi due parametri manualmente o fare clic sul pulsante **Seleziona** e selezionare l'applicazione che si desidera aggiungere nella finestra visualizzata. In questo caso i valori di questi parametri verranno inseriti automaticamente.

c. Nella sezione **Opzioni** selezionare almeno un tipo di attività che non si desidera venga monitorato dall'applicazione Kaspersky Endpoint Security:

- **Non monitorare l'attività del file**
- **Non monitorare l'attività di rete**

d. Fare clic su **OK**.

- Per rimuovere un'applicazione dall'elenco:

a. Selezionare un'applicazione che si desidera rimuovere.

b. Fare clic su –.

Per impostazione predefinita, l'elenco delle applicazioni attendibili è vuoto.

Modificare un'applicazione attendibile

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Esclusioni** della scheda **Minacce** fare clic su **Area attendibile**.

   Verrà visualizzata la finestra delle impostazioni dell'area attendibile.

   È inoltre possibile aprire questa finestra facendo clic sul pulsante **Area attendibile** nella sezione **Generale** della scheda **Essenziale**.

3. Nella scheda **Applicazioni attendibili** selezionare un'applicazione che si desidera modificare.

4. Fare clic su **Modifica**.

5. Nella finestra visualizzata modificare i parametri dell'applicazione:

6. Fare clic su **OK**.

Abilitare il monitoraggio di un indirizzo Web attendibile

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Esclusioni** della scheda **Minacce** fare clic su **Area attendibile**.

   Verrà visualizzata la finestra delle impostazioni dell'area attendibile.

3. Nella scheda **Indirizzi Web** deselezionare la casella relativa a un indirizzo Web che deve essere monitorato dall'applicazione Kaspersky Endpoint Security.

4. Fare clic su **OK**.

Protezione Minacce File

Protezione Minacce File impedisce l'infezione del file system del computer. Il componente viene avviato durante l'avvio del sistema operativo, rimane nella memoria del computer ed esamina tutti i file aperti, salvati o eseguiti nel computer e in tutti i dischi connessi alla ricerca di malware. Se si disabilita Protezione Minacce File, non verrà avviato all'avvio del sistema operativo. Sarà necessario riabilitare Protezione Minacce File manualmente.

Abilitare o disabilitare Protezione Minacce File

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale**, nella sezione **Protezione minacce file**, selezionare o deselezionare la casella di controllo **Abilita Protezione minacce file**.

   È anche possibile abilitare Protezione Minacce File in Centro protezione. Disabilitando la protezione del computer o i componenti di protezione, il computer è soggetto a un rischio molto più elevato di infezione. Per questo motivo Centro protezione informa l'utente quando la protezione del computer viene disabilitata.

È possibile creare un ambito di protezione per Protezione Minacce File.

Aggiungere o rimuovere un file o una cartella all'ambito di protezione o dall'ambito di protezione

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Protezione minacce file** della scheda **Essenziale** fare clic su **Ambito della protezione**.

   Verrà aperta una finestra con un elenco di oggetti esaminati da Protezione Minacce File. Per impostazione predefinita, Protezione Minacce File esamina tutti gli oggetti archiviati su dischi interni, nei dischi di rete e nei supporti rimovibili collegati al computer.

   Nota: è possibile ignorare la scansione del volume di sistema di sola lettura per ridurre in modo significativo i tempi di scansione. Per impostazione predefinita, Protezione Minacce File non esamina il volume di sistema di sola lettura.

3. Nella sezione **Ambito della protezione** aggiungere/rimuovere gli oggetti a/dall'ambito di protezione:

   - Per aggiungere un file o una cartella all'ambito di protezione:

     a. Fare clic su +.

     Verrà visualizzato un menu pop-up in cui è possibile selezionare gli oggetti da aggiungere all'ambito della protezione.

     b. Nel menu pop-up selezionare la voce **File e cartelle**.

     Verrà visualizzata una finestra di dialogo in cui è possibile selezionare un file o una cartella.

     c. Selezionare un file o una cartella da aggiungere all'ambito di protezione.

     d. Fare clic su **Apri**.

   - Per rimuovere un file o una cartella dall'ambito di protezione:

     a. Selezionare un oggetto nell'elenco di oggetti dell'ambito di protezione.

     b. Trascinare l'oggetto selezionato dalla finestra oppure fare clic su –.

4. Se si desidera esaminare il volume di sistema di sola lettura, nella sezione **Ottimizzazione** deselezionare la casella di controllo **Ignora la scansione del volume di sistema di sola lettura**.

   Importante: l'ottimizzazione potrebbe essere disabilitata per motivi di sicurezza.

5. Fare clic su **Salva**.

Aggiungere o rimuovere un oggetto nell'elenco degli oggetti predefiniti nell'ambito della protezione

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Protezione minacce file** della scheda **Essenziale** fare clic su **Ambito della protezione**.

   Verrà aperta una finestra con un elenco di oggetti esaminati da Protezione Minacce File. Per impostazione predefinita, Protezione Minacce File esamina tutti gli oggetti archiviati su dischi interni, nei dischi di rete e nei supporti rimovibili collegati al computer.

   Nota: è possibile ignorare la scansione del volume di sistema di sola lettura per ridurre in modo significativo i tempi di scansione. Per impostazione predefinita, Protezione Minacce File non esamina il volume di sistema di sola lettura.

3. Nella sezione **Ambito della protezione** aggiungere/rimuovere gli oggetti nell'elenco degli oggetti predefiniti a o dall'ambito di protezione:

   - Per aggiungere un oggetto nell'elenco degli oggetti predefiniti all'ambito di protezione:

     a. Fare clic su +.

     Verrà visualizzato un menu pop-up in cui è possibile selezionare gli oggetti da aggiungere all'ambito della protezione.

     b. Nel menu pop-up selezionare un oggetto da aggiungere all'ambito della protezione (ad esempio **Tutti i dischi interni)**.

   - Per rimuovere un oggetto nell'elenco degli oggetti predefiniti dall'ambito di protezione:

     a. Selezionare un oggetto nell'elenco di oggetti dell'ambito di protezione.

     b. Trascinare l'oggetto selezionato dalla finestra oppure fare clic su –.

4. Se si desidera esaminare il volume di sistema di sola lettura, nella sezione **Ottimizzazione** deselezionare la casella di controllo **Ignora la scansione del volume di sistema di sola lettura**.

   Importante: l'ottimizzazione potrebbe essere disabilitata per motivi di sicurezza.

5. Fare clic su **Salva**.

Disabilitare la protezione di un oggetto nell'ambito di protezione

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Protezione minacce file** della scheda **Essenziale** fare clic su **Ambito della protezione**.

   Verrà aperta una finestra con un elenco di oggetti esaminati da Protezione Minacce File. Per impostazione predefinita, Protezione Minacce File esamina tutti gli oggetti archiviati su dischi interni, nei dischi di rete e nei supporti rimovibili collegati al computer.

   Nota: è possibile ignorare la scansione del volume di sistema di sola lettura per ridurre in modo significativo i tempi di scansione. Per impostazione predefinita, Protezione Minacce File non esamina il volume di sistema di sola lettura.

3. Deselezionare la casella relativa a un oggetto nell'elenco di oggetti dell'ambito di protezione.

4. Fare clic su **Salva**.

Abilitare la scansione del volume di attività di sola lettura

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Protezione minacce file** della scheda **Essenziale** fare clic su **Ambito della protezione**.

   Verrà aperta una finestra con un elenco di oggetti esaminati da Protezione Minacce File. Per impostazione predefinita, Protezione Minacce File esamina tutti gli oggetti archiviati su dischi interni, nei dischi di rete e nei supporti rimovibili collegati al computer.

   Nota: è possibile ignorare la scansione del volume di sistema di sola lettura per ridurre in modo significativo i tempi di scansione. Per impostazione predefinita, Protezione Minacce File non esamina il volume di sistema di sola lettura.

3. Nella sezione **Ottimizzazione** deselezionare la casella di controllo **Ignora la scansione del volume di sistema di sola lettura**.

   Importante: l'ottimizzazione potrebbe essere disabilitata per motivi di sicurezza.

4. Fare clic su **Salva**.

Quando l'utente o un'applicazione tenta di accedere a un file incluso nell'ambito della protezione, Protezione Minacce File verifica se i database di iSwift contengono informazioni su tale file e utilizza le informazioni per decidere se esaminare il file.

Il riconoscimento degli oggetti dannosi è possibile mediante l'*analisi delle firme*, una modalità di ricerca delle minacce basata sulle descrizioni delle minacce incluse nei database anti-malware. Oltre all'analisi delle firme, Protezione Minacce File utilizza l'analisi euristica e altre tecnologie di scansione.

Se in un file viene rilevata una minaccia, Kaspersky Endpoint Security identifica il tipo di malware rilevato (ad esempio *virus* o *Trojan*). Successivamente, l'applicazione visualizza una notifica sull'oggetto rilevato ed esegue l'azione sull'oggetto in base alle impostazioni di Protezione Minacce File.

Selezionare l'azione eseguita da Protezione Minacce File in caso di rilevamento di un file infetto

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Protezione minacce file** della scheda **Essenziale** selezionare l'azione eseguita da Protezione Minacce File in seguito al rilevamento di un file infetto.

Prima di provare a disinfettare o eliminare un file infetto, Kaspersky Endpoint Security ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento.

Le informazioni relative all'esecuzione di Protezione Minacce File e a tutti gli oggetti rilevati vengono registrate in un rapporto.

Nota: se l'esecuzione di Protezione Minacce File viene interrotta con un errore, è possibile visualizzare il rapporto e tentare di riavviare il componente. Se il problema persiste, è possibile contattare l'Assistenza tecnica di Kaspersky.

Visualizzare il rapporto di Protezione Minacce File

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.

   Verrà visualizzata la finestra **Rapporti**.

2. Aprire la scheda **Protezione minacce file**.

Protezione Minacce Web

Durante l'utilizzo di Internet, il computer è a rischio di infezione da parte di malware e altre minacce per la sicurezza. Le minacce per la sicurezza del computer possono penetrare nel computer durante il download di programmi gratuiti o l'esplorazione di siti Web che hanno subito l'attacco di hacker. Inoltre, i worm di rete possono attaccare il computer dell'utente non appena viene stabilita una connessione Internet, anche prima dell'apertura di un indirizzo Web o del download di un file.

Kaspersky Endpoint Security protegge le informazioni che il computer invia e riceve tramite i protocolli HTTP e HTTPS in Safari, Chrome o Firefox.

Nota: Kaspersky Endpoint Security monitora il traffico Web nelle porte utilizzate più di frequente per il trasferimento di dati HTTP e HTTPS. Kaspersky Endpoint Security esegue la scansione delle connessioni criptate (HTTPS) solo se è selezionata la casella di controllo **Controlla connessioni protette (HTTPS)** nella sezione **Generale**.

Abilitare o disabilitare Protezione Minacce Web

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale**, nella sezione **Protezione minacce Web**, selezionare o deselezionare la casella di controllo **Abilita Protezione minacce Web**.

È anche possibile abilitare Protezione Minacce Web tramite Centro protezione. Disabilitando la protezione del computer o i componenti di protezione, il computer è soggetto a un rischio molto più elevato di infezione. Per questo motivo Centro protezione informa l'utente quando la protezione del computer viene disabilitata.

Importante: se è stato disabilitato Protezione Minacce Web, il componente non verrà riabilitato automaticamente al riavvio di Kaspersky Endpoint Security o del sistema operativo. È necessario riabilitare Protezione Minacce Web manualmente.

Protezione Minacce Web esamina il traffico Web in base alle impostazioni consigliate da Kaspersky. Gli oggetti dannosi vengono riconosciuti mediante l'analisi delle firme, l'analisi euristica e i dati di Kaspersky Security Network.

Il controllo dei collegamenti presenti nei siti Web per verificare la presenza di minacce di phishing e indirizzi Web dannosi consente di evitare gli *attacchi di phishing*. Gli *attacchi di phishing* si presentano solitamente sotto forma di messaggi e-mail di criminali che, fingendosi istituzioni finanziarie (ad esempio banche), inviano collegamenti a siti Web fraudolenti. In questi messaggi e-mail, i criminali tentano di istigare l'utente a visitare un sito Web di phishing e a inserire dati riservati (ad esempio il numero della carta bancaria o il nome e la password del conto bancario online). Un attacco di phishing può ad esempio presentarsi sotto forma di un messaggio proveniente dalla propria banca con un collegamento al relativo sito Web ufficiale, mentre in realtà il collegamento rimanda a una copia identica del sito Web ufficiale della banca creato dagli impostori.

Protezione Minacce Web monitora il traffico Web per rilevare eventuali tentativi di accesso a un sito Web di phishing e blocca l'accesso a tali siti Web. Per il controllo dei collegamenti nei siti Web per verificare la presenza di minacce di phishing e indirizzi Web dannosi, Kaspersky Endpoint Security utilizza i database dell'applicazione, l'analisi euristica e i dati di Kaspersky Security Network.

Algoritmo di scansione del traffico Web

Ogni sito Web o file a cui accede l'utente o un'applicazione tramite i protocolli HTTP e HTTPS viene intercettato ed esaminato da Protezione Minacce Web per escludere la presenza di codice dannoso:

- Se un sito Web o un file contiene codice dannoso, Kaspersky Endpoint Security provvede al relativo blocco e visualizza una notifica per segnalare l'infezione del file richiesto o del sito Web richiesto.
- Se il file o il sito Web non contiene codice dannoso, è possibile accedervi immediatamente.

Selezionare l'azione che deve essere eseguita da Protezione Minacce Web in seguito al rilevamento di un oggetto del traffico Web pericoloso

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale** della sezione **Protezione minacce Web** selezionare l'azione eseguita da Protezione Minacce Web dopo il rilevamento di un oggetto del traffico Web pericoloso.

Le informazioni relative all'esecuzione di Protezione Minacce Web e a tutti gli oggetti pericolosi del traffico Web rilevati vengono registrate in un rapporto.

Nota: se l'esecuzione di Protezione Minacce Web viene interrotta con un errore, è possibile visualizzare il relativo rapporto e provare a riavviare il componente. Se il problema persiste, è possibile contattare l'Assistenza tecnica di Kaspersky.

Visualizzare il rapporto di Protezione Minacce Web

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.

   Verrà visualizzata la finestra **Rapporti**.

2. Aprire la scheda **Protezione minacce Web**.

Protezione minacce di posta

Il componente Protezione minacce di posta esamina gli allegati dei messaggi e-mail in entrata e in uscita alla ricerca di malware e altre minacce. Il componente garantisce la protezione del computer mediante database anti-malware, il servizio cloud Kaspersky Security Network e l'analisi euristica.

L'applicazione supporta i seguenti client di posta: Apple Mail, Microsoft Outlook, Mozilla Thunderbird, Canary Mail, Spark, Mimestream, Airmail, Post Box, Boxy Suite 2, Twobird, Shift, Clean Email, eM Client, Superhuman, Polymail, HEY, Mail+ per Gmail e Spike mail.

Per impostazione predefinita, Protezione minacce di posta è abilitato. Se necessario, è possibile disabilitare Protezione minacce di posta.

A seconda della modalità operativa selezionata, Protezione minacce di posta esegue le seguenti azioni:

- **Elimina oggetti dannosi automaticamente**. Se questa opzione è selezionata, quando Kaspersky Endpoint Security rileva un oggetto infetto in un messaggio e-mail, elimina l'oggetto infetto e sostituisce il contenuto dell'oggetto con il testo "The requested file infected with <nome virus> has been deleted".

- **Blocca oggetti dannosi automaticamente**. Se questa opzione è selezionata, quando Kaspersky Endpoint Security rileva un oggetto infetto in un messaggio e-mail, sostituisce l'oggetto del messaggio e-mail con "Message is infected: <oggetto originale>", dove <oggetto originale> è l'oggetto originale. L'oggetto del messaggio e-mail viene sostituito solo per il protocollo POP3.

Abilitare/disabilitare Protezione minacce di posta utilizzando Web Console

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

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

   Viene visualizzata la finestra delle proprietà dei criteri.

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

4. Passare a **Comunicazione e protezione Web → Protezione minacce di posta**.

5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione minacce di posta**.

6. Se Protezione minacce di posta è abilitato, selezionare l'azione che deve essere eseguita dall'applicazione quando viene rilevato malware:

   - **Elimina**

   - **Blocca**

7. Se necessario, nella sezione **Impostazioni avanzate** configurare il limite di tempo per il controllo degli archivi o la dimensione massima dell'archivio per la scansione.

8. Salvare le modifiche.

Abilitare/disabilitare Protezione minacce di posta utilizzando Administration Console

1. Avviare Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nella struttura della console fare clic su **Dispositivi gestiti**.

4. Nell'area di lavoro selezionare la scheda **Criteri**.

5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.

6. Nella finestra **Proprietà** selezionare **Protezione minacce essenziale** > **Protezione minacce di posta**.

7. Selezionare o deselezionare la casella di controllo **Abilita Protezione minacce di posta**.

8. Nella sezione **Azione se viene rilevata una minaccia**, selezionare l'azione da eseguire quando Kaspersky Endpoint Security rileva una minaccia.

9. Se necessario, nella sezione **Protezione minacce di posta: impostazioni** configurare il limite di tempo per il controllo degli archivi o la dimensione massima dell'archivio per la scansione.

10. Fare clic su **OK** per salvare le modifiche.

11. Per applicare le modifiche al criterio eseguire una delle seguenti operazioni:

    - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.

    - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.

Abilitare/disabilitare Protezione minacce di posta utilizzando l'applicazione Kaspersky Endpoint Security

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale**, nella sezione **Protezione minacce di posta**, selezionare o deselezionare la casella di controllo **Abilita Protezione minacce di posta**.

3. Se la casella di controllo **Abilita Protezione minacce di posta** è selezionata, selezionare l'azione da eseguire quando Kaspersky Endpoint Security rileva una minaccia.

4. Se necessario, configurare il limite di tempo per il controllo degli archivi o la dimensione massima dell'archivio per la scansione.

Visualizzare il rapporto di Protezione minacce di posta

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.

   Verrà visualizzata la finestra **Rapporti**.

2. Aprire la scheda **Protezione minacce di posta**.

Protezione Minacce di Rete

Kaspersky Endpoint Security assicura la protezione del computer dagli attacchi di rete.

Un *attacco di rete* è un tentativo di penetrare nel sistema operativo di un computer remoto. I criminali informatici tentano di eseguire attacchi di rete per ottenere il controllo del sistema operativo, rendere non disponibili i servizi del sistema operativo (Denial of Service) o accedere a informazioni sensibili. Per raggiungere questi obiettivi, i criminali eseguono attacchi diretti come la scansione delle porte e gli attacchi brute force oppure utilizzano il malware installato in un computer in cui è in corso un attacco.

Gli attacchi di rete noti possono essere suddivisi nei seguenti tipi:

- *Scansione delle porte*. Questo tipo di attacco di rete viene in genere eseguito in preparazione a un attacco di rete più pericoloso. Un intruso esegue la scansione delle porte UDP/TCP che utilizzano servizi di rete nel computer oggetto dell'attacco e determina il livello di vulnerabilità dei computer oggetti dell'attacco rispetto ad altri tipi di attacchi di rete più pericolosi. La scansione delle porte consente anche all'intruso di determinare il sistema operativo nel computer oggetto dell'attacco e di selezionare gli attacchi di rete appropriati per tale sistema operativo.

- *Attacchi DoS (Denial of Service)* o attacchi di rete che provocano l'interruzione del servizio. Questi attacchi di rete rendono instabile o completamente inutilizzabile il sistema operativo oggetto dell'attacco.

  I principali tipi di attacchi DoS sono:

  - Trasmissione di pacchetti di rete appositamente progettati che non sono previsti dal computer oggetto dell'attacco e che possono causare il malfunzionamento o l'arresto anomalo del sistema operativo.

  - Invio a un computer remoto di un numero elevato di pacchetti di rete in un breve periodo. Tutte le risorse del computer oggetto dell'attacco vengono utilizzate per elaborare i pacchetti di rete inviati dall'intruso. In seguito a questa operazione, il computer interrompe l'esecuzione delle relative funzioni.

- *Attacchi di intrusione nella rete*. Tali attacchi di rete sono progettati per assumere il controllo del sistema operativo del computer colpito. Si tratta del tipo di attacco di rete più pericoloso perché, se l'attacco va a buon fine, l'intruso ottiene il completo controllo del sistema operativo.

  Questo tipo di attacco di rete viene impiegato quando l'intruso desidera ottenere dati riservati da un computer remoto (ad esempio, numeri di carte bancarie o password) o utilizzare segretamente il computer remoto per i propri scopi (ad esempio, per attaccare altri computer da questo computer).

Abilitare o disabilitare Protezione Minacce di Rete

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale**, nella sezione **Protezione minacce di rete**, selezionare o deselezionare la casella di controllo **Abilita Protezione minacce di rete**.

È anche possibile abilitare Protezione Minacce di Rete in Centro protezione. Disabilitando la protezione del computer o i componenti di protezione, il computer è soggetto a un rischio molto più elevato di infezione. Per questo motivo Centro protezione informa l'utente quando la protezione del computer viene disabilitata.

Importante: se è stato disabilitato Protezione Minacce di Rete, il componente non verrà riabilitato automaticamente al riavvio di Kaspersky Endpoint Security o del sistema operativo. È necessario riabilitare Protezione Minacce di Rete manualmente.

Quando l'applicazione rileva attività di rete pericolosa, Kaspersky Endpoint Security aggiunge automaticamente l'indirizzo IP del computer da cui è stato originato l'attacco all'elenco dei computer bloccati, a meno che il computer che ha originato l'attacco non sia nell'elenco dei computer attendibili.

Modificare l'elenco dei computer bloccati

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale**, nella sezione **Protezione minacce di rete**, selezionare la casella di controllo **Abilita Protezione minacce di rete**.

3. Fare clic su **Impostazioni**.

   Verrà visualizzata una finestra con un elenco di computer attendibili e un elenco di computer bloccati.

4. Aprire la scheda **Computer bloccati**.

5. Se si è certi che il computer bloccato non sia una minaccia, selezionare l'indirizzo IP del computer nell'elenco e fare clic su **Sblocca**.

   Verrà visualizzata una finestra di dialogo di conferma.

6. Nella finestra di conferma eseguire una delle seguenti opzioni:

   - Se si desidera sbloccare il computer, fare clic su **Sblocca**.

     Kaspersky Endpoint Security sblocca l'indirizzo IP.

   - Se si desidera che Kaspersky Endpoint Security non blocchi mai l'indirizzo IP selezionato, fare clic su **Sblocca ed escludi**.

     Kaspersky Endpoint Security sblocca l'indirizzo IP e lo aggiunge all'elenco dei computer attendibili.

7. Fare clic su **Salva**.

È possibile creare e modificare l'elenco di computer attendibili. L'applicazione Kaspersky Endpoint Security non blocca automaticamente gli indirizzi IP di questi computer nemmeno in seguito al rilevamento di attività di rete pericolosa.

Modificare l'elenco dei computer attendibili

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Essenziale**, nella sezione **Protezione minacce di rete**, selezionare la casella di controllo **Abilita Protezione minacce di rete**.

3. Fare clic su **Impostazioni**.

   Verrà visualizzata una finestra con un elenco di computer attendibili e un elenco di computer bloccati.

4. Aprire la scheda **Computer attendibili**.

5. Modificare l'elenco dei computer attendibili:

   - Per aggiungere un indirizzo IP all'elenco dei computer attendibili:

     a. Fare clic su +.

     b. Nel campo visualizzato immettere l'indirizzo IP del computer che si ritiene attendibile.

   - Per rimuovere un indirizzo IP dall'elenco dei computer attendibili:

     a. Selezionare un indirizzo IP dall'elenco.

     b. Fare clic su –.

   - Per modificare un indirizzo IP nell'elenco dei computer attendibili:

     a. Selezionare un indirizzo IP dall'elenco.

     b. Fare clic su **Modifica**.

     c. Modificare l'indirizzo IP.

6. Fare clic su **Salva**.

Quando viene rilevato un attacco di rete, Kaspersky Endpoint Security registra le informazioni sull'attacco in un rapporto.

Nota: se l'esecuzione del componente Protezione Minacce di Rete viene interrotta con un errore, è possibile visualizzare il rapporto e tentare di riavviare il componente. Se il problema persiste, è possibile contattare l'Assistenza tecnica di Kaspersky.

Visualizzare il rapporto Protezione Minacce di Rete

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.

   Verrà visualizzata la finestra **Rapporti**.

2. Aprire la scheda **Protezione minacce di rete**.

Firewall

Firewall blocca le connessioni non autorizzate al computer durante l'utilizzo di Internet o della rete locale. Questo consente di proteggere la LAN aziendale da furto di identità e altri attacchi. Il componente garantisce la protezione del computer mediante database anti-malware, il servizio cloud Kaspersky Security Network e le regole di rete predefinite.

Priorità Regole di rete

Ogni regola ha una priorità. Più in alto si trova una regola nell'elenco, maggiore è la sua priorità. Se l'attività di rete viene aggiunta a più regole, Firewall regola l'attività di rete in base alla regola con la priorità più alta.

Tipi di connessione di rete

Firewall consente di controllare l'attività di rete a seconda del tipo di connessione di rete. È possibile modificare il tipo di connessione di rete nelle impostazioni di Kaspersky Endpoint Security.

Sono disponibili i seguenti tipi di connessione di rete:

- **Rete pubblica**. La rete non è protetta da applicazioni anti-malware, firewall o filtri (ad esempio Wi-Fi in un bar). Quando l'utente utilizza un computer connesso a tale rete, Firewall blocca l'accesso ai file e alle stampanti del computer. Gli utenti esterni non sono inoltre in grado di accedere ai dati tramite le cartelle condivise e l'accesso remoto al desktop del computer. Firewall assegna a Internet il tipo di rete Pubblica per impostazione predefinita. Non è possibile modificare il tipo di Internet.

- **Rete locale**. Rete per gli utenti con accesso limitato a file e stampanti nel computer (ad esempio una LAN aziendale o una rete domestica).

- **Rete attendibile**. Rete sicura in cui il computer non è esposto ad attacchi o tentativi di accesso non autorizzati ai dati. Firewall consente qualsiasi attività di rete all'interno di reti con questo stato.

Gestire il componente Firewall in Administration Console

1. Avviare Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà** selezionare **Protezione minacce essenziale** > **Firewall**.
7. Selezionare o deselezionare la casella di controllo **Abilita Firewall**.
8. Nella sezione **Impostazioni di Firewall**, fare clic sul pulsante **Impostazioni** e aggiungere, modificare, eliminare o cambiare la priorità delle regole.
9. Nella sezione **Reti disponibili** fare clic sul pulsante **Impostazioni** e aggiungere, modificare, eliminare o cambiare il tipo di reti.
10. Fare clic su **OK** per salvare le modifiche.

11. Per applicare le modifiche al criterio eseguire una delle seguenti operazioni:

    - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.
    - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.

Gestire il componente Firewall in Web Console

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Comunicazione e protezione Web** → **Firewall**.
5. Abilitare o disabilitare il componente utilizzando l'interruttore **Firewall**.
6. Nella sezione **Impostazioni di Firewall**, fare clic sul pulsante **Regole per i pacchetti di rete** e aggiungere, modificare, eliminare o cambiare la priorità delle regole.
7. Nella sezione **Reti disponibili** fare clic sul pulsante **Impostazioni di rete** e aggiungere, modificare o cambiare il tipo di reti.
8. Salvare le modifiche.

Gestire il componente Firewall nell'applicazione Kaspersky Endpoint Security

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.
2. Nella scheda **Essenziale**, nella sezione **Firewall**, deselezionare o selezionare la casella di controllo **Abilita Firewall**.
3. Se necessario, fare clic sul pulsante **Impostazioni** e configurare le impostazioni Firewall:

    - Nella scheda **Regole per i pacchetti di rete** è possibile aggiungere, modificare, eliminare o cambiare la priorità delle regole.
    - Nella scheda **Reti disponibili** è possibile aggiungere, modificare o cambiare il tipo di reti.

Di conseguenza, se Firewall è abilitato, Kaspersky Endpoint Security controlla le attività di rete e blocca le connessioni di rete non autorizzate al computer.

Visualizzare il rapporto Firewall

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.

   Verrà visualizzata la finestra **Rapporti**.
2. Aprire la scheda **Firewall**.

Rilevamento del Comportamento

Il componente Rilevamento del Comportamento riceve i dati sulle azioni delle applicazioni nel computer e fornisce queste informazioni ad altri componenti della protezione per migliorarne le prestazioni. Il componente Rilevamento del Comportamento utilizza le firme del flusso di comportamento (BSS) delle applicazioni. Se l'attività dell'applicazione corrisponde alla firma di un flusso di comportamento, Kaspersky Endpoint Security esegue l'azione di risposta selezionata. La funzionalità di Kaspersky Endpoint Security basata sulle firme del flusso di comportamento offre una difesa proattiva per il computer.

Per impostazione predefinita, Rilevamento del Comportamento è abilitato e viene eseguito nella modalità consigliata dagli esperti di Kaspersky. È possibile disabilitare Rilevamento del Comportamento, se necessario.

Abilitare/disabilitare Rilevamento del Comportamento utilizzando Web Console

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare alla sezione **Protezione minacce host** → **Analisi del comportamento** → **Rilevamento del Comportamento**.
5. Abilitare o disabilitare il componente utilizzando l'interruttore **Rilevamento del Comportamento**.
6. Se Rilevamento del Comportamento è abilitato, selezionare una delle seguenti azioni da eseguire quando viene rilevata un'attività malware:

   - **Blocca**

     Se questa opzione è selezionata, l'applicazione Kaspersky Endpoint Security termina l'applicazione quando rileva attività dannose.

   - **Elimina**

     Se questa opzione è selezionata, durante il rilevamento di attività dannose l'applicazione Kaspersky Endpoint Security elimina il file eseguibile dell'applicazione dannosa e crea una copia di backup del file in Backup.

   - **Richiedi l'intervento dell'utente**

     Se questa opzione è selezionata, quando viene rilevata attività malware, l'applicazione Kaspersky Endpoint Security visualizza una finestra di notifica con le informazioni sull'oggetto dannoso e richiede all'utente di scegliere l'azione che l'applicazione Kaspersky Endpoint Security deve intraprendere. Le azioni disponibili possono variare in base allo stato dell'oggetto.

7. Se Rilevamento del Comportamento e Protezione delle cartelle condivise dal criptaggio esterno sono abilitati, selezionare una delle seguenti azioni da eseguire quando viene rilevato il criptaggio esterno:

   - **Informa**

     Se questa opzione è selezionata, al rilevamento di un tentativo di modifica dei file nelle cartelle condivise, Kaspersky Endpoint Security aggiunge le informazioni su questo tentativo all'elenco delle minacce attive, aggiunge una voce ai rapporti locali dell'applicazione e invia le informazioni dell'attività dannosa rilevata a Kaspersky Security Center.

   - **Blocca il dispositivo da cui ha origine l'attacco per**

     Se questa opzione è selezionata, quando l'applicazione Kaspersky Endpoint Security rileva un tentativo di modifica dei file nelle cartelle condivise, blocca l'accesso alla modifica dei file (sola lettura) per la sessione che ha avviato l'attività dannosa e crea copie di backup dei file modificati.

8. Salvare le modifiche.

Abilitare/disabilitare Rilevamento del Comportamento utilizzando Administration Console

1. Avviare Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà** selezionare **Protezione minacce avanzata** > **Rilevamento del comportamento**
7. Selezionare o deselezionare la casella di controllo **Abilita Rilevamento del comportamento**.
8. Se necessario, nella sezione **Azione se viene rilevata un'attività malware** selezionare l'azione da eseguire quando viene rilevata un'attività malware.
9. Fare clic su **OK** per salvare le modifiche.
10. Per applicare le modifiche al criterio eseguire una delle seguenti operazioni:

    - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.
    - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.

Abilitare/disabilitare Rilevamento del Comportamento utilizzando l'applicazione Kaspersky Endpoint Security

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione **Rilevamento del Comportamento** della scheda **Avanzate**, selezionare o deselezionare la casella di controllo **Abilita Rilevamento del comportamento**.

3. Se la casella di controllo **Abilita Rilevamento del comportamento** è selezionata, selezionare una delle seguenti azioni da eseguire quando viene rilevata un'attività malware:

   - **Blocca**

     Se questa opzione è selezionata, l'applicazione Kaspersky Endpoint Security termina l'applicazione quando rileva attività dannose.

   - **Elimina**

     Se questa opzione è selezionata, durante il rilevamento di attività dannose l'applicazione Kaspersky Endpoint Security elimina il file eseguibile dell'applicazione dannosa e crea una copia di backup del file in Backup.

   - **Richiedi l'intervento dell'utente**

     Se questa opzione è selezionata, quando viene rilevata attività malware, l'applicazione Kaspersky Endpoint Security visualizza una finestra di notifica con le informazioni sull'oggetto dannoso e richiede all'utente di scegliere l'azione che l'applicazione Kaspersky Endpoint Security deve intraprendere. Le azioni disponibili possono variare in base allo stato dell'oggetto.

Di conseguenza, se Rilevamento del Comportamento è abilitato, Kaspersky Endpoint Security utilizza le firme del flusso di comportamento per analizzare l'attività delle applicazioni nel sistema operativo.

Importante: non è consigliabile disabilitare Rilevamento del Comportamento a meno che non sia assolutamente necessario poiché così facendo si ridurrà l'efficacia dei componenti della protezione. Per rilevare le minacce, i componenti della protezione possono richiedere i dati raccolti dal componente Rilevamento del Comportamento.

Scansione

Protezione minacce file e Protezione minacce Web forniscono protezione del computer in tempo reale. È inoltre consigliabile eseguire periodicamente la scansione del computer alla ricerca di malware e altre minacce alla sicurezza del computer. La scansione del computer è necessaria per impedire la diffusione di malware non rilevato dai componenti di protezione.

Kaspersky Endpoint Security contiene le seguenti attività di scansione integrate:

- **Scansione completa**.

  Scansione anti-malware della memoria del computer, degli oggetti di avvio e di tutti i dischi interni del computer.

- **Scansione rapida**.

  Scansione anti-malware delle sole aree critiche del computer: memoria, oggetti di avvio e cartelle di sistema.

- **Scansione personalizzata**.

  Scansione anti-malware di un oggetto specificato (file, cartella, disco interno o rimovibile).

- **Scansione dischi esterni**

  Scansione malware dei dischi esterni eseguita quando un disco esterno viene connesso al computer.

Quando l'applicazione esegue un'attività di scansione, gli oggetti dannosi vengono riconosciuti tramite l'analisi delle firme. Oltre all'analisi delle firme, Kaspersky Endpoint Security utilizza l'analisi euristica e altre tecnologie di scansione.

La finestra **Scansione** consente di visualizzare le informazioni sull'avanzamento di ciascuna attività di scansione in esecuzione (percentuale di completamento e tempo rimanente) e la cronologia delle scansioni (le 100 attività di scansione più recenti).

Avviare le attività Scansione completa e Scansione rapida

1. Nella barra laterale della finestra principale dell'applicazione, fare clic su **Scansione**.
   Verrà visualizzata la finestra **Scansione**.
2. Nella finestra **Scansione** fare clic sul pulsante **Scansione completa** o **Scansione rapida**.

L'attività di scansione viene avviata.

Avviare un'attività Scansione personalizzata

1. Nella barra laterale della finestra principale dell'applicazione, fare clic su **Scansione**.
   Verrà visualizzata la finestra **Scansione**.
2. Per avviare l'attività **Scansione personalizzata**, eseguire una delle seguenti operazioni:
   - Trascinare un file o una cartella nella finestra.
   - Fare clic su **Seleziona** e aprire un file o una cartella.

L'attività di scansione viene avviata.

Interrompere un'attività di scansione

1. Nella barra laterale della finestra principale dell'applicazione, fare clic su **Scansione**.
   Verrà visualizzata la finestra **Scansione**.
2. Nella finestra **Scansione** fare clic su Interrompi ( ) accanto all'attività di scansione che si desidera interrompere.
   Verrà visualizzata una finestra di dialogo di conferma.
3. Nella finestra di dialogo di conferma fare clic su **Interrompi**.

L'attività di scansione viene interrotta.

È possibile pianificare un'attività Scansione completa o Scansione rapida.

Pianificare un'attività di scansione dalla finestra Scansione

1. Nella barra laterale della finestra principale dell'applicazione, fare clic su **Scansione**.
   Verrà visualizzata la finestra **Scansione**.
2. Fare clic su **Pianifica scansione**.
   Verrà visualizzata una finestra di dialogo in cui è possibile impostare la pianificazione.
3. Selezionare la casella di controllo **Scansione completa** o **Scansione rapida**.

4. Specificare la frequenza di scansione e l'ora di avvio della scansione.

5. Fare clic su **OK**.

Pianificare un'attività di scansione dalla finestra Impostazioni

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Scansione** fare clic su **Pianifica**.

3. Nella finestra visualizzata selezionare la casella di controllo accanto al nome dell'attività di scansione che si desidera avviare in base a una pianificazione.

4. Configurare l'ora e la frequenza dell'attività di scansione.

5. Fare clic su **OK** per salvare le modifiche apportate alla pianificazione dell'attività di scansione.

Quando si connette un disco esterno al computer, l'applicazione Kaspersky Endpoint Security può avviare automaticamente la scansione del disco, richiedere se si desidera eseguire la scansione o non eseguire alcuna operazione. È possibile selezionare una delle opzioni nelle impostazioni dell'attività Scansione dischi esterni.

Selezionare l'azione eseguita dall'applicazione Kaspersky Endpoint Security quando si connette un disco esterno al computer

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nell'elenco a sinistra della scheda **Scansione** selezionare **Scansione dischi esterni**.

3. Nella sezione **Quando si connette un disco esterno** selezionare l'azione che Kaspersky Endpoint Security deve eseguire quando viene connesso un disco esterno.

Le attività Scansione completa e Scansione rapida contengono già ambiti di scansione. Durante l'esecuzione dell'attività Scansione completa, l'applicazione Kaspersky Endpoint Security esamina la memoria, gli oggetti di avvio e tutti i dischi interni del computer. Durante l'esecuzione dell'attività Scansione rapida, l'applicazione esegue la scansione della memoria del computer, degli oggetti di avvio e delle cartelle di sistema. È possibile modificare l'ambito della scansione dell'attività Scansione rapida.

Nota: è possibile ignorare la scansione del volume di sistema di sola lettura per ridurre in modo significativo i tempi di scansione. Per impostazione predefinita, Kaspersky Endpoint Security non esamina il volume di sistema di sola lettura quando esegue un'attività di Scansione rapida e lo esamina quando esegue un'attività di Scansione completa.

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Abilitare/disabilitare la scansione del volume di sistema di sola lettura

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nell'elenco a sinistra della scheda **Scansione** selezionare l'attività **Scansione completa** o **Scansione rapida**.

3. Nella sezione **Ottimizzazione** deselezionare/selezionare la casella di controllo **Ignora la scansione del volume di sistema di sola lettura**.

> **Importante:** l'ottimizzazione potrebbe essere disabilitata per motivi di sicurezza.

Aggiungere o rimuovere un file o una cartella nell'ambito della scansione dell'attività Scansione rapida

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nell'elenco a sinistra della scheda **Scansione** selezionare l'attività **Scansione rapida**.

3. Nella sezione **Ambito della scansione** fare clic su **Modifica**.

   Verrà visualizzata una finestra con l'elenco degli oggetti nell'ambito della scansione dell'attività Scansione rapida.

4. Modificare l'elenco degli oggetti dell'ambito di scansione:

   - Per aggiungere un file o una cartella all'ambito della scansione dell'attività Scansione rapida:

     a. Fare clic su +.

        Verrà visualizzato un menu pop-up in cui è possibile selezionare gli oggetti da aggiungere all'ambito della scansione.

     b. Scegliere la voce **File e cartelle**.

        Verrà visualizzata una finestra di dialogo in cui è possibile selezionare un file o una cartella.

     c. Selezionare un file o una cartella da aggiungere all'ambito della scansione dell'attività Scansione rapida.

     d. Fare clic su **Apri**.

   - Per rimuovere un file o una cartella dall'ambito della scansione dell'attività Scansione rapida:

     a. Selezionare un oggetto che si desidera rimuovere.

     b. Trascinare l'oggetto selezionato dalla finestra oppure fare clic su –.

5. Fare clic su **Salva**.

Aggiungere un oggetto nell'elenco predefinito Scansione rapida all'ambito della scansione dell'attività Scansione rapida

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nell'elenco a sinistra della scheda **Scansione** selezionare l'attività **Scansione rapida**.

3. Nella sezione **Ambito della scansione** fare clic su **Modifica**.

   Verrà visualizzata una finestra con l'elenco degli oggetti dell'ambito della scansione.

4. Fare clic su +.

   Verrà visualizzato un menu pop-up in cui è possibile selezionare gli oggetti da aggiungere all'ambito della scansione.

5. Nel menu pop-up selezionare un oggetto da aggiungere all'ambito della scansione (ad esempio **Memoria**).

6. Fare clic su **OK**.

Disabilitare la protezione di un oggetto nell'ambito della scansione dell'attività Scansione rapida

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nell'elenco a sinistra della scheda **Scansione** selezionare l'attività **Scansione rapida**.

3. Nella sezione **Ambito della scansione** fare clic su **Modifica**.

   Verrà visualizzata una finestra con l'elenco degli oggetti dell'ambito della scansione.

4. Deselezionare la casella relativa all'oggetto nell'elenco di oggetti dell'ambito della scansione.

5. Fare clic su **OK**.

Se viene rilevata una minaccia in un file, l'applicazione visualizza una notifica ed esegue sull'oggetto l'azione specificata. È possibile modificare l'azione da eseguire in caso di rilevamento di un oggetto.

Selezionare l'azione eseguita da Kaspersky Endpoint Security in caso di rilevamento di file infetti

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Scansione** selezionare un'attività nell'elenco delle attività.

3. Nella sezione **Azione** selezionare l'azione che l'applicazione deve eseguire al rilevamento di file infetti.

Prima di disinfettare o eliminare un file infetto, Kaspersky Endpoint Security ne salva una copia in Backup per consentire di ripristinare il file originale in caso di necessità.

Le informazioni relative ai risultati delle attività di scansione e a tutti gli oggetti rilevati vengono registrate in un rapporto.

Nota: se si verifica un errore durante l'esecuzione di un'attività di scansione anti-malware, riavviare l'attività. Se anche il nuovo tentativo di eseguire la scansione genera un errore, contattare l'Assistenza tecnica di Kaspersky.

Visualizzazione di un rapporto sulle attività di scansione

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.

   Verrà visualizzata la finestra **Rapporti**.

2. Aprire la scheda **Scansione**.

Attività di aggiornamento

Aggiornamenti periodici dei database dell'applicazione consentono di mantenere sempre protetto il computer. Protezione Minacce File, Protezione Minacce Web e le attività di scansione utilizzano i database dell'applicazione per il rilevamento e la neutralizzazione del malware presente nel computer. I database dell'applicazione vengono aggiornati regolarmente con diversi tipi di minacce e metodi per neutralizzarle, pertanto è importante aggiornarli periodicamente.

Kaspersky Endpoint Security scarica i database dell'applicazione e i nuovi moduli dell'applicazione dai server di aggiornamento di Kaspersky e li installa nel computer. Kaspersky Endpoint Security può inoltre utilizzare i punti di distribuzione, le cartelle locali o altri server Web.

Nota: è necessario l'accesso a Internet per la connessione ai server degli aggiornamenti e il download degli aggiornamenti. Se ci si connette a Internet tramite un server proxy, è necessario configurare le impostazioni di rete.

È possibile eseguire il download degli aggiornamenti dei database dell'applicazione in uno dei seguenti modi:

- **Automaticamente**. Kaspersky Endpoint Security controlla regolarmente la presenza di aggiornamenti nei server degli aggiornamenti di Kaspersky. Se in un server è disponibile un nuovo aggiornamento, Kaspersky Endpoint Security esegue il download dell'aggiornamento in background e lo installa nel computer. Questa opzione è abilitata per impostazione predefinita.
- **Manualmente**. È possibile verificare manualmente la disponibilità di aggiornamenti di Kaspersky Endpoint Security in qualsiasi momento.

Abilitare/disabilitare i download automatici degli aggiornamenti dei database di Kaspersky Endpoint Security

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Aggiornamento**, nella sezione **Database**, selezionare o deselezionare la casella di controllo **Scarica gli aggiornamenti automaticamente**.

Verificare la presenza di aggiornamenti dei database di Kaspersky Endpoint Security

1. Nella barra laterale della finestra principale dell'applicazione fare clic su **Aggiornamento**.

   Verrà visualizzata la finestra **Aggiornamento**.

2. Fare clic su **Aggiorna**.

L'applicazione avvierà l'aggiornamento dei database.

È inoltre possibile avviare un'attività di aggiornamento in uno dei seguenti modi:

- Fare clic sull'icona dell'applicazione e scegliere **Aggiornamento**.
- Nella barra dei menu scegliere **Protezione** > **Aggiornamento**.

Durante un aggiornamento, i moduli e i database dell'applicazione vengono confrontati con quelli attualmente disponibili nei server degli aggiornamenti. Se nel computer è installata la versione più recente dei database, nella finestra **Aggiornamento** viene visualizzato un messaggio per segnalare che i database dell'applicazione sono aggiornati. Se la versione e i database dell'applicazione sono diversi da quelli attualmente disponibili nei server degli aggiornamenti, nel computer saranno scaricati e installati solo i componenti mancanti dell'aggiornamento. Gli aggiornamenti incrementali dei database delle applicazioni richiedono meno tempo e meno traffico Web.

Se ci si connette a Internet tramite un server proxy, è possibile configurare le impostazioni di connessione al server proxy. Kaspersky Endpoint Security utilizza queste impostazioni per aggiornare i database dell'applicazione e scaricare gli aggiornamenti dei moduli dell'applicazione.

Configurare una connessione a un server proxy

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Selezionare la scheda **Aggiornamento**.

3. Nella sezione **Proxy** selezionare la casella di controllo **Usa server proxy** e fare clic su **Impostazioni**.

   Verrà visualizzata una finestra in cui è possibile configurare le impostazioni di connessione al server proxy.

4. Configurare la connessione a un server proxy.

5. Fare clic su **Salva** per salvare le modifiche apportate alle impostazioni di connessione al server proxy.

Prima di aggiornare i database dell'applicazione, Kaspersky Endpoint Security crea copie di backup, in modo da poter eseguire un rollback, se necessario. La funzionalità di rollback è utile quando una nuova versione dei database dell'applicazione contiene una firma non corretta che determina il blocco di un'applicazione sicura da parte di Kaspersky Endpoint Security.

Nota: se i database di Kaspersky Endpoint Security sono danneggiati, è consigliabile avviare un aggiornamento per scaricare e installare la versione più recente dei database dell'applicazione.

Eseguire il rollback dell'ultimo aggiornamento

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Selezionare la scheda **Aggiornamento**.

3. Nella sezione **Rollback** fare clic su **Rollback aggiornamento**.

Kaspersky Endpoint Security fornisce un rapporto dettagliato sui risultati delle attività di aggiornamento nella finestra **Rapporti**.

Visualizzare un rapporto sulle attività di aggiornamento:

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.
2. Verrà visualizzata la finestra **Rapporti**.
3. Selezionare la scheda **Aggiornamento database**.

Nota: Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Attività locali

Attività di scansione dei dischi esterni

Kaspersky Endpoint Security può eseguire la scansione di tutti i file eseguiti o copiati, anche se il file si trova su un disco esterno. Per prevenire la diffusione di malware, è possibile configurare scansioni automatiche dei dischi esterni quando sono connessi al dispositivo.

È possibile configurare le seguenti impostazioni di Scansione dischi esterni:

- **L'azione eseguita da Kaspersky Endpoint Security quando è connesso un disco esterno.**

  Scansione

  Se questa opzione è selezionata, Kaspersky Endpoint Security avvia un'attività di scansione malware per il disco esterno connesso.

  Questa opzione è selezionata per impostazione predefinita.

  Non eseguire alcuna operazione

  Se questa opzione è selezionata, Kaspersky Endpoint Security non esegue la scansione del disco esterno connesso.

- **L'azione eseguita da Kaspersky Endpoint Security in caso di rilevamento di un oggetto dannoso.**

  Disinfetta (se non è possibile, elimina)

  Se questa opzione è selezionata Kaspersky Endpoint Security blocca l'accesso all'oggetto infetto e tenta di disinfettarlo senza richiedere una conferma da parte dell'utente.

  Se l'oggetto viene disinfettato, Kaspersky Endpoint Security lo salva nella posizione originale con il nome originale. Se la disinfezione non riesce, Kaspersky Endpoint Security elimina gli oggetti infetti che non è stato possibile disinfettare.

  Questa opzione è selezionata per impostazione predefinita.

  Richiedi l'intervento dell'utente

Se questa opzione è selezionata, Kaspersky Endpoint Security visualizza una finestra di notifica con le informazioni sull'oggetto dannoso e richiede all'utente di scegliere l'azione che Kaspersky Endpoint Security deve intraprendere. Le azioni disponibili possono variare in base allo stato dell'oggetto.

È possibile configurare la Scansione dischi esterni in Administration Console, Web Console o nell'applicazione Kaspersky Endpoint Security.

Come configurare Scansione dischi esterni in Administration Console (MMC)

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà** selezionare **Attività locali** > **Scansione dischi esterni**.
7. Configurare le impostazioni dell'attività.
8. Fare clic su **OK** per salvare le modifiche.

Come configurare l'esecuzione di Scansione dischi esterni in Web Console e in Cloud Console

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Protezione minacce host** → **Scansione unità rimovibili**.
5. Abilitare o disabilitare il componente utilizzando l'interruttore **Scansione unità rimovibili**.
6. Salvare le modifiche.

Come configurare l'esecuzione della Scansione dischi esterni nell'interfaccia dell'applicazione

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.
   Verrà visualizzata la finestra delle impostazioni dell'applicazione.
2. Nell'elenco a sinistra della scheda **Scansione** selezionare **Scansione dischi esterni**.
3. Nella sezione **Quando si connette un disco esterno** selezionare l'azione che Kaspersky Endpoint Security deve eseguire quando viene connesso un disco esterno.

Backup

Talvolta non è possibile preservare l'integrità dei file infetti durante il processo di disinfezione. Se un file disinfettato conteneva informazioni importanti che risultano in parte o del tutto inaccessibili dopo la disinfezione, è possibile ripristinare il file originale da Backup.

Una *copia di backup* è una copia di un file pericoloso creata quando il file viene disinfettato o eliminato. La copia viene memorizzata in Backup.

Backup è un'area di archiviazione speciale contenente copie di backup dei file eliminati o modificati durante la disinfezione. La principale funzione di Backup è offrire all'utente la possibilità di ripristinare un file originale in qualsiasi momento. I file in Backup vengono salvati in un formato speciale e non sono pericolosi per il computer.

Visualizzare i contenuti di Backup

1. Nella barra dei menu scegliere **Protezione** > **Oggetti rilevati**.

   Verrà visualizzata la finestra **Oggetti rilevati**.

2. Nella sezione **Backup** visualizzare l'elenco dei file sottoposti a backup.

È possibile ripristinare o rimuovere le copie di backup dei file da Backup.

Ripristinare una copia di backup di un file da Backup

1. Nella barra dei menu scegliere **Protezione** > **Oggetti rilevati**.

   Verrà visualizzata la finestra **Oggetti rilevati**.

2. Nella sezione **Backup** fare clic su ••• accanto al file che si desidera ripristinare.

   Verrà visualizzato il menu pop-up.

3. Scegliere **Ripristina file**.

   Si aprirà una finestra in cui specificare il nome del file, il tag e la cartella in cui verrà ripristinato il file. Per impostazione predefinita, sono già specificati il nome del file e la posizione originali.

4. Specificare il nome del file e la cartella in cui verrà ripristinato il file.

5. Fare clic su **Salva**.

   L'applicazione ripristina il file nel percorso specificato e con il nome specificato.

È necessario sottoporre il file a una scansione anti-malware subito dopo averlo ripristinato. È possibile che l'oggetto venga disinfettato utilizzando i database aggiornati senza essere danneggiato.

Importante: non è consigliabile ripristinare le copie di backup dei file a meno che non sia assolutamente necessario, poiché il ripristino potrebbe esporre il computer al rischio di infezione.

Rimuovere una copia di backup di un file da Backup

1. Nella barra dei menu scegliere **Protezione** > **Oggetti rilevati**.

   Verrà visualizzata la finestra **Oggetti rilevati**.

2. Nella sezione **Backup** eseguire le seguenti operazioni:

   - Per eliminare tutte le copie di backup dei file, fare clic su **Elimina tutto**.
   - Per eliminare la copia di backup selezionata, fare clic su ••• accanto alla copia e scegliere **Elimina copia sottoposta a backup**.

Per impostazione predefinita, il periodo massimo di archiviazione dei file in Backup è 30 giorni. Al termine di questo periodo, i file vengono eliminati. È possibile modificare il periodo massimo di archiviazione dei file in Backup o rimuovere il limite relativo al periodo di archiviazione.

Configurare il periodo di archiviazione dei file in Backup

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Minacce** della sezione **Backup** selezionare la casella di controllo **Elimina oggetti sottoposti a backup dopo <numero> giorni** e specificare il periodo di tempo dopo il quale i file archiviati in Backup devono essere eliminati automaticamente.

Rapporti

È possibile visualizzare un rapporto di Kaspersky Endpoint Security in cui sono elencati tutti gli oggetti rilevati nella scheda **Oggetti elaborati**. Gli eventi di sistema vengono visualizzati nella scheda **Eventi di sistema**. In aggiunta, viene creato un altro rapporto dettagliato distinto per ciascuno dei seguenti componenti dell'applicazione: Protezione Minacce File, Protezione Minacce Web, Protezione Minacce di Rete, Rilevamento del Comportamento e le attività di scansione e aggiornamento.

Aprire la finestra Rapporti

Nella barra dei menu scegliere **Protezione** > **Rapporti**.

Kaspersky Endpoint Security può salvare i rapporti in formato di testo. Questa funzionalità può essere utile se le attività o i componenti dell'applicazione generano errori che non è possibile risolvere autonomamente ed è necessario l'intervento dell'Assistenza tecnica di Kaspersky. In tal caso, inviare il rapporto in formato di testo all'Assistenza tecnica di Kaspersky, così che i nostri esperti possano prendere in esame il problema e risolverlo il prima possibile.

Esportare un rapporto sui componenti o sulle attività di Kaspersky Endpoint Security in un file di testo

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.

   Verrà visualizzata la finestra **Rapporti**.

2. Nel riquadro sinistro selezionare la scheda con il rapporto desiderato.
3. Nell'angolo superiore destro fare clic su .
4. Nella finestra visualizzata specificare il nome di file, i tag e la cartella di destinazione per il rapporto.
5. Fare clic su **Salva**.

Per impostazione predefinita, Kaspersky Endpoint Security non registra nei rapporti gli eventi informativi. È possibile consentire la registrazione degli eventi informativi.

Consentire la registrazione degli eventi informativi nei rapporti

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Interfaccia**, nella sezione **Rapporti**, selezionare la casella di controllo **Registra eventi non critici** per ricevere le notifiche sugli eventi informativi di Kaspersky Endpoint Security.

Managed Detection and Response

Il componente Managed Detection and Response è stato aggiunto in Kaspersky Endpoint Security nella versione 11.2. Questo componente interagisce con una soluzione nota come Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* cerca, rileva ed elimina continuamente le minacce rivolte all'organizzazione. Per informazioni dettagliate sul funzionamento della soluzione, fare riferimento alla *Guida di Kaspersky Managed Detection and Response*.

Durante l'interazione con Kaspersky Managed Detection and Response, l'applicazione consente di eseguire le seguenti funzioni:

- Attivare Managed Detection and Response utilizzando un file di configurazione BLOB.
- Eseguire comandi da Kaspersky Managed Detection and Response.
- Inviare i dati di telemetria a Kaspersky Managed Detection and Response per il rilevamento delle minacce.

Il componente Managed Detection and Response presenta i seguenti requisiti aggiuntivi:

- macOS 14 o versione successiva
- Mac basato su Intel, Apple Silicon
- Licenza Kaspersky Endpoint Security attiva

È necessario abilitare i seguenti componenti per il corretto funzionamento di Managed Detection and Response:

- Protezione Minacce File
- Protezione Minacce Web
- Protezione minacce di posta

L'abilitazione di questi componenti non è facoltativa. In caso contrario Kaspersky Managed Detection and Response non può funzionare perché non riceve i dati di telemetria richiesti.

Inoltre, Kaspersky Managed Detection and Response utilizza i dati ricevuti da altri componenti dell'applicazione. L'abilitazione di questi componenti è facoltativa. Tra i componenti che forniscono dati aggiuntivi sono inclusi:

- Rilevamento del Comportamento

Integrazione con Kaspersky Managed Detection and Response

L'integrazione con Kaspersky Managed Detection and Response prevede i seguenti passaggi:

1. **Configurazione del server proxy Kaspersky Security Network.**

   Il server proxy Kaspersky Security Network facilita lo scambio di dati tra i computer e l'infrastruttura del servizio cloud Kaspersky Security Network tramite Administration Server anziché tramite scambio diretto.

   Caricare il file di configurazione di Kaspersky Security Network nelle proprietà di Administration Server. Il file di configurazione di Kaspersky Security Network si trova nell'archivio ZIP del file di configurazione MDR. È possibile ottenere l'archivio ZIP in Kaspersky Managed Detection and Response Console. Per informazioni dettagliate sulla configurazione del server proxy Kaspersky Security Network, fare riferimento alla *Guida di Kaspersky Security Center*.

   Di conseguenza, Kaspersky Endpoint Security utilizzerà KSN Privato per determinare la reputazione di file, applicazioni e siti Web. Lo stato operativo *"Infrastruttura Kaspersky Private Security Network"* verrà indicato nelle impostazioni dei criteri nella sezione Kaspersky Security Network.

   L'utilizzo di KSN Privato con Kaspersky Managed Detection and Response garantisce l'invio della telemetria ai server conformi al GDPR (General Data Protection Regulation). Se KSN Privato non viene utilizzato, è possibile inviare la telemetria a KSN Globale. Questo potrebbe violare la legislazione in vigore nel paese di appartenenza.

   Importante: è necessario abilitare la modalità KSN estesa per il corretto funzionamento di Managed Detection and Response.

2. **Attivazione di Kaspersky Managed Detection and Response**

   È possibile attivare il componente Managed Detection and Response nel dispositivo endpoint utilizzando i seguenti metodi:

   - **Eseguire l'attivazione utilizzando un codice di attivazione nell'applicazione Kaspersky Endpoint Security**.

     1. Aprire la finestra principale dell'applicazione.
     2. Nella barra laterale della finestra principale dell'applicazione fare clic su **Licenza**.

        Verrà visualizzata la finestra **Licenza**.
     3. Nella finestra **Licenza** inserire il codice di attivazione ricevuto al momento dell'acquisto.

        Nota: il codice di attivazione è una combinazione univoca di venti lettere e numeri dell'alfabeto latino nel formato xxxxx-xxxxx-xxxxx-xxxxx.
     4. Fare clic su **Attiva**.

        L'applicazione si connette ai server di attivazione di Kaspersky e invia il codice di attivazione per verificarne l'autenticità. Se il codice di attivazione viene verificato correttamente, l'applicazione riceve e aggiunge automaticamente la chiave di licenza.

        Nota: a seconda del codice di attivazione ricevuto, può essere necessario compilare un modulo di registrazione.

Se la verifica del codice di attivazione ha esito negativo, viene visualizzata una notifica. In questo caso, contattare il rivenditore del software che ha fornito il codice di attivazione.

- **Eseguire l'attivazione utilizzando il file BLOB**.

  Caricare il file di configurazione BLOB nel criterio di sicurezza di Kaspersky Endpoint Security (vedere le istruzioni di seguito). Il file BLOB contiene l'ID client e le informazioni sulla licenza per Kaspersky Managed Detection and Response. Il file BLOB si trova nell'archivio ZIP del file di configurazione MDR. È possibile ottenere l'archivio ZIP in Kaspersky Managed Detection and Response Console. Per informazioni dettagliate su un file BLOB, fare riferimento alla *Guida di Kaspersky Managed Detection and Response*.

  Attivare Kaspersky Managed Detection and Response in Administration Console (MMC)

  1. Avviare Kaspersky Security Center Administration Console.
  2. Ingrandire il nodo **Administration Server <nome server>**.
  3. Nella struttura della console fare clic su **Dispositivi gestiti**.
  4. Nell'area di lavoro selezionare la scheda **Criteri**.
  5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
  6. Nella finestra **Proprietà** selezionare **Detection and Response** > **Managed Detection and Response**.
  7. Selezionare la casella di controllo **Abilita Managed Detection and Response**.
  8. Nella sezione **File di configurazione MDR** fare clic su **Importa** e selezionare il file BLOB ricevuto in Kaspersky Managed Detection and Response Console. Il file ha l'estensione .P7.
  9. Fare clic su **OK** per salvare le modifiche.

  Attivare Kaspersky Managed Detection and Response in Web Console e Cloud Console

  1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Criteri e profili**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security for Mac.
  3. Viene visualizzata la finestra delle proprietà dei criteri.
  4. Selezionare la scheda **Impostazioni applicazione**.
  5. Selezionare **Detection and Response** > **Managed Detection and Response**.
  6. Attivare l'interruttore di **Managed Detection and Response**.
  7. Fare clic su **Importa** e selezionare il file BLOB ottenuto in Kaspersky Managed Detection and Response Console. Il file ha l'estensione .P7.
  8. Salvare le modifiche.

  Di conseguenza, Kaspersky Endpoint Security verificherà il file BLOB. La verifica dei file BLOB include il controllo della firma digitale e del periodo di validità della licenza. Se il file BLOB viene verificato correttamente, Kaspersky Endpoint Security caricherà il file e invierà il file al computer durante la sincronizzazione successiva con Kaspersky Security Center.

- **Eseguire l'attivazione utilizzando l'attività Aggiungi chiave**.

  - **Attivare Kaspersky Managed Detection and Response in Administration Console (MMC)**

    1. Nella finestra **Selezionare il tipo di attività** ingrandire il nodo **Kaspersky Endpoint Security for Mac 12.2.1**.

    2. Per creare un'attività per l'aggiunta di una chiave, selezionare **Aggiungi chiave**.

    3. Nella finestra **Attivazione dell'applicazione** eseguire le seguenti operazioni:

       a. Selezionare un codice di attivazione o una chiave dall'archivio di Kaspersky Security Center o aggiungere un file chiave archiviato nel computer.

       b. Per aggiungere la chiave specificata come chiave di riserva, selezionare la casella **Aggiungi come chiave di riserva**.

          La chiave di riserva diventa attiva allo scadere della chiave attiva corrente.

       Le informazioni sulla chiave specificata (chiave, tipo di chiave e data di scadenza della chiave) sono visualizzate nella finestra **Attivazione dell'applicazione**.

    4. Nella finestra Selezionare i dispositivi a cui assegnare l'attività selezionare il metodo che si desidera utilizzare per specificare i computer client:

       - Per scegliere tra i computer rilevati nella rete da Administration Server, selezionare l'opzione **Selezionare i dispositivi della rete rilevati da Administration Server**.

       - Per specificare gli indirizzi IP dei computer manualmente o per importare gli indirizzi IP dei computer da un file, selezionare l'opzione **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**.

       - Per creare un'attività per una selezione di dispositivi in base a un criterio preimpostato, selezionare l'opzione **Assegnare un'attività a una selezione di dispositivi**.

       - Per selezionare i computer da un gruppo di amministrazione specifico, selezionare l'opzione **Assegnare un'attività a un gruppo di amministrazione**.

    5. Nella finestra visualizzata (**Seleziona dispositivi**, **Selezione dispositivi** o **Seleziona gruppo di amministrazione**, a seconda dell'opzione selezionata nel passaggio precedente), selezionare i computer client, specificare gli indirizzi IP dei computer, specificare una selezione di computer o selezionare il gruppo di amministrazione a cui verrà applicata l'attività.

       Nota: questo passaggio non è attinente alle attività di gruppo o locali.

    6. Nella finestra **Configurare la pianificazione delle attività** selezionare la modalità di avvio nell'elenco a discesa **Avvio pianificato**.

    7. Se necessario, configurare l'avvio automatico di un'attività pianificata (specificando la data e l'ora di inizio dell'attività).

8. Se si desidera eseguire attività che l'applicazione non è stata in grado di avviare in base alla pianificazione (ad esempio perché il computer era spento all'ora pianificata), selezionare la casella **Esegui attività non effettuate**.

   Kaspersky Endpoint Security avvia l'attività non appena viene eliminato l'ostacolo che impedisce l'avvio dell'attività.

9. Se si desidera che Kaspersky Security Center determini automaticamente l'intervallo tra gli avvii dell'attività in diversi computer, selezionare la casella **Usa automaticamente il ritardo casuale per l'avvio delle attività**.

   Questo consente di ridurre il carico su Kaspersky Security Center Administration Server.

10. Per impostare l'intervallo tra gli avvii dell'attività in diversi computer manualmente, selezionare la casella **Usa ritardo casuale per l'avvio dell'attività con un intervallo di (min)** e specificare il numero di minuti.

    Questo consente di ridurre il carico su Kaspersky Security Center Administration Server.

11. Nel campo **Nome** della finestra **Definire il nome dell'attività** immettere il nome dell'attività che si intende creare.

1. Nella finestra **Completare la creazione dell'attività** eseguire le seguenti operazioni:

   a. Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella **Esegui l'attività al termine della procedura guidata**.

   b. Fare clic su **Fine** per chiudere la procedura guidata.

- **Attivare Kaspersky Managed Detection and Response in Web Console e Cloud Console**

1. Nella finestra principale di Web Console selezionare **Risorse (Dispositivi)** > **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la **Creazione guidata nuova attività**.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione** selezionare Kaspersky Endpoint Security for Mac (12.2.1).

   b. Nell'elenco a discesa **Tipo di attività** selezionare **Aggiungi chiave**.

   c. Nel campo **Nome attività** immettere una breve descrizione.

   d. Selezionare una delle seguenti opzioni:

      - **Assegnare un'attività a un gruppo di amministrazione**

        L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

        Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in uno specifico gruppo di amministrazione.

Se un'attività viene assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività poiché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi a cui si applicano.

- **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**

  È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

  È possibile utilizzare questa opzione per eseguire un'attività per una subnet specifica. Ad esempio, è possibile installare una determinata applicazione nei dispositivi dei contabili o eseguire la scansione dei dispositivi in una subnet probabilmente infetta.

- **Assegnare un'attività a una selezione di dispositivi**

  L'attività viene assegnata ai dispositivi inclusi in una selezione di dispositivi. È possibile specificare una delle selezioni esistenti.

  Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata.
5. Selezionare la chiave di licenza dall'elenco. Se l'elenco non contiene una licenza appropriata, è possibile aggiungere una nuova chiave di licenza nell'archivio di Administration Server.
6. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Nota: per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (root).

7. Al passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

   Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, viene aperta la finestra delle impostazioni dell'attività. In questa finestra è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio dell'attività, se necessario.

8. Fare clic sulla nuova attività.

   Viene visualizzata la finestra delle proprietà dell'attività.

9. Selezionare la scheda **Pianificazione**.
10. Configurare la pianificazione attività.

    Nota: assicurarsi che il computer sia acceso per eseguire l'attività.

11. Fare clic su **Salva**.

12. Per eseguire immediatamente l'attività indipendentemente dalla pianificazione configurata, effettuare le seguenti operazioni:

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

    b. Fare clic sul pulsante **Esegui**.

Endpoint Detection and Response Expert (on premises)

Kaspersky Endpoint Security supporta l'integrazione con il componente Kaspersky Endpoint Detection and Response come parte della soluzione Kaspersky Anti Targeted Attack Platform. Questa soluzione è progettata per rilevare tempestivamente le minacce avanzate, come attacchi mirati, minacce persistenti avanzate, attacchi zero-day e altro. Per informazioni dettagliate sul funzionamento della soluzione, fare riferimento alla *Guida di Kaspersky Managed Detection and Response*.

Quando l'integrazione con Endpoint Detection and Response (KATA) è configurata, il server KATA riceve le informazioni sugli eventi che si verificano durante il funzionamento di Kaspersky Endpoint Security, le minacce rilevate dall'applicazione e le informazioni sull'elaborazione di tali minacce. Per reagire alle minacce rilevate, Kaspersky Endpoint Security può quindi eseguire attività avviate nell'interfaccia Web di Kaspersky Anti Targeted Attack Platform.

Endpoint Detection and Response Expert (on-premise) presenta i seguenti requisiti aggiuntivi:

- Kaspersky Anti Targeted Attack Platform 6.0 o versione successiva.
- Kaspersky Security Center 14.2 o versione successiva.
- L'integrazione con Endpoint Detection and Response Expert (7.1 o versione precedente) può essere configurata in Kaspersky Security Center Administration Console (MMC), Web Console o Cloud Console.
- L'integrazione con Endpoint Detection and Response Expert (8.0 o versione successiva) può essere configurata in Kaspersky Security Center Administration Console (MMC), Web Console o Cloud Console.

Integrazione con Kaspersky Endpoint Detection and Response (KATA)

L'integrazione con Kaspersky Endpoint Detection and Response (KATA) prevede i seguenti passaggi:

1. **Installazione del componente Endpoint Detection and Response**

   È possibile selezionare il componente Endpoint Detection and Response durante l'installazione di Kaspersky Endpoint Security.

2. **Attivazione di Endpoint Detection and Response**

   Se il componente Endpoint Detection and Response non è supportato dalla licenza corrente, è necessario attivare separatamente Kaspersky Endpoint Detection and Response.

   È possibile verificare se la funzionalità Endpoint Detection and Response è supportata dalla licenza corrente nella finestra **Licenza**.

3. **Connessione a un server KATA**

Kaspersky Anti Targeted Attack Platform richiede la creazione di una connessione affidabile tra Kaspersky Endpoint Security e un server KATA. Per configurare una connessione affidabile, è necessario utilizzare un certificato TLS. È possibile scaricare un certificato TLS nell'interfaccia Web di Kaspersky Anti Targeted Attack Platform. Per informazioni dettagliate sul download di un certificato, fare riferimento alla *Guida di Kaspersky Anti Targeted Attack Platform*.

Per impostazione predefinita, Kaspersky Endpoint Security controlla solo il certificato TLS del server KATA. Per rendere la connessione più sicura, è possibile abilitare la verifica bidirezionale. Per abilitare la verifica bidirezionale, è necessario utilizzare un contenitore criptato protetto da password. Per informazioni dettagliate sul download di un contenitore criptato, fare riferimento alla *Guida di Kaspersky Anti Targeted Attack Platform*.

Connettere i computer con Kaspersky Endpoint Security a un server KATA utilizzando Administration Console

1. Avviare Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà** selezionare **Detection and Response** > **Endpoint Detection and Response Expert (on-premise)**.
7. Selezionare la casella di controllo **Abilitare Endpoint Detection and Response Expert (7.1 o versioni precedenti)**.
8. Fare clic su **Impostazioni della connessione al server**.
9. Nella finestra **Impostazioni della connessione al server** visualizzata, configurare le seguenti impostazioni:
   - Fare clic su **Carica certificato TLS** per selezionare un certificato TLS che verrà utilizzato per stabilire una connessione attendibile con un server KATA.
   - Se si desidera modificare il timeout di risposta del server KATA, specificare il timeout nel campo **Timeout (s)**. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server KATA.
   - Se si desidera utilizzare la verifica bidirezionale, selezionare la casella di controllo **Usa autenticazione a due fattori**. Fare clic su **Carica contenitore crittografico** per selezionare un file del contenitore criptato e immettere la password nel campo **Password contenitore crittografico**.
10. Fare clic su **Salva**.
11. Per aggiungere un server KATA, fare clic su **Aggiungi**.
12. Nella finestra del **Server KATA** visualizzata, specificare l'indirizzo e la porta del server e fare clic su **Salva**.
13. Fare clic su **OK** per salvare le modifiche.

Connettere i computer con Kaspersky Endpoint Security a un server KATA utilizzando Web Console

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Criteri e profili**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security for Mac.

   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Selezionare Detection and Response > **Endpoint Detection and Response Expert (on-premise)**.
5. Attivare l'interruttore **Endpoint Detection and Response Expert (on-premise)**.
6. Fare clic su **Impostazioni di connessione**.
7. Nella finestra **Impostazioni della connessione al server** visualizzata, configurare le seguenti impostazioni:
   - Fare clic su **Aggiungi certificato TLS** per selezionare un certificato TLS che verrà utilizzato per stabilire una connessione attendibile con un server KATA.
   - Se si desidera modificare il timeout di risposta del server KATA, specificare il timeout nel campo **Timeout (s)**. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server KATA.
   - Se si desidera utilizzare la verifica bidirezionale, selezionare la casella di controllo **Usa autenticazione a due vie**. Fare clic su **Carica contenitore crittografico** per selezionare un file del contenitore criptato e immettere la password nel campo **Password contenitore crittografico**.
8. Fare clic su **OK**.
9. Per aggiungere un server KATA, fare clic su **Aggiungi**.
10. Nella finestra di dialogo visualizzata, specificare l'indirizzo e la porta del server e fare clic su **OK**.
11. Salvare le modifiche.

Di conseguenza, i computer verranno visualizzati nell'interfaccia Web di Kaspersky Anti Targeted Attack Platform.

Endpoint Detection and Response Optimum

A partire dalla versione 12.1, Kaspersky Endpoint Security for Mac include un agente integrato per la soluzione Kaspersky Endpoint Detection and Response Optimum (di seguito anche "EDR Optimum"). Questa soluzione è progettata per proteggere l'infrastruttura IT aziendale dalle cyberminacce avanzate. La funzionalità della soluzione combina il rilevamento automatico delle minacce con la capacità di reagire a queste minacce per contrastare gli attacchi avanzati, inclusi nuovi exploit, ransomware, attacchi senza file, nonché metodi che utilizzano strumenti di sistema legittimi. Per i dettagli su questa soluzione, vedere la Guida di Kaspersky Endpoint Detection and Response Optimum.

Kaspersky Endpoint Detection and Response esamina e analizza lo sviluppo delle minacce e fornisce al *personale addetto alla sicurezza* o all'*Amministratore* le informazioni sul potenziale attacco necessarie per una risposta tempestiva. Kaspersky Endpoint Detection and Response visualizza i dettagli dell'avviso in una finestra separata. *Dettagli avviso* è uno strumento per visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Tra i dettagli degli avvisi sono inclusi, ad esempio, la cronologia dei file visualizzati nel computer. Per ulteriori informazioni sulla gestione dei dettagli degli avvisi, fare riferimento alla Guida di Kaspersky Endpoint Detection and Response Optimum.

Nota: è possibile configurare il componente EDR Optimum in Web Console.

Impostazioni di Endpoint Detection and Response

Parametro	Descrizione
Isolamento di rete	Isolamento automatico del computer dalla rete in risposta alle minacce rilevate. Quando l'isolamento di rete è attivato, l'applicazione interrompe tutte le connessioni attive e blocca tutte le nuove connessioni TCP/IP nel computer. L'applicazione lascia attive solo le seguenti connessioni: • Connessioni elencate in Esclusioni dall'isolamento di rete. • Connessioni avviate dai servizi di Kaspersky Endpoint Security. • Connessioni avviate da Kaspersky Security Center Network Agent.
Sblocca automaticamente il computer isolato tra N ore	L'isolamento di rete può essere disattivato automaticamente dopo un periodo di tempo specificato o manualmente. Per impostazione predefinita, Kaspersky Endpoint Security disattiva Isolamento di rete 8 ore dopo l'inizio dell'isolamento.
Esclusioni dall'isolamento di rete	Elenco di regole per le esclusioni dall'isolamento di rete. Le connessioni di rete che corrispondono alle regole non vengono bloccate nei computer quando Isolamento di rete è attivato. Per configurare Esclusioni dall'isolamento di rete, è possibile utilizzare un elenco di profili di rete standard. Per impostazione predefinita, le esclusioni includono i profili di rete che contengono regole che garantiscono il funzionamento costante dei dispositivi con il server DNS/DHCP e i ruoli client DNS/DHCP. È inoltre possibile modificare le impostazioni dei profili di rete standard o definire manualmente le esclusioni. **Importante:** le esclusioni specificate nelle proprietà dei criteri vengono applicate solo se l'isolamento di rete viene attivato automaticamente in risposta a una minaccia rilevata. Le esclusioni specificate nelle proprietà del computer vengono applicate solo se Isolamento di rete è attivato manualmente nelle proprietà del computer in Kaspersky Security Center Console o nei dettagli degli avvisi.
Prevenzione dell'esecuzione	La prevenzione dell'esecuzione consente di gestire l'esecuzione di file eseguibili e script, nonché di aprire file in formato Office. In questo modo è possibile, ad esempio, impedire l'esecuzione di applicazioni considerate non sicure. Di conseguenza, la diffusione della minaccia può essere fermata. La prevenzione dell'esecuzione supporta un set di interpreti di script. Per utilizzare il componente Prevenzione dell'esecuzione, è necessario aggiungere regole di prevenzione dell'esecuzione. La regola di prevenzione dell'esecuzione è un insieme di criteri che l'applicazione prende in considerazione quando reagisce all'esecuzione di un oggetto, ad esempio quando si blocca l'esecuzione di un oggetto. L'applicazione identifica i file in base ai loro percorsi o checksum calcolati utilizzando gli algoritmi di hash MD5 e SHA256.

Parametro	Descrizione
Azione in caso di esecuzione o apertura di un oggetto vietato	**Blocca e scrivi nel rapporto**. In questa modalità, l'applicazione blocca l'esecuzione di oggetti o l'apertura di documenti che soddisfano i criteri della regola di prevenzione. L'applicazione pubblica anche un evento sui tentativi di esecuzione di oggetti o di documenti aperti nel registro eventi di Kaspersky Security Center e nel sistema di registrazione unificato. **Registra solo gli eventi**. In questa modalità, Kaspersky Endpoint Security pubblica un evento sui tentativi di esecuzione di oggetti eseguibili o di documenti aperti che corrispondono ai criteri della regola di prevenzione nel registro eventi di Kaspersky Security Center e nel sistema di registrazione unificato, ma non blocca il tentativo di eseguire o aprire l'oggetto o il documento. Questa modalità è selezionata per impostazione predefinita.
Sandbox cloud	Cloud Sandbox è una tecnologia che consente di rilevare le minacce avanzate in un computer. Kaspersky Endpoint Security inoltra automaticamente i file rilevati a sandbox cloud per l'analisi. Sandbox cloud esegue questi file in un ambiente isolato per identificare le attività dannose e decidere in merito alla reputazione. I dati su questi file vengono quindi inviati a Kaspersky Security Network. Pertanto, se Cloud Sandbox ha rilevato un file dannoso, Kaspersky Endpoint Security eseguirà l'azione appropriata per eliminare questa minaccia in tutti i computer in cui viene rilevato questo file. **Nota:** la tecnologia sandbox cloud è abilitata in modo permanente ed è disponibile per tutti gli utenti di Kaspersky Security Network, indipendentemente dal tipo di licenza che stanno utilizzando.

Integrazione con Endpoint Detection and Response Optimum

Per l'integrazione con Kaspersky Endpoint Detection and Response, è necessario aggiungere il componente Endpoint Detection and Response Optimum (EDR Optimum) e configurare Kaspersky Endpoint Security.

Nota: i componenti EDR Optimum e Endpoint Detection and Response (KATA) non sono compatibili tra loro.

Affinché Endpoint Detection and Response funzioni devono essere soddisfatte le seguenti condizioni:

- Kaspersky Security Center 13.2 o versione successiva. Nelle versioni precedenti di Kaspersky Security Center è impossibile attivare la funzionalità Endpoint Detection and Response.
- Il plug-in di amministrazione di Kaspersky Endpoint Detection and Response è installato. Si tratta di un plug-in singolo per il funzionamento degli agent nei sistemi operativi Windows, Mac e Linux. Quando si lavora con Endpoint Detection and Response Optimum, sarà necessario il plug-in di amministrazione di Kaspersky Endpoint Security per creare attività di reazione alle minacce e il plug-in di amministrazione EDR per visualizzare i dettagli degli avvisi.
- Il componente EDR Optimum come parte di Kaspersky Endpoint Security supporta l'interazione con la soluzione Kaspersky Endpoint Detection and Response Optimum 3.0. L'interazione con le versioni precedenti di Kaspersky Endpoint Detection and Response Optimum non è supportata.
- EDR Optimum può essere gestito in Web Console.
- L'applicazione è attivata e la funzionalità è coperta dalla licenza.
- Il componente Endpoint Detection and Response è abilitato.

Integrazione con Kaspersky Endpoint Detection and Response Optimum

L'integrazione con Kaspersky Endpoint Detection and Response Optimum prevede i seguenti passaggi:

1. **Installazione del componente Endpoint Detection and Response Optimum**

   È possibile selezionare il componente Endpoint Detection and Response durante l'installazione di Kaspersky Endpoint Security.

2. **Attivazione di Endpoint Detection and Response**

   Se il componente Endpoint Detection and Response non è supportato dalla licenza corrente, è necessario attivare separatamente Kaspersky Endpoint Detection and Response.

   È possibile verificare se la funzionalità Endpoint Detection and Response è supportata dalla licenza corrente nella finestra **Licenza**.

3. **Abilitazione del componente Endpoint Detection and Response**

   È possibile abilitare o disabilitare il componente nelle impostazioni dei criteri di Kaspersky Endpoint Security for Mac.

   Come abilitare o disabilitare il componente Endpoint Detection and Response in Web Console

   1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
   2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

      Viene visualizzata la finestra delle proprietà dei criteri.
   3. Selezionare la scheda **Impostazioni applicazione**.
   4. Selezionare **Detection and Response** > **Endpoint Detection and Response**.
   5. Attivare l'interruttore **Endpoint Detection and Response Expert (on-premise)**.
   6. Salvare le modifiche.

Scansione per indicatori di compromissione

Un **Indicatore di Compromissione (IOC)** è un insieme di dati su un oggetto o un'attività che indica l'accesso non autorizzato al computer (compromissione dei dati). Ad esempio, molti tentativi non riusciti di accesso al sistema possono costituire un indicatore di compromissione. L'attività **Scansione IOC** consente di trovare indicatori di compromissione nel computer e di adottare misure di risposta alle minacce.

Kaspersky Endpoint Security ricerca gli indicatori di compromissione utilizzando i file IOC. I file IOC sono file contenenti i set di indicatori che l'applicazione tenta di abbinare per contare un rilevamento. I file IOC devono essere conformi ai requisiti per i file IOC.

Modalità di esecuzione dell'attività di scansione IOC

Kaspersky Endpoint Detection and Response consente di creare attività di scansione IOC standard per rilevare i dati compromessi. L'attività di scansione IOC standard è un'attività locale o di gruppo creata e configurata manualmente in Web Console. Le attività vengono eseguite utilizzando i file IOC preparati dall'utente. Se si desidera aggiungere manualmente un indicatore di compromissione, leggere i requisiti per i file IOC.

Creazione di un'attività di scansione IOC

È possibile creare manualmente attività di scansione IOC:

- Nei dettagli dell'avviso (solo per EDR Optimum).

  Dettagli avviso è uno strumento per visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Tra i dettagli degli avvisi sono inclusi, ad esempio, la cronologia dei file visualizzati nel computer. Per ulteriori informazioni sulla gestione dei dettagli degli avvisi, fare riferimento alla Guida di Kaspersky Endpoint Detection and Response Optimum.

- Utilizzo dell'attività guidata.

Per creare un'attività Scansione IOC:

1. Nella finestra principale di Web Console selezionare **Risorse (Dispositivi)** > **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la **Creazione guidata nuova attività**.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione** selezionare Kaspersky Endpoint Security for Mac (12.2.1).

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

   c. Nel campo **Nome attività** immettere una breve descrizione.

   d. Nella sezione **Selezionare i dispositivi a cui assegnare l'attività** selezionare l'ambito dell'attività.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata.

5. Nella sezione **Impostazioni Scansione IOC** caricare i file IOC per cercare gli indicatori di compromissione. È possibile aggiungere un file IOC o generarne uno da un file contenente hash di file o indirizzi IP.

   Dopo aver caricato i file IOC, è possibile visualizzare e modificare l'elenco degli indicatori dai file IOC.

   Nota: l'aggiunta o la rimozione di file IOC dopo l'esecuzione dell'attività non è consigliata. Ciò può causare la visualizzazione errata dei risultati della scansione IOC per le precedenti esecuzioni dell'attività. Per cercare gli indicatori di compromissione in base a nuovi file IOC, si consiglia di aggiungere nuove attività.

6. Configurare le azioni in base al rilevamento IOC:

   - **Isola il computer dalla rete**. Se questa opzione è selezionata, Kaspersky Endpoint Security isola il computer dalla rete per impedire la diffusione della minaccia. È possibile configurare la durata dell'isolamento nelle impostazioni del componente Endpoint Detection and Response.

   - **Sposta la copia in Quarantena ed elimina l'oggetto**. Se questa opzione è selezionata, Kaspersky Endpoint Security elimina l'oggetto dannoso trovato nel computer. Prima di eliminare l'oggetto, Kaspersky Endpoint Security crea una copia di backup nel caso in cui l'oggetto debba essere ripristinato in un secondo momento. Kaspersky Endpoint Security sposta la copia di backup in Quarantena.

   - **Esegui scansione delle aree critiche**. Se questa opzione è selezionata, Kaspersky Endpoint Security esegue l'attività Scansione rapida. Per impostazione predefinita, Kaspersky Endpoint Security esegue la scansione della memoria, degli oggetti di avvio e delle cartelle di sistema.

7. Passare alla sezione **Avanzate**.

8. Selezionare i tipi di dati (documenti IOC) che devono essere analizzati come parte dell'attività.

   Nota: Kaspersky Endpoint Security seleziona automaticamente i tipi di dati (documenti IOC) per l'attività Scansione IoC in base al contenuto dei file IoC caricati. Non è consigliabile deselezionare i tipi di dati.

   È inoltre possibile configurare gli ambiti di scansione per i seguenti tipi di dati:

   - **Processi - ProcessItem**
   - **File - FileItem**
   - **Porte di rete - PortItem**
   - **Account utente - UserItem**
   - **Tabelle ARP - ArpEntryItem**
   - **Host – SystemInfoItem**
   - **URL – UrlHistoryItem**
   - **Route – RouteEntryItem**

9. Fare clic su **OK**.

10. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

    Nota: per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (root).

11. Al passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

    Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, viene aperta la finestra delle impostazioni dell'attività. In questa finestra è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio dell'attività, se necessario.

12. Fare clic sulla nuova attività.

    Viene visualizzata la finestra delle proprietà dell'attività.

13. Selezionare la scheda **Pianificazione**.

14. Configurare la pianificazione attività.

    Nota: assicurarsi che il computer sia acceso per eseguire l'attività.

15. Fare clic su **Salva**.

16. Per eseguire immediatamente l'attività indipendentemente dalla pianificazione configurata, effettuare le seguenti operazioni:

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

    b. Fare clic sul pulsante **Esegui**.

17. Di conseguenza, Kaspersky Endpoint Security esegue la ricerca degli indicatori di compromissione nel computer. È possibile visualizzare i risultati dell'attività nelle proprietà dell'attività nella sezione **Risultati**. È possibile visualizzare le informazioni sugli indicatori di compromissione rilevati nelle proprietà dell'attività: **Impostazioni dell'applicazione** > **Risultati Scansione IOC**.

Nota: i risultati della scansione IOC vengono conservati per 30 giorni. Dopo questo periodo, Kaspersky Endpoint Security elimina automaticamente le voci più vecchie.

Sposta file in Quarantena

Quando reagiscono alle minacce, Kaspersky Endpoint Detection and Response può creare attività *Sposta file in Quarantena*. Ciò è necessario per ridurre al minimo le conseguenze della minaccia. La *Quarantena* è uno speciale archivio locale nel computer. L'utente può mettere in quarantena i file che considera pericolosi per il computer. I file in quarantena vengono archiviati in uno stato criptato e non minacciano la sicurezza del dispositivo. Kaspersky Endpoint Security utilizza Backup come archivio file. Per informazioni dettagliate sulla gestione della Quarantena nell'ambito delle soluzioni, fare riferimento alla Guida di Kaspersky Endpoint Detection and Response Optimum.

È possibile creare attività *Sposta file in Quarantena* nei seguenti modi:

- Nei dettagli dell'avviso (solo per EDR Optimum).

  Dettagli avviso è uno strumento per visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Tra i dettagli degli avvisi sono inclusi, ad esempio, la cronologia dei file visualizzati nel computer. Per ulteriori informazioni sulla gestione dei dettagli degli avvisi, fare riferimento alla Guida di Kaspersky Endpoint Detection and Response Optimum.

- Utilizzo dell'attività guidata.

  È necessario immettere il percorso del file o l'hash (SHA256 o MD5) o sia il percorso del file che l'hash del file.

L'attività *Sposta file in Quarantena* presenta le seguenti limitazioni:

- La dimensione del file non deve superare i 100 MB.
- È possibile configurare l'attività per EDR Optimum in Web Console.
- La capacità di backup è limitata dallo spazio libero sul disco.

Per creare un'attività Sposta file in Quarantena:

1. Nella finestra principale di Web Console selezionare **Risorse (Dispositivi)** > **Attività**.
   Viene aperto l'elenco delle attività.
2. Fare clic su **Aggiungi**.
   Verrà avviata la **Creazione guidata nuova attività**.
3. Configurare le impostazioni dell'attività:
   a. Nell'elenco a discesa **Applicazione** selezionare Kaspersky Endpoint Security for Mac (12.2.1).
   b. Nell'elenco a discesa **Tipo di attività** selezionare **Sposta file in Quarantena**.
   c. Nel campo **Nome attività** immettere una breve descrizione.
   d. Selezionare una delle seguenti opzioni:
      - **Assegnare un'attività a un gruppo di amministrazione**

        L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

        Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in uno specifico gruppo di amministrazione.

        Se un'attività viene assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività poiché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi a cui si applicano.
      - **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**

        È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

        È possibile utilizzare questa opzione per eseguire un'attività per una subnet specifica. Ad esempio, è possibile installare una determinata applicazione nei dispositivi dei contabili o eseguire la scansione dei dispositivi in una subnet probabilmente infetta.
      - **Assegnare un'attività a una selezione di dispositivi**

        L'attività viene assegnata ai dispositivi inclusi in una selezione di dispositivi. È possibile specificare una delle selezioni esistenti.

        Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.
4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata.

5. Nel passaggio **Ambito attività** specificare un gruppo di amministrazione, dispositivi con indirizzi specifici o una selezione di dispositivi.

   Le impostazioni disponibili dipendono dall'opzione selezionata al passaggio precedente.

6. Nell'elenco dei file, fare clic su **Aggiungi**.

   Verrà avviata la procedura guidata per l'aggiunta dei file.

7. Nell'elenco a discesa **Specificare il file da spostare in Quarantena** selezionare una delle opzioni e compilare i campi richiesti. Per aggiungere il file, è necessario immettere il percorso completo del file o sia l'hash del file che il percorso.

8. Se si desidera che l'attività sia applicabile agli oggetti di sistema critici, selezionare la casella di controllo **Applica agli oggetti critici di sistema**.

9. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Nota: per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (root).

10. Al passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

    Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, viene aperta la finestra delle impostazioni dell'attività. In questa finestra è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio dell'attività, se necessario.

11. Fare clic sulla nuova attività.

    Viene visualizzata la finestra delle proprietà dell'attività.

12. Selezionare la scheda **Pianificazione**.

13. Configurare la pianificazione attività.

    Nota: assicurarsi che il computer sia acceso per eseguire l'attività.

14. Fare clic su **Salva**.

15. Per eseguire immediatamente l'attività indipendentemente dalla pianificazione configurata, effettuare le seguenti operazioni:

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

    b. Fare clic sul pulsante **Esegui**.

Di conseguenza, Kaspersky Endpoint Security sposta il file in Quarantena.

L'attività *Sposta file in Quarantena* può terminare con l'errore *Accesso negato* se si sta tentando di mettere in Quarantena un file eseguibile attualmente in esecuzione. Creare un'attività Termina processo per il file e riprovare.

L'attività *Sposta file in Quarantena* può terminare con l'errore *Spazio insufficiente nell'archivio Quarantena* se si tenta di mettere in Quarantena un file troppo grande. Liberare lo spazio su disco e riprovare.

Ottieni file

È possibile ottenere file dai computer degli utenti. Ad esempio, è possibile configurare il recupero di un file di registro eventi creato da un'applicazione di terze parti. Per ottenere il file, è necessario creare un'attività dedicata. Come risultato dell'esecuzione dell'attività, il file viene salvato in Backup. È possibile scaricare questo file da Backup nel computer utilizzando Web Console. Nel computer dell'utente il file rimane nella cartella originale.

Importante: la dimensione del file non deve superare i 100 MB. La capacità di backup è limitata dallo spazio libero sul disco.

Per creare un'attività Ottieni file:

1. Nella finestra principale di Web Console selezionare **Risorse (Dispositivi)** > **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la **Creazione guidata nuova attività**.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione** selezionare Kaspersky Endpoint Security for Mac (12.2.1).

   b. Nell'elenco a discesa **Tipo di attività** selezionare **Ottieni file**.

   c. Nel campo **Nome attività** immettere una breve descrizione.

   d. Selezionare una delle seguenti opzioni:

   - **Assegnare un'attività a un gruppo di amministrazione**

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in uno specifico gruppo di amministrazione.

     Se un'attività viene assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività poiché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi a cui si applicano.

   - **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**

     È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     È possibile utilizzare questa opzione per eseguire un'attività per una subnet specifica. Ad esempio, è possibile installare una determinata applicazione nei dispositivi dei contabili o eseguire la scansione dei dispositivi in una subnet probabilmente infetta.

- **Assegnare un'attività a una selezione di dispositivi**

  L'attività viene assegnata ai dispositivi inclusi in una selezione di dispositivi. È possibile specificare una delle selezioni esistenti.

  Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata. Nella finestra **Ottieni file**, fare clic su **Aggiungi**.

   Viene aperta la finestra di dialogo **Ottieni file**.

5. Nell'elenco a discesa **Specificare il file da ottenere** selezionare una delle opzioni e compilare i campi richiesti.

   Per aggiungere il file, è necessario immettere il percorso completo del file o sia l'hash del file che il percorso.

6. Fare clic su **OK**.

   Le impostazioni del file da aggiungere verranno visualizzate nell'elenco dei file.

7. Fare clic su **Avanti**.

8. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Nota: per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (root).

9. Al passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

   Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, viene aperta la finestra delle impostazioni dell'attività. In questa finestra è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio dell'attività, se necessario.

10. Fare clic sulla nuova attività.

    Viene visualizzata la finestra delle proprietà dell'attività.

11. Selezionare la scheda **Pianificazione**.

12. Configurare la pianificazione attività.

    Nota: assicurarsi che il computer sia acceso per eseguire l'attività.

13. Fare clic su **Salva**.

14. Per eseguire immediatamente l'attività indipendentemente dalla pianificazione configurata, effettuare le seguenti operazioni:

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

    b. Fare clic sul pulsante **Esegui**.

Di conseguenza, Kaspersky Endpoint Security crea una copia del file e la sposta in Backup. È possibile scaricare il file da Backup in Web Console.

Elimina file

È possibile eliminare i file in remoto utilizzando l'attività *Elimina file*. Ad esempio, è possibile eliminare in remoto un file quando si risponde alle minacce.

Per creare un'attività Elimina file:

1. Nella finestra principale di Web Console selezionare **Risorse (Dispositivi)** > **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la **Creazione guidata nuova attività**.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione** selezionare Kaspersky Endpoint Security for Mac (12.2.1).

   b. Nell'elenco a discesa **Tipo di attività** selezionare **Elimina file**.

   c. Nel campo **Nome attività** immettere una breve descrizione.

   d. Selezionare una delle seguenti opzioni:

   - **Assegnare un'attività a un gruppo di amministrazione**

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in uno specifico gruppo di amministrazione.

     Se un'attività viene assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività poiché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi a cui si applicano.

   - **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**

     È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     È possibile utilizzare questa opzione per eseguire un'attività per una subnet specifica. Ad esempio, è possibile installare una determinata applicazione nei dispositivi dei contabili o eseguire la scansione dei dispositivi in una subnet probabilmente infetta.

   - **Assegnare un'attività a una selezione di dispositivi**

     L'attività viene assegnata ai dispositivi inclusi in una selezione di dispositivi. È possibile specificare una delle selezioni esistenti.

     Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata.

5. Nell'elenco a discesa **Specifica il file da eliminare** selezionare una delle opzioni e compilare i campi richiesti. Per aggiungere il file, è necessario immettere il percorso completo del file o sia l'hash del file che il percorso.

6. Se si desidera che l'attività sia applicabile agli oggetti di sistema critici, selezionare la casella di controllo **Applica agli oggetti critici di sistema**.

7. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Nota: per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (root).

8. Al passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

   Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, viene aperta la finestra delle impostazioni dell'attività. In questa finestra è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio dell'attività, se necessario.

9. Fare clic sulla nuova attività.

   Viene visualizzata la finestra delle proprietà dell'attività.

10. Selezionare la scheda **Pianificazione**.

11. Configurare la pianificazione attività.

    Nota: assicurarsi che il computer sia acceso per eseguire l'attività.

12. Fare clic su **Salva**.

13. Per eseguire immediatamente l'attività indipendentemente dalla pianificazione configurata, effettuare le seguenti operazioni:

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

    b. Fare clic sul pulsante **Esegui**.

Di conseguenza, Kaspersky Endpoint Security elimina il file dal computer. Se il file è bloccato da un processo diverso, l'attività viene visualizzata come *Completata*, ma il file stesso viene eliminato solo dopo il riavvio del computer. Dopo aver riavviato il computer, confermare che il file è stato eliminato.

L'attività *Elimina file* può terminare con l'errore *Accesso negato* se si tenta di eliminare un file eseguibile attualmente in esecuzione. Creare un'attività Termina processo per il file e riprovare.

Avvia processo

È possibile eseguire i file in remoto utilizzando l'attività *Avvia processo*.

Importante: è possibile configurare l'attività per EDR Optimum in Web Console.

Per creare un'attività Avvia processo:

1. Nella finestra principale di Web Console selezionare **Risorse (Dispositivi)** > **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la **Creazione guidata nuova attività**.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione** selezionare Kaspersky Endpoint Security for Mac (12.2.1).

   b. Nell'elenco a discesa **Tipo di attività** selezionare **Avvia processo**.

   c. Nel campo **Nome attività** immettere una breve descrizione.

   d. Selezionare una delle seguenti opzioni:

   - **Assegnare un'attività a un gruppo di amministrazione**

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in uno specifico gruppo di amministrazione.

     Se un'attività viene assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività poiché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi a cui si applicano.

   - **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**

     È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     È possibile utilizzare questa opzione per eseguire un'attività per una subnet specifica. Ad esempio, è possibile installare una determinata applicazione nei dispositivi dei contabili o eseguire la scansione dei dispositivi in una subnet probabilmente infetta.

   - **Assegnare un'attività a una selezione di dispositivi**

     L'attività viene assegnata ai dispositivi inclusi in una selezione di dispositivi. È possibile specificare una delle selezioni esistenti.

     Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata.

5. Nel passaggio **Ambito attività** specificare un gruppo di amministrazione, dispositivi con indirizzi specifici o una selezione di dispositivi.

   Le impostazioni disponibili dipendono dall'opzione selezionata al passaggio precedente.

6. Configurare le impostazioni dell'attività:

    a. Nel campo **Comando eseguibile** specificare il comando da eseguire nel dispositivo locale.

    b. Se necessario, specificare gli argomenti della riga di comando nel campo **Argomenti della riga di comando (facoltativo)**.

    c. Se necessario, specificare il percorso del file eseguibile nel campo **Percorso della cartella di lavoro (non obbligatorio)**.

7. Al passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

    Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, viene aperta la finestra delle impostazioni dell'attività. In questa finestra è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio dell'attività, se necessario.

8. Fare clic sulla nuova attività.

    Viene visualizzata la finestra delle proprietà dell'attività.

9. Selezionare la scheda **Pianificazione**.

10. Configurare la pianificazione attività.

    > **Nota:** assicurarsi che il computer sia acceso per eseguire l'attività.

11. Fare clic su **Salva**.

12. Per eseguire immediatamente l'attività indipendentemente dalla pianificazione configurata, effettuare le seguenti operazioni:

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

    b. Fare clic sul pulsante **Esegui**.

Di conseguenza, Kaspersky Endpoint Security esegue il comando in modalità automatica e avvia il processo. È possibile visualizzare i risultati dell'attività nelle proprietà dell'attività nella sezione **Risultati dell'esecuzione**.

Termina processo

È possibile terminare i processi in remoto utilizzando l'attività *Termina processo*. Ad esempio, è possibile terminare in remoto un'utilità di test della velocità Internet avviata utilizzando l'attività Avvia processo.

Se si desidera vietare l'esecuzione di un file, è possibile configurare il componente Prevenzione dell'esecuzione. È possibile vietare l'esecuzione di file eseguibili, script e file in formato Office.

L'attività *Termina processo* presenta le seguenti limitazioni:

- È possibile configurare l'attività solo per EDR Optimum in Web Console.

Per creare un'attività Termina processo:

1. Nella finestra principale di Web Console selezionare **Risorse (Dispositivi)** > **Attività**.

   Viene aperto l'elenco delle attività.

2. Fare clic su **Aggiungi**.

   Verrà avviata la **Creazione guidata nuova attività**.

3. Configurare le impostazioni dell'attività:

   a. Nell'elenco a discesa **Applicazione** selezionare Kaspersky Endpoint Security for Mac (12.2.1).

   b. Nell'elenco a discesa **Tipo di attività** selezionare **Termina processo**.

   c. Nel campo **Nome attività** immettere una breve descrizione.

   d. Selezionare una delle seguenti opzioni:

   - **Assegnare un'attività a un gruppo di amministrazione**

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in uno specifico gruppo di amministrazione.

     Se un'attività viene assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività poiché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi a cui si applicano.

   - **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**

     È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     È possibile utilizzare questa opzione per eseguire un'attività per una subnet specifica. Ad esempio, è possibile installare una determinata applicazione nei dispositivi dei contabili o eseguire la scansione dei dispositivi in una subnet probabilmente infetta.

   - **Assegnare un'attività a una selezione di dispositivi**

     L'attività viene assegnata ai dispositivi inclusi in una selezione di dispositivi. È possibile specificare una delle selezioni esistenti.

     Ad esempio, è possibile utilizzare questa opzione per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

4. Selezionare i dispositivi in base all'opzione dell'ambito dell'attività selezionata.

5. Nel passaggio **Ambito attività** specificare un gruppo di amministrazione, dispositivi con indirizzi specifici o una selezione di dispositivi.

   Le impostazioni disponibili dipendono dall'opzione selezionata al passaggio precedente.

6. In questo passaggio della procedura guidata, nell'elenco a discesa **Specificare i processi del file che devono essere terminati**, selezionare una delle opzioni e compilare i campi richiesti. Per specificare il file, è necessario immettere il percorso completo del file o sia l'hash del file che il percorso.

   Nota: se si crea questa attività per un dispositivo locale, è possibile specificare il processo per PID.

7. Se si desidera che l'attività sia applicabile agli oggetti di sistema critici, selezionare la casella di controllo **Applica agli oggetti critici di sistema**.

8. Immettere le credenziali dell'account dell'utente di cui si desidera utilizzare i diritti per eseguire l'attività. Fare clic su **Avanti**.

   Nota: per impostazione predefinita, Kaspersky Endpoint Security avvia l'attività come account utente di sistema (root).

9. Al passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

   Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, viene aperta la finestra delle impostazioni dell'attività. In questa finestra è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio dell'attività, se necessario.

10. Fare clic sulla nuova attività.

    Viene visualizzata la finestra delle proprietà dell'attività.

11. Selezionare la scheda **Pianificazione**.

12. Configurare la pianificazione attività.

    Nota: assicurarsi che il computer sia acceso per eseguire l'attività.

13. Fare clic su **Salva**.

14. Per eseguire immediatamente l'attività indipendentemente dalla pianificazione configurata, effettuare le seguenti operazioni:

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

    b. Fare clic sul pulsante **Esegui**.

Di conseguenza, Kaspersky Endpoint Security interrompe il processo nel computer. Ad esempio, se un'applicazione di *gioco* è in esecuzione e si termina il processo di *gioco*, l'applicazione viene chiusa senza salvare i dati. È possibile visualizzare i risultati dell'attività nelle proprietà dell'attività nella sezione **Risultati**.

Prevenzione dell'esecuzione

La prevenzione dell'esecuzione consente di gestire l'esecuzione di file eseguibili e script, nonché di aprire file in formato Office. In questo modo è possibile, ad esempio, impedire l'esecuzione di applicazioni considerate non sicure. Di conseguenza, la diffusione della minaccia può essere fermata. La prevenzione dell'esecuzione supporta un set di interpreti di script.

Regola di prevenzione dell'esecuzione

La prevenzione dell'esecuzione gestisce l'accesso degli utenti ai file con regole di prevenzione dell'esecuzione. La regola di prevenzione dell'esecuzione è un insieme di criteri che l'applicazione prende in considerazione quando reagisce all'esecuzione di un oggetto, ad esempio quando si blocca l'esecuzione di un oggetto. L'applicazione identifica i file in base ai loro percorsi o checksum calcolati utilizzando gli algoritmi di hash MD5 e SHA256.

È possibile creare regole di prevenzione dell'esecuzione:

- Nei dettagli dell'avviso (solo per EDR Optimum).

  Dettagli avviso è uno strumento per visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Tra i dettagli degli avvisi sono inclusi, ad esempio, la cronologia dei file visualizzati nel computer. Per ulteriori informazioni sulla gestione dei dettagli degli avvisi, fare riferimento alla Guida di Kaspersky Endpoint Detection and Response Optimum.

- Utilizzando un criterio di gruppo o le impostazioni dell'applicazione locale. È necessario immettere il percorso del file o l'hash (SHA256 o MD5) o sia il percorso del file che l'hash del file.

È inoltre possibile gestire la prevenzione dell'esecuzione in locale utilizzando la riga di comando.

Nota: è impossibile bloccare l'avvio di oggetti critici di sistema (SCO). Gli SCO sono file richiesti dal sistema operativo e dall'applicazione Kaspersky Endpoint Security for Mac per poter essere eseguiti.

Modalità della regola di prevenzione dell'esecuzione

Il componente Prevenzione dell'esecuzione può funzionare in due modalità:

- **Solo statistiche**

  In questa modalità, Kaspersky Endpoint Security pubblica un evento sui tentativi di esecuzione di oggetti eseguibili o di documenti aperti che corrispondono ai criteri della regola di prevenzione nel registro eventi di Kaspersky Security Center e nel sistema di registrazione unificato, ma non blocca il tentativo di eseguire o aprire l'oggetto o il documento. Questa modalità è selezionata per impostazione predefinita.

- **Attivo**

  In questa modalità, l'applicazione blocca l'esecuzione di oggetti o l'apertura di documenti che soddisfano i criteri della regola di prevenzione. L'applicazione pubblica anche un evento sui tentativi di esecuzione di oggetti o di documenti aperti nel registro eventi di Kaspersky Security Center e nel sistema di registrazione unificato.

Gestire Prevenzione dell'esecuzione

Importante: è possibile configurare le impostazioni del componente solo in Web Console.

Per impedire l'esecuzione:

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Criteri e profili**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security for Mac.

   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Selezionare **Detection and Response** > **Endpoint Detection and Response**.
5. Attivare l'interruttore **Prevenzione dell'esecuzione**.
6. Nella sezione **Azione in caso di esecuzione o apertura di un oggetto vietato** selezionare la modalità di funzionamento del componente:

   - **Blocca e scrivi nel rapporto**. In questa modalità, l'applicazione blocca l'esecuzione di oggetti o l'apertura di documenti che soddisfano i criteri della regola di prevenzione. L'applicazione pubblica anche un evento sui tentativi di esecuzione di oggetti o di documenti aperti nel registro eventi di Kaspersky Security Center e nel sistema di registrazione unificato.
   - **Registra solo gli eventi**. In questa modalità, Kaspersky Endpoint Security pubblica un evento sui tentativi di esecuzione di oggetti eseguibili o di documenti aperti che corrispondono ai criteri della regola di prevenzione nel registro eventi di Kaspersky Security Center e nel sistema di registrazione unificato, ma non blocca il tentativo di eseguire o aprire l'oggetto o il documento. Questa modalità è selezionata per impostazione predefinita.
7. Creare un elenco di regole di prevenzione dell'esecuzione:

   a. Fare clic su **Aggiungi**.

   b. Nella finestra di dialogo visualizzata, immettere il nome della regola di prevenzione dell'esecuzione (ad esempio, Applicazione A).

   c. Nell'elenco a discesa **Tipo** selezionare l'oggetto che si desidera bloccare: **Applicazione**, **Script**, **Documento**.

   Se si seleziona un tipo di oggetto errato, Kaspersky Endpoint Security non blocca il file o lo script.

   d. Per aggiungere il file, è necessario immettere l'hash del file (SHA256 o MD5), il percorso completo del file o sia l'hash che il percorso.

   Nota: se il file si trova in un'unità di rete, immettere il percorso del file nel modo seguente: /Volumes/shared_folder_name/filename. Se il percorso del file contiene una lettera di unità di rete, Kaspersky Endpoint Security non blocca il file o lo script.

   a. Fare clic su **OK**.
8. Salvare le modifiche.

Di conseguenza, Kaspersky Endpoint Security blocca l'esecuzione di oggetti: esecuzione di file eseguibili e script, apertura di file in formato Office. È tuttavia possibile, ad esempio, aprire un file di script in un editor di testo anche se l'esecuzione dello script è stata impedita. Quando si blocca l'esecuzione di un oggetto, Kaspersky Endpoint Security visualizza una notifica standard se le notifiche sono abilitate nelle impostazioni dell'applicazione.

Isolamento di rete del computer

L'isolamento di rete del computer consente di isolare automaticamente un computer dalla rete in risposta al rilevamento di un indicatore di compromissione (IOC): questa è la modalità automatica. È possibile attivare l'isolamento della rete manualmente mentre si esamina la minaccia rilevata: questa è la modalità manuale.

Quando l'isolamento della rete è attivato, l'applicazione interrompe tutte le connessioni attive e blocca tutte le nuove connessioni di rete TCP/IP nel computer ad eccezione delle seguenti connessioni:

- Connessioni elencate in Esclusioni dall'isolamento di rete.
- Connessioni avviate dai servizi di Kaspersky Endpoint Security.
- Connessioni avviate da Kaspersky Security Center Network Agent.

Importante: è possibile configurare le impostazioni del componente solo in Web Console.

Modalità di isolamento di rete automatico

È possibile configurare l'isolamento di rete per l'attivazione automatica in risposta a un rilevamento IOC. È possibile configurare la modalità di isolamento di rete automatica con un criterio di gruppo.

Come configurare l'isolamento di rete per l'attivazione automatica in risposta a un rilevamento IOC

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Attività**.
2. Viene aperto l'elenco delle attività.
3. Fare clic sull'attività **Scansione IOC** di Kaspersky Endpoint Security.

   Viene visualizzata la finestra delle proprietà dell'attività.

   Se necessario, creare l'attività Scansione IOC.
4. Selezionare la scheda **Impostazioni applicazione**.
5. Nella sezione **Azione se viene rilevato un oggetto IOC**, selezionare l'opzione **Avvisa e intraprendi azioni di risposta in seguito al rilevamento di un oggetto IOC**, quindi la casella di controllo **Isola il computer dalla rete (8 ore)**.
6. Salvare le modifiche.
7. Di conseguenza, quando viene rilevato un IOC, l'applicazione isola il computer dalla rete per impedire la diffusione della minaccia.

È possibile configurare l'isolamento di rete in modo che venga disattivato automaticamente dopo che è trascorso un periodo di tempo specificato. Per impostazione predefinita, l'applicazione disattiva l'Isolamento di rete dopo che sono trascorse 8 ore dall'attivazione. È inoltre possibile disattivare l'Isolamento di rete manualmente (vedere le istruzioni di seguito). Dopo aver disattivato l'isolamento di rete, il computer può utilizzare la Rete senza restrizioni.

Come configurare il ritardo per la disattivazione dell'Isolamento di rete di un computer in modalità automatica

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Criteri e profili**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Selezionare **Detection and Response** > **Endpoint Detection and Response**.
5. Nella sezione **Isolamento di rete** fare clic su **Configura le impostazioni di sblocco del computer**.
6. Nella finestra visualizzata selezionare la casella di controllo **Sblocca automaticamente il computer isolato tra** e immettere il ritardo per la disattivazione automatica dell'Isolamento di rete.
7. Salvare le modifiche.

Modalità di Isolamento di rete manuale

È possibile attivare e disattivare manualmente l'Isolamento di rete. È possibile configurare la modalità di Isolamento di rete manuale utilizzando le proprietà del computer nella console Kaspersky Endpoint Security Center.

È possibile attivare l'Isolamento di rete:

- Nei dettagli dell'avviso (solo per EDR Optimum).

  Dettagli avviso è uno strumento per visualizzare la totalità delle informazioni raccolte su una minaccia rilevata. Tra i dettagli degli avvisi sono inclusi, ad esempio, la cronologia dei file visualizzati nel computer. Per ulteriori informazioni sulla gestione dei dettagli degli avvisi, fare riferimento alla Guida di Kaspersky Endpoint Detection and Response Optimum.
- Utilizzo delle impostazioni dell'applicazione locale.

Come attivare manualmente l'Isolamento di rete di un computer

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Dispositivi gestiti**.
2. Selezionare il computer per il quale si desidera configurare le impostazioni dell'applicazione locale.

   Vengono aperte le proprietà del computer.
3. Selezionare la scheda **Applicazioni**.
4. Fare clic su **Kaspersky Endpoint Security for Mac**.

   Vengono aperte le impostazioni dell'applicazione locale.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Selezionare **Detection and Response** > **Endpoint Detection and Response**.
7. Nella sezione **Isolamento di rete** fare clic su **Isola il computer dalla rete**.

È possibile configurare l'isolamento di rete in modo che venga disattivato automaticamente dopo che è trascorso un periodo di tempo specificato. Per impostazione predefinita, l'applicazione disattiva l'Isolamento di rete dopo che sono trascorse 8 ore dall'attivazione. Dopo aver disattivato l'isolamento di rete, il computer può utilizzare la Rete senza restrizioni.

Come configurare il ritardo per la disattivazione dell'Isolamento di rete di un computer in modalità manuale

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Dispositivi gestiti**.
2. Selezionare il computer per il quale si desidera configurare le impostazioni dell'applicazione locale.

   Vengono aperte le proprietà del computer.
3. Selezionare la scheda **Attività**.

   Viene visualizzato l'elenco delle attività disponibili nel computer.
4. Selezionare l'attività **Isolamento di rete**.
5. Selezionare la scheda **Impostazioni applicazione**.
6. Nella finestra visualizzata selezionare il ritardo per la disattivazione dell'Isolamento di rete.
7. Salvare le modifiche.

Come disattivare manualmente l'Isolamento di rete di un computer

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Dispositivi gestiti**.
2. Selezionare il computer per il quale si desidera configurare le impostazioni dell'applicazione locale.
3. Vengono aperte le proprietà del computer.
4. Selezionare la scheda **Applicazioni**.
5. Fare clic su Kaspersky Endpoint Security for Mac.
6. Vengono aperte le impostazioni dell'applicazione locale.
7. Selezionare la scheda **Impostazioni applicazione**.
8. Selezionare **Detection and Response** > **Endpoint Detection and Response**.
9. Nella sezione **Isolamento di rete**, fare clic su **Sblocca il computer isolato dalla rete**.

È inoltre possibile disabilitare l'isolamento della rete in locale utilizzando la riga di comando.

Esclusioni dall'Isolamento di rete

È possibile configurare le esclusioni dell'Isolamento di rete. Le connessioni di rete che corrispondono alle regole non vengono bloccate nel computer quando l'isolamento di rete è attivato.

Per configurare Esclusioni dall'isolamento di rete, è possibile utilizzare un elenco di profili di rete standard. Per impostazione predefinita, le esclusioni includono i profili di rete che contengono regole che garantiscono il funzionamento costante dei dispositivi con il server DNS/DHCP e i ruoli client DNS/DHCP. È inoltre possibile modificare le impostazioni dei profili di rete standard o definire manualmente le esclusioni (vedere le istruzioni di seguito).

Importante: le esclusioni specificate nelle proprietà dei criteri vengono applicate solo se l'isolamento di rete viene attivato automaticamente in risposta a una minaccia rilevata. Le esclusioni specificate nelle proprietà del computer vengono applicate solo se l'isolamento di rete è attivato manualmente nelle proprietà del computer nella console Kaspersky Security Center.

Nota: un criterio attivo non impedisce l'applicazione di esclusioni dall'Isolamento di rete configurato nelle proprietà del computer poiché questi parametri hanno scenari di utilizzo diversi.

Come aggiungere un'esclusione dell'Isolamento di rete in modalità automatica

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Criteri e profili**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
3. Viene visualizzata la finestra delle proprietà dei criteri.
4. Selezionare la scheda **Impostazioni applicazione**.
5. Selezionare **Detection and Response** > **Endpoint Detection and Response**.
6. Nella sezione **Esclusioni dall'isolamento di rete**, fare clic su **Esclusioni**.
7. Nella finestra successiva, fare clic su **Aggiungi dal profilo** e selezionare i profili di rete standard per la configurazione delle esclusioni.
8. Le esclusioni dall'Isolamento di rete dal profilo vengono aggiunte all'elenco delle esclusioni dall'Isolamento di rete. È possibile visualizzare le proprietà delle connessioni di rete. Se necessario, è possibile modificare le impostazioni della connessione di rete.
9. Se necessario, aggiungere manualmente un'esclusione dall'Isolamento di rete. A tale scopo, nella finestra con l'elenco delle esclusioni, fare clic su **Aggiungi** e modificare manualmente le impostazioni della connessione di rete.
10. Salvare le modifiche.

Come aggiungere un'esclusione dall'Isolamento di rete in modalità manuale

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Dispositivi gestiti**.
2. Selezionare il computer per il quale si desidera configurare le impostazioni dell'applicazione locale.
3. Vengono aperte le proprietà del computer.
4. Selezionare la scheda **Attività**.
5. Viene visualizzato l'elenco delle attività disponibili nel computer.

6. Selezionare l'attività **Isolamento di rete**.
7. Selezionare la scheda **Impostazioni applicazione**.
8. Nella finestra visualizzata fare clic su **Esclusioni**.
9. Nella finestra successiva, fare clic su **Aggiungi dal profilo** e selezionare i profili di rete standard per la configurazione delle esclusioni.
10. Le esclusioni dall'Isolamento di rete dal profilo vengono aggiunte all'elenco delle esclusioni dall'Isolamento di rete. È possibile visualizzare le proprietà delle connessioni di rete. Se necessario, è possibile modificare le impostazioni della connessione di rete.
11. Se necessario, aggiungere manualmente un'esclusione dall'Isolamento di rete. A tale scopo, nella finestra con l'elenco delle esclusioni, fare clic su **Aggiungi** e modificare manualmente le impostazioni della connessione di rete.
12. Salvare le modifiche.

È inoltre possibile visualizzare l'elenco delle esclusioni dall'isolamento di rete in locale utilizzando la riga di comando. In questo caso, il computer deve essere isolato.

Cloud Sandbox

Cloud Sandbox è una tecnologia che consente di rilevare le minacce avanzate in un computer. Kaspersky Endpoint Security inoltra automaticamente i file rilevati a sandbox cloud per l'analisi. Sandbox cloud esegue questi file in un ambiente isolato per identificare le attività dannose e decidere in merito alla reputazione. I dati su questi file vengono quindi inviati a Kaspersky Security Network. Pertanto, se Cloud Sandbox rileva un file dannoso, Kaspersky Endpoint Security eseguirà l'azione appropriata per eliminare la minaccia in tutti i computer in cui viene rilevato questo file.

Importante: per il funzionamento di Cloud Sandbox, è necessario abilitare l'utilizzo di Kaspersky Security Network.

Nota: se si utilizza Kaspersky Private Security Network, la tecnologia Cloud Sandbox non è disponibile.

Per abilitare Cloud Sandbox:

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Accedere alla sezione **Configurazione agenti integrati** → **Endpoint Detection and Response**.
5. Selezionare la scheda **Sandbox cloud**.

6. Attivare l'interruttore **Cloud Sandbox**.

7. Salvare le modifiche.

Ogni volta che è presente una minaccia, Kaspersky Endpoint Security attiva il contatore delle minacce rilevate utilizzando Cloud Sandbox nella finestra principale dell'applicazione nella sezione **Rilevamento delle minacce**. Kaspersky Endpoint Security indicherà anche la tecnologia di rilevamento delle minacce Cloud Sandbox nel Rapporto sulle minacce nella console Kaspersky Security Center.

Criptaggio disco FileVault

Kaspersky Endpoint Security consente la gestione remota del criptaggio FileVault. Il criptaggio impedisce agli utenti non autorizzati di accedere ai dati sensibili archiviati nel disco di avvio del computer dell'utente.

Quando un amministratore avvia il criptaggio FileVault in un computer da Kaspersky Security Center, Kaspersky Endpoint Security richiede all'utente di questo computer di immettere le proprie credenziali. Il criptaggio del disco viene avviato solo dopo che l'utente fornisce le credenziali, il computer viene riavviato e sono trascorsi 30 minuti dalla ricezione delle impostazioni dei criteri nel computer. Anche l'intervallo minimo tra le richieste per le credenziali è 30 minuti.

Per impedire all'utente di decriptare il disco di avvio del proprio Mac quando la crittografia FileVault è abilitata, un amministratore deve utilizzare JAMF per distribuire un profilo MDM che proibisca il decriptaggio del disco. Per decriptare il disco di avvio di un Mac con un profilo MDM che vieta il decriptaggio del disco, l'amministratore deve prima rimuovere il profilo.

Nota: se la gestione criptaggio FileVault non è abilitata in Kaspersky Security Center, gli utenti con i diritti di amministratore possono criptare e decriptare i propri dischi di avvio Mac dalle impostazioni di sistema. Per ulteriori informazioni su FileVault, fare riferimento alla documentazione di Apple.

Se nel computer sono presenti più account computer, il criptaggio FileVault rende il disco inaccessibile a tutti gli utenti ad eccezione dell'utente che ha immesso le credenziali.

Consentire ad altri utenti di sbloccare il disco

1. Scegliere **menu Apple** > **Impostazioni di Sistema** > **Privacy e sicurezza**.

2. Fare clic su **FileVault**.

   Verrà visualizzata la finestra **FileVault**.

3. Fare clic su **Abilita utenti**.

4. Nella finestra visualizzata selezionare un utente da autorizzare per sbloccare il computer.

5. Immettere la password dell'account del computer dell'utente e fare clic su **OK**.

6. Fare clic su **Continua**.

L'utente può accedere al disco criptato.

Nota: sono necessari i diritti di amministratore per consentire ad altri utenti di sbloccare il disco.

Se un amministratore gestisce Kaspersky Endpoint Security tramite Kaspersky Security Center Administration Console, Web Console o Cloud Console e un utente di questo computer dimentica o smarrisce le credenziali e non può accedere a un disco criptato, l'amministratore può ottenere una chiave di ripristino.

Come ottenere una chiave di ripristino utilizzando Kaspersky Security Center Administration Console

Come ottenere una chiave di ripristino utilizzando Kaspersky Security Center Web Console e Cloud Console

Protezione tramite password

Kaspersky Endpoint Security consente di limitare le azioni indesiderate nei dispositivi degli utenti impostando una password amministratore.

Se la protezione tramite password è abilitata, Kaspersky Endpoint Security richiede una password quando tenta di eseguire una delle seguenti operazioni:

- Configurare le impostazioni dell'applicazione
- Uscire dall'applicazione
- Rimuovere la chiave di licenza
- Rimuovere l'applicazione

  > **Nota:** la protezione tramite password limita la rimozione di Kaspersky Endpoint Security solo se eseguita tramite il programma di disinstallazione.

- Ripristina i file spostati in Quarantena dal Backup
- Visualizza rapporti.

La disabilitazione della protezione tramite password non disabilita le impostazioni dei criteri. Se la modifica di un'impostazione è vietata nel criterio, non può essere modificata anche se la protezione tramite password è disabilitata.

Abilitare la protezione tramite password utilizzando Administration Console

1. Avviare Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà** selezionare **Impostazioni avanzate > Interazione utente**.
7. Nella sezione **Protezione tramite password** selezionare la casella di controllo **Abilita protezione tramite password**.

8. Nella finestra **Impostazioni di protezione tramite password** visualizzata, configurare le seguenti impostazioni:
    - Immettere la password nel campo **Password** e inserirla una seconda volta nel campo **Conferma password**.
    - Nella sezione **Richiedi password per le seguenti operazioni** selezionare le caselle di controllo richieste per proteggere le azioni corrispondenti nel dispositivo dell'utente.
9. Fare clic su **OK** per salvare le modifiche.
10. Per applicare le modifiche al criterio eseguire una delle seguenti operazioni:
    - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.
    - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.

Modificare le impostazioni di protezione tramite password utilizzando Administration Console

1. Avviare Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà** selezionare **Impostazioni avanzate > Interazione utente**.
7. Nella sezione **Protezione tramite password**, fare clic sul pulsante **Impostazioni**.
8. Nella finestra **Impostazioni di protezione tramite password** visualizzata, modificare le impostazioni che si desidera modificare.
9. Fare clic su **OK** per salvare le modifiche.

Abilitare Protezione tramite password utilizzando Web Console

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Criteri e profili**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security for Mac.
3. Viene visualizzata la finestra delle proprietà dei criteri.
4. Selezionare la scheda **Impostazioni applicazione**.
5. Selezionare **Impostazioni aggiuntive** > **Interazione utente**.
6. Attivare l'interruttore **Protezione tramite password**.

7. Nella finestra **Impostazioni di protezione tramite password** visualizzata, configurare le seguenti impostazioni:

    - Immettere la password nel campo **Password** e inserirla una seconda volta nel campo **Confermare la password**. Per impostazione predefinita, i caratteri della password sono nascosti per motivi di sicurezza. Per visualizzare la password, fare clic su **Mostra**.

    - Nella sezione **Richiedi password per le seguenti operazioni** selezionare le caselle di controllo richieste per proteggere le azioni corrispondenti nel dispositivo dell'utente.

8. Fare clic su **OK** per chiudere la finestra di dialogo **Impostazioni di protezione tramite password**.

9. Fare clic su **OK** per chiudere la sezione **Interazione utente**.

10. Fare clic su **Salva** per salvare le modifiche al criterio.

Modificare Protezione tramite password utilizzando Web Console

1. Nella finestra principale di Web Console selezionare **Dispositivi** > **Criteri e profili**.

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

3. Viene visualizzata la finestra delle proprietà dei criteri.

4. Selezionare la scheda **Impostazioni applicazione**.

5. Selezionare **Impostazioni aggiuntive** > **Interazione utente**.

6. Nella sezione **Protezione tramite password**, fare clic sul pulsante **Impostazioni**.

7. Nella finestra **Impostazioni di protezione tramite password** visualizzata, modificare le impostazioni che si desidera modificare.

8. Fare clic su **OK** per chiudere la finestra di dialogo **Impostazioni di protezione tramite password**.

9. Fare clic su **OK** per chiudere la sezione **Interazione utente**.

10. Fare clic su **Salva** per salvare le modifiche al criterio.

Abilitare Protezione tramite password utilizzando l'applicazione Kaspersky Endpoint Security

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

    Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Interfaccia**, nella sezione **Protezione tramite password**, selezionare la casella di controllo **Abilita protezione tramite password**.

3. Nella finestra visualizzata, configurare le seguenti impostazioni:

    - Immettere la password nel campo **Password** e inserirla una seconda volta nel campo **Conferma password**.

    - Nella sezione **Richiedi password per** selezionare le caselle di controllo richieste per proteggere le azioni corrispondenti nel dispositivo dell'utente.

4. Fare clic su **OK**.

> **Nota:** se si seleziona **Modifica le impostazioni dell'applicazione** come azione protetta tramite password, è necessario immettere la password due volte per modificare le impostazioni di protezione tramite password.

Modificare Protezione tramite password utilizzando l'applicazione Kaspersky Endpoint Security

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Interfaccia**, nella sezione **Protezione tramite password**, fare clic su **Impostazioni**.

3. Nella finestra visualizzata, modificare le impostazioni che si desidera modificare.

4. Fare clic su **OK**.

Prevenzione Exploit

Il componente Prevenzione Exploit rileva codice di programma che sfrutta le vulnerabilità del computer per sfruttare i privilegi di amministratore o per eseguire attività dannose. Gli exploit possono ad esempio utilizzare un attacco di overflow del buffer. A tale scopo, l'exploit invia una grande quantità di dati a un'applicazione vulnerabile. Durante l'elaborazione di questi dati, l'applicazione vulnerabile esegue un codice dannoso. In seguito a questo attacco, l'exploit può avviare un'installazione non autorizzata di malware. In caso di tentativo di esecuzione di un file eseguibile da un'applicazione vulnerabile non eseguito dall'utente, Kaspersky Endpoint Security blocca l'esecuzione di questo file o invia una notifica all'utente.

Per impostazione predefinita, Prevenzione Exploit è abilitato. Se necessario, è possibile disabilitare Prevenzione Exploit.

Abilitare/disabilitare Prevenzione Exploit utilizzando Web Console

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

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

   Viene visualizzata la finestra delle proprietà dei criteri.

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

4. Passare alla sezione **Protezione minacce host** → **Analisi del comportamento** → **Prevenzione Exploit**.

5. Abilitare o disabilitare il componente utilizzando l'interruttore **Prevenzione Exploit**.

6. Se Prevenzione Exploit è abilitato, selezionare una delle seguenti azioni da eseguire quando viene rilevato un exploit:

   - **Blocca**

     Se questo elemento è selezionato durante il rilevamento di un exploit, Kaspersky Endpoint Security blocca le operazioni di questo exploit e crea una voce di registro con le informazioni sull'exploit.

- **Informa**

  Se questo elemento è selezionato, quando Kaspersky Endpoint Security rileva un exploit registra una voce contenente informazioni sull'exploit e aggiunge le informazioni sull'exploit all'elenco delle minacce attive.

7. Salvare le modifiche.

Abilitare/disabilitare Prevenzione Exploit utilizzando Administration Console

1. Avviare Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà** selezionare **Protezione minacce avanzata** > **Prevenzione Exploit**.
7. Selezionare o deselezionare la casella di controllo **Abilita Prevenzione Exploit**.
8. Se necessario, nella sezione **Al rilevamento di exploit** selezionare l'azione da eseguire quando Kaspersky Endpoint Security rileva un exploit.
9. Fare clic su **OK** per salvare le modifiche.
10. Per applicare le modifiche al criterio eseguire una delle seguenti operazioni:

    - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.
    - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.

Abilitare/disabilitare Prevenzione Exploit utilizzando l'applicazione Kaspersky Endpoint Security

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella sezione Prevenzione Exploit della scheda **Avanzate**, selezionare o deselezionare la casella di controllo **Abilita Prevenzione Exploit**.
3. Se la casella di controllo **Abilita Rilevamento del Comportamento** è selezionata, selezionare una delle seguenti azioni da eseguire quando viene rilevata un'attività malware:

   - **Blocca automaticamente l'attività malware pericolosa**

     Se questo elemento è selezionato durante il rilevamento di un exploit, Kaspersky Endpoint Security blocca le operazioni di questo exploit e crea una voce di registro con le informazioni sull'exploit.

   - **Informa**

     Se questo elemento è selezionato, quando Kaspersky Endpoint Security rileva un exploit registra una voce contenente informazioni sull'exploit e aggiunge le informazioni sull'exploit all'elenco delle minacce attive.

Visualizzare il rapporto Prevenzione Exploit

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.

   Verrà visualizzata la finestra **Rapporti**.

2. Aprire la scheda **Prevenzione Exploit**.

Motore di Remediation

Motore di Remediation consente a Kaspersky Endpoint Security di eseguire il rollback delle azioni eseguite dal malware nel sistema operativo.

Durante il rollback dell'attività malware nel sistema operativo, Kaspersky Endpoint Security gestisce i seguenti tipi di attività malware:

- **Attività dei file**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Elimina i file eseguibili creati da un malware (in tutti i supporti ad eccezione delle unità di rete).
  - Elimina i file eseguibili creati da programmi che sono stati infiltrati da malware.
  - Ripristina i file che sono stati modificati o eliminati da un malware.

- **Attività del sistema**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Termina i processi avviati da malware.
  - Termina i processi in cui è penetrata un'applicazione dannosa.
  - Non ripristina i processi che sono stati interrotti da un malware.

- **Attività di rete**

  Kaspersky Endpoint Security esegue le seguenti azioni:

  - Blocca l'attività di rete del malware.

È possibile avviare un rollback delle azioni del malware dal componente Protezione Minacce File o Rilevamento del Comportamento oppure durante una scansione malware.

Il rollback delle operazioni malware influisce su un set di dati rigorosamente definito. Il rollback non ha effetti negativi sul sistema operativo o sull'integrità dei dati del computer.

Abilitare/disabilitare Motore di Remediation in Administration Console

1. Avviare Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.

4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà** selezionare **Protezione minacce avanzata** > **Motore di Remediation**.
7. Selezionare o deselezionare la casella di controllo **Abilita Motore di Remediation**.
8. Fare clic su **OK** per salvare le modifiche.
9. Per applicare le modifiche al criterio eseguire una delle seguenti operazioni:
   - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.
   - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.

Abilitare/disabilitare Motore di Remediation utilizzando Web Console

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare alla sezione **Protezione minacce host** → **Analisi del comportamento** → **Motore di Remediation**.
5. Abilitare o disabilitare il componente utilizzando l'interruttore **Motore di Remediation**.
6. Salvare le modifiche.

Abilitare/disabilitare Motore di Remediation nell'interfaccia dell'applicazione

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.
   Verrà visualizzata la finestra delle impostazioni dell'applicazione.
2. Nella sezione **Avanzate** della scheda **Motore di Remediation** selezionare o deselezionare la casella di controllo **Abilita Motore di Remediation**.

Di conseguenza, se Motore di Remediation è abilitato, Kaspersky Endpoint Security eseguirà il rollback delle azioni intraprese dalle applicazioni dannose nel sistema operativo.

Controllo Web

Controllo Web gestisce l'accesso degli utenti alle risorse Web. Questo aiuta a ridurre il traffico e l'utilizzo inappropriato dell'orario di lavoro. Quando un utente tenta di aprire un sito Web limitato da Controllo Web, Kaspersky Endpoint Security blocca l'accesso o visualizza un avviso.

È possibile bloccare l'accesso a siti Web specifici o a categorie selezionate di siti Web.

Nota: L'applicazione Kaspersky Endpoint Security può bloccare l'accesso solo ai siti Web che utilizzano HTTPS per le connessioni. L'applicazione esegue la scansione delle connessioni criptate (HTTPS) solo se è selezionata la casella di controllo **Controlla connessioni protette (HTTPS)** nella sezione **Essenziale** della scheda **Generale**.

Aggiungere una nuova regola in Administration Console

1. Avviare Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà** selezionare **Controlli di sicurezza** > **Controllo Web**.
7. Selezionare la casella di controllo **Abilita Controllo Web**.
8. Fare clic su **Aggiungi**.
9. Nella finestra visualizzata immettere un nome per la regola.
10. Se si desidera che la regola sia attiva, selezionare la casella di controllo **Regola attiva**.
11. Eseguire una delle seguenti operazioni:
    - Se si desidera che la regola venga applicata a indirizzi Web specifici, selezionare l'opzione **Indirizzo Web o gruppo di indirizzi Web in base alla maschera**.
    - Se si desidera che la regola venga applicata a categorie di siti Web specifiche, selezionare l'opzione **Categorie di siti Web**.
12. Fare clic su **Specifica**.
13. Nella finestra visualizzata specificare l'ambito della regola.
14. Eseguire una delle seguenti operazioni:
    - Se si desidera che Kaspersky Endpoint Security blocchi l'accesso, selezionare l'opzione **Blocca**.
    - Se si desidera che Kaspersky Endpoint Security consenta l'accesso, selezionare l'opzione **Consenti**.
    - Se si desidera che Kaspersky Endpoint Security visualizzi un avviso, selezionare l'opzione **Mostra avviso**.
15. Fare clic su **OK** per salvare le modifiche.

16. Per applicare le modifiche al criterio eseguire una delle seguenti operazioni:

    - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.
    - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.

Aggiungere una nuova regola in Web Console

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Accedere a **Controlli di sicurezza** → **Controllo Web**.
5. Attivare l'interruttore **Controllo Web**.
6. Fare clic su **Aggiungi**.
7. Nella finestra visualizzata immettere un nome per la regola.
8. Eseguire una delle seguenti operazioni:

    - Se si desidera che la regola sia attiva, selezionare l'opzione **Attiva**.
    - Se si desidera che la regola non sia attiva, selezionare l'opzione **Inattiva**.
9. Eseguire una delle seguenti operazioni:

    - Se si desidera che Kaspersky Endpoint Security consenta l'accesso, selezionare l'opzione **Consenti**.
    - Se si desidera che Kaspersky Endpoint Security blocchi l'accesso, selezionare l'opzione **Blocca**.
    - Se si desidera che Kaspersky Endpoint Security visualizzi un avviso, selezionare l'opzione **Mostra avviso**.
10. Eseguire una delle seguenti operazioni:

    - Se si desidera che la regola venga applicata a categorie di siti Web specifiche, selezionare l'opzione **Categorie** e fare clic su **Seleziona categorie** per selezionare le categorie.
    - Se si desidera che la regola venga applicata a indirizzi Web specifici, selezionare l'opzione **Indirizzi singoli** e aggiungerli alla tabella seguente.
11. Salvare le modifiche.

Nota: Non è possibile gestire le impostazioni di Controllo Web nell'applicazione Kaspersky Endpoint Security.

Controllo dispositivi

Controllo dispositivi gestisce l'accesso degli utenti ai dispositivi installati o connessi al computer. Ciò consente di proteggere il computer dalle infezioni quando vengono collegati tali dispositivi e impedire perdite o fughe di dati.

Livelli di accesso ai dispositivi

Controllo dispositivi controlla l'accesso ai seguenti livelli:

- **Tipo di dispositivo**. È possibile controllare l'accesso a dischi rigidi, dischi rimovibili, floppy disk, unità CD/DVD e alle reti Wi-Fi.

  È possibile configurare l'accesso ai dispositivi come segue:

  - Consenti.
  - Blocca.
  - Blocca con eccezioni (solo Wi-Fi).

- **Dispositivi attendibili.** I dispositivi attendibili sono dispositivi a cui gli utenti specificati nelle impostazioni del dispositivo attendibile hanno sempre accesso completo.

  È possibile aggiungere dispositivi attendibili in base ai seguenti dati:

  - **Dispositivi in base all'ID**. Ogni dispositivo dispone di un ID univoco (ID hardware o HWID). È possibile visualizzare l'ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. Esempio di ID dispositivo: SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000. L'aggiunta di dispositivi in base all'ID è utile se si desidera aggiungere diversi dispositivi specifici.
  - **Dispositivi in base al modello**. Ogni dispositivo ha un ID fornitore (VID) e un ID prodotto (PID). È possibile visualizzare gli ID nelle proprietà del dispositivo utilizzando gli strumenti del sistema operativo. Modello per l'immissione di VID e PID: VID_1234&PID_5678. L'aggiunta di dispositivi in base al modello è utile se si utilizzano dispositivi di un determinato modello nell'organizzazione. In questo modo è possibile aggiungere tutti i dispositivi di questo modello.
  - **Dispositivi in base alla maschera ID**. Se si utilizzano più dispositivi con ID simili, è possibile aggiungere dispositivi all'elenco dei dispositivi attendibili utilizzando le maschere. Il carattere `*` sostituisce qualsiasi set di caratteri. Kaspersky Endpoint Security non supporta il carattere `?` quando si immette una maschera. Ad esempio, `WDC_C*`.
  - **Dispositivi in base alla maschera del modello**. Se si utilizzano più dispositivi con VID o PID simili (ad esempio dispositivi dello stesso produttore), è possibile aggiungere dispositivi all'elenco dei dispositivi attendibili utilizzando le maschere. Il carattere `*` sostituisce qualsiasi set di caratteri. Kaspersky Endpoint Security non supporta il carattere `?` quando si immette una maschera. Ad esempio, `VID_05AC&PID_*`.

Gestire il componente Controllo dispositivi in Administration Console

1. Avviare Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Nell'area di lavoro selezionare la scheda **Criteri**.
5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.
6. Nella finestra **Proprietà**, selezionare **Controlli di sicurezza** > **Controllo dispositivi**.
7. Selezionare la casella di controllo **Abilita Controllo dispositivi**.
8. Nella scheda **Tipi di dispositivi** configurare le regole di accesso per i tipi di dispositivi e le reti Wi-Fi.
9. Nella scheda **Dispositivi attendibili** configurare le regole di accesso per i singoli dispositivi o i gruppi di dispositivi.
10. Fare clic su **OK** per salvare le modifiche.
11. Per applicare le modifiche al criterio eseguire una delle seguenti operazioni:
    - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.
    - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome criterio>** dopo il salvataggio delle modifiche.

Gestire il componente Controllo dispositivi in Web Console

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Accedere a **Controlli di sicurezza** > **Controllo dispositivi**.
5. Attivare l'interruttore **Controllo dispositivi**.
6. Nella sezione **Impostazioni di Controllo dispositivi** configurare le regole di accesso per dispositivi, tipi di dispositivi e reti Wi-Fi.
7. Salvare le modifiche.

Nota: Non è possibile gestire le impostazioni di Controllo dispositivi nell'applicazione Kaspersky Endpoint Security.

Di conseguenza, se Controllo dispositivi è abilitato, l'applicazione trasmette le informazioni sui dispositivi connessi a Kaspersky Security Center. È possibile visualizzare l'elenco dei dispositivi connessi in Kaspersky Security Center in **Avanzate** → **Archivi** → **cartella Hardware**.

Visualizzare il rapporto Controllo dispositivi

1. Nella barra dei menu scegliere **Protezione** > **Rapporti**.

   Verrà visualizzata la finestra **Rapporti**.

2. Aprire la scheda **Controllo dispositivi**.

Partecipa a Kaspersky Security Network

Quando si partecipa a Kaspersky Security Network, le statistiche dell'applicazione Kaspersky Endpoint Security vengono automaticamente inviate a Kaspersky per ottimizzare la protezione del dispositivo Mac.

Nota: Kaspersky non riceve, elabora o archivia dati personali senza il consenso esplicito dell'utente.

La partecipazione al programma Kaspersky Security Network è facoltativa. La decisione di partecipare viene presa dall'utente durante l'installazione dell'applicazione. Tuttavia, è possibile rivedere tale decisione in qualsiasi momento.

Abilitare Kaspersky Security Network

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Avanzate** della sezione **KSN** fare clic su **Mostra Informativa KSN** per visualizzare l'Informativa sulla raccolta dei dati di KSN.

3. Se si desidera che Kaspersky Endpoint Security utilizzi le informazioni sulla reputazione di file, risorse Web e applicazioni ricevute da Kaspersky Security Network e si accettano tutte le condizioni dell'Informativa, selezionare la casella di controllo **Partecipa a Kaspersky Security Network**.

4. Nella finestra visualizzata fare clic su **Conferma**.

Le caselle di controllo **Partecipa a Kaspersky Security Network** e **Abilita modalità KSN estesa** saranno selezionate.

Nota: per impostazione predefinita, Kaspersky Endpoint Security utilizza la modalità KSN estesa. La *modalità KSN estesa* è una modalità con cui Kaspersky Endpoint Security invia dati aggiuntivi a Kaspersky. Se non si desidera fornire questi dati a Kaspersky, deselezionare la casella di controllo **Abilita modalità KSN estesa**.

Dati forniti a Kaspersky durante l'utilizzo di Kaspersky Security Network

Se la casella di controllo **Partecipa a Kaspersky Security Network** è selezionata e la casella di controllo **Abilita modalità KSN estesa** è deselezionata, Kaspersky Endpoint Security fornisce a Kaspersky i seguenti dati:

- Informazioni sulla licenza utilizzata: tipo di licenza e relativo periodo di validità, numero di giorni restanti prima della scadenza della licenza, identificatore del partner dal quale la licenza è stata acquistata, identificatore del Centro regionale di attivazione, checksum del codice di attivazione, hash del corpo del ticket calcolato tramite l'algoritmo SHA1, data e ora di creazione del ticket di licenza, identificatore dei dati della licenza, identificatore del ticket della licenza, identificatore di sequenza del ticket della licenza, identificatore univoco del computer dell'utente, data di inizio validità del ticket della licenza, data di fine validità del ticket della licenza, stato corrente del ticket della licenza, versione intestazione ticket, versione della licenza, identificatore certificato di firma intestazione ticket, checksum del file chiave, numero di serie firmatario intestazione ticket, token di autenticazione.

- Versione completa del Software installato;
  tipo di software installato;
  ID aggiornamento Software; ID del servizio di reputazione; ID del tipo di protocollo; ID di un centro di attivazione regionale; versione dell'elenco delle decisioni del servizio Software revocato; ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record dei

database anti-virus del Software attivati; ID univoco dell'istanza di installazione dell'applicazione nel computer; data di attivazione della licenza; data di scadenza della licenza; identificatore della licenza; stato della licenza utilizzata dal software; tipo di checksum per l'oggetto elaborato; nome del malware rilevato o del software legittimo che può essere utilizzato per danneggiare i dati o il dispositivo dell'utente; checksum dell'oggetto elaborato; checksum del codice di attivazione del Software; versione completa del software; ID dispositivo univoco; ID Software; checksum del file chiave del Software; ID del modello di informazioni utilizzato per fornire la licenza Software; identificatore del certificato utilizzato per accedere all'intestazione del ticket della licenza Software; data e ora di creazione del ticket di licenza Software; checksum del ticket di licenza Software; versione del ticket di licenza Software; versione del codice di attivazione del Software; formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; ID ticket licenza corrente; ID componente Software; risultato dell'azione del Software; codice errore; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); numero di porta; indirizzo Web dell'origine della richiesta del servizio Web (Referrer); chiave pubblica del certificato; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash.

Se le caselle di controllo **Partecipa a Kaspersky Security Network** e **Abilita modalità KSN estesa** sono selezionate, Kaspersky Endpoint Security fornisce a Kaspersky i seguenti dati:

- Informazioni sulla versione del sistema operativo (OS) e dei service pack installati sul computer, sulla versione e sui checksum (MD5, SHA2-256, SHA1) del file kernel del sistema operativo e sui parametri della modalità di esecuzione del sistema operativo; versione del sistema operativo, numero build del sistema operativo, numero di aggiornamento del sistema operativo, edizione del sistema operativo, informazioni estese sull'edizione del sistema operativo; versione Service Pack del sistema operativo; data e ora di avvio del sistema operativo; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di analisi comportamentale; numero di eventi azione del sistema operativo del tipo corrente ritardati; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di difesa proattiva; numero di eventi azione del sistema operativo elaborati; numero di eventi azione del sistema operativo sincroni elaborati; ritardo totale di tutti gli eventi azione del sistema operativo del tipo corrente; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di archiviazione degli eventi persistenti; ritardo totale di tutti gli eventi azione del sistema operativo; numero di eventi azione del sistema operativo sincroni in attesa; data e ora dell'evento ricevuto di un'azione nel sistema operativo.

- Informazioni sull'ultimo riavvio non riuscito del sistema operativo: numero di riavvii non riusciti.

- Informazioni sull'applicazione installata dal Titolare dei diritti e sullo stato della protezione anti-virus: ID installazione Software (PCID); versione del record del database del Software; identificativo univoco dell'istanza di installazione dell'applicazione sul computer, tipo di applicazione, ID del tipo di applicazione, versione completa dell'applicazione installata, identificativo della versione delle impostazioni dell'applicazione, identificativo del tipo di computer, identificativo univoco del computer su cui è installata l'applicazione, identificativo univoco dell'Utente nei servizi del Titolare dei diritti, lingua locale e stato operativo, versione dei componenti del Software installato e relativo stato operativo, versione del protocollo utilizzato per connettersi ai servizi del Titolare dei diritti. versione completa del Software installato; tipo di software installato; ID aggiornamento Software; ID del servizio di reputazione; ID del tipo di protocollo; ID di un centro di attivazione regionale; versione dell'elenco delle decisioni del servizio Software revocato; ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record dei database anti-virus del Software attivati; ID univoco dell'istanza di installazione dell'applicazione nel computer; data di attivazione della licenza; data di scadenza della licenza; identificatore della licenza; stato della licenza utilizzata dal software; tipo di checksum per l'oggetto elaborato; nome del malware rilevato o del software legittimo che può essere utilizzato per danneggiare i dati o il dispositivo dell'utente; checksum dell'oggetto elaborato; checksum del codice di attivazione del Software; versione completa del software; ID Software; checksum del file chiave del Software; ID del modello di informazioni utilizzato per fornire la licenza Software; identificatore del certificato utilizzato per accedere all'intestazione del ticket della licenza Software; data e ora di creazione del ticket di licenza Software; checksum del ticket di licenza Software; versione del ticket di licenza Software; versione del codice di attivazione del Software; formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; ID ticket licenza corrente; ID componente Software; risultato dell'azione del Software; codice errore; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); numero di porta; indirizzo Web dell'origine della richiesta del servizio Web (Referrer); numero di cicli di applicazione degli aggiornamenti per i database anti-virus; data e ora dell'ultimo aggiornamento e dell'applicazione dei database anti-virus; data e ora di rilascio dei database del Software; versione del componente del Software; ID aggiornamento Software; tipo di software installato; data e ora di avvio di Controllo sistema; data e ora di installazione del Software; probabilità di invio statistiche da parte di Controllo sistema; codice dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; tempo di elaborazione del database dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; tempo massimo consentito per l'elaborazione di un evento da parte di Controllo sistema; tempo di elaborazione dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; numero totale di eventi che hanno richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema.

- Informazioni su tutti gli oggetti elaborati e sulle operazioni: verdetto del Software sull'oggetto elaborato; codice directory; dimensioni dell'oggetto elaborato; checksum (SHA256) dell'oggetto elaborato; numero del software rilevato nel contesto Controllo sistema; data e ora di rilevamento del software da parte di Controllo sistema; caratteristiche di rilevamento; ID del record attivato nei database anti-virus del Software; motivo del rilevamento del software da parte di Controllo sistema; checksum (MD5) dell'oggetto elaborato; risultato del controllo dell'integrità del modulo; nome dell'oggetto elaborato; tipo di record dei database anti-virus del Software attivati; percorso dell'oggetto elaborato; nome dell'oggetto esaminato; data e ora della scansione; URL e indirizzi Referrer da cui è stato scaricato; dimensioni dei file esaminati e dei relativi percorsi; segno dell'archivio; data e ora di creazione del file; nome, dimensioni e checksum (MD5, SHA2-256) dello strumento di creazione dei pacchetti (se il file è stato compresso); l'entropia del file; tipo di file; codice del tipo di file; formato, ID e segno del file eseguibile; checksum dell'oggetto (MD5, SHA2-256); tipo e il valore del checksum supplementare dell'oggetto; dati relativi alla firma digitale dell'oggetto (certificato): dati sull'entità di pubblicazione del certificato, numero di avvii dell'oggetto dall'ultimo invio di dati statistici, ID dell'attività di scansione dell'applicazione, modalità di ricezione delle informazioni sulla reputazione dell'oggetto, valore del filtro di destinazione, parametri tecnici delle tecnologie di rilevamento applicabili; percorso dell'oggetto elaborato; codice directory.

- Per i file eseguibili: entropia delle sezioni dei file, flag di verifica della reputazione o flag di firma del file, nome, tipo, ID, checksum (MD5) e dimensione dell'applicazione caricata dall'oggetto in fase di convalida, percorso dell'applicazione e percorsi del template, attributo indicante la presenza nell'elenco di esecuzione automatica, data di inserimento, elenco di attributi, nome dello strumento di creazione dei pacchetti, informazioni sulla firma digitale dell'applicazione: certificato dell'autore, nome del file caricato nel formato MIME, data e ora di compilazione del file.

- Informazioni sulle applicazioni avviate e sui rispettivi moduli: checksum (MD5, SHA2-256) dei file in esecuzione, dimensioni, attributi, data di creazione, nome dello strumento di creazione dei pacchetti (se il file è stato inserito in un pacchetto), nomi dei file, informazioni sui processi in esecuzione nel sistema (ID processo (PID), nome processo, informazioni sull'account da cui è stato avviato il processo, l'applicazione e il comando che hanno avviato il processo, percorso completo dei file del processo e riga di comando iniziale, descrizione dell'applicazione alla quale appartiene il processo (nome dell'applicazione e informazioni sull'autore), certificati digitali utilizzati e informazioni necessarie per verificarne l'autenticità o informazioni sull'assenza della firma digitale di un file), nonché informazioni sui moduli caricati nei processi: nome, dimensione, tipo, data di creazione, attributi, checksum (MD5, SHA2-256, SHA1), percorsi, informazioni sull'intestazione dei file PE, nomi degli strumenti di creazione dei pacchetti (se il file è stato inserito in un pacchetto), informazioni sulla disponibilità e la validità di queste statistiche e ID della modalità utilizzata per generare le statistiche inviate.

- Se vengono identificate minacce o vulnerabilità, oltre alle informazioni sull'oggetto rilevato verranno fornite informazioni sull'identificatore, sulla versione e sul tipo di record nel database anti-virus, il nome della minaccia in base alla classificazione Kaspersky, la data e l'ora dell'ultimo aggiornamento del database anti-virus, il nome del file eseguibile, il checksum (MD5) del file dell'applicazione che ha richiesto l'URL in cui è stata rilevata la minaccia, l'indirizzo IP (IPv4 o IPv6) della minaccia rilevata, l'identificatore della vulnerabilità e il livello della minaccia, l'URL e il Referrer della pagina Web in cui è stata rilevata la vulnerabilità.

- Se viene rilevato un oggetto potenzialmente dannoso, le relative informazioni sui dati vengono trasmesse nella memoria dei processi.

- Informazioni sugli attacchi di rete: indirizzo IP del computer da cui proviene l'attacco e numero della porta nel computer dell'utente interessata dall'attacco di rete, ID del protocollo di attacco, nome e tipo di attacco.

- Informazioni sulle connessioni di rete: la versione e i checksum (MD5, SHA2-256, SHA1) del file da cui il processo è stato avviato che ha aperto la porta, il percorso del file del processo e la sua firma digitale, gli indirizzi IP locale e remoto, i numeri delle porte di connessione locali e remote, lo stato di connessione, il timestamp dell'apertura della porta.

- L'URL e l'indirizzo IP della pagina web su cui è stato rilevato il contenuto dannoso o sospetto, il nome, la dimensione e il checksum del file che ha richiesto l'URL, il codice identificativo, il peso e il grado della regola impiegata per raggiungere il verdetto, l'oggetto dell'attacco.

- Informazioni sugli aggiornamenti dell'applicazione installata e dei database anti-virus: stato di completamento dell'attività di aggiornamento, tipo di errore che potrebbe essersi verificato durante il processo di aggiornamento, numero di aggiornamenti non riusciti e identificatore del componente dell'applicazione che esegue gli aggiornamenti.

- Informazioni sull'utilizzo di Kaspersky Security Network (KSN): identificatore KSN, identificatore dell'applicazione, versione completa dell'applicazione, indirizzo IP depersonalizzato del dispositivo dell'Utente, indicatori della qualità di adempimento delle richieste KSN, indicatori della qualità di elaborazione dei pacchetti KSN, indicatori del numero di richieste KSN e informazioni sui tipi di richieste KSN, data e ora di inizio e fine dell'invio delle statistiche; Informazioni sugli aggiornamenti della configurazione KSN: identificatore della configurazione attiva, identificatore della configurazione ricevuta, codice di errore dell'aggiornamento della configurazione.

- Informazioni sugli eventi del registro di sistema: ora dell'evento, nome del registro in cui è stato rilevato l'evento, tipo e categoria dell'evento, nome dell'origine dell'evento e descrizione dell'evento.

- Informazioni per determinare la reputazione dei file e gli indirizzi URL: l'indirizzo URL a cui si chiede la reputazione e il Referrer, il tipo di protocollo della connessione, l'ID interno del tipo di applicazione, il numero della porta in uso, l'ID Utente, il checksum del file analizzato (MD5), il tipo di minaccia rilevata e le informazioni sul registro utilizzato per rilevare una minaccia (l'identificatore del registro per il database anti-virus, il tipo e la marca temporale); chiave pubblica del certificato; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash.

- Dati sulla distribuzione territoriale dell'applicazione: data di installazione e attivazione dell'applicazione, ID del partner che fornisce la licenza per l'attivazione dell'applicazione, ID dell'applicazione, ID localizzazione lingua applicazione, numero di serie della licenza di attivazione dell'applicazione, indicazione di partecipazione a KSN.

- Informazioni sulla licenza utilizzata: tipo di licenza e relativo periodo di validità, numero di giorni restanti prima della scadenza della licenza, identificatore del partner dal quale la licenza è stata acquistata, identificatore del Centro regionale di attivazione, checksum del codice di attivazione, hash del corpo del ticket calcolato tramite l'algoritmo SHA1, data e ora di creazione del ticket di licenza, identificatore dei dati della licenza, identificatore del ticket della licenza, identificatore di sequenza del ticket della licenza, identificatore univoco del computer dell'utente, data di inizio validità del ticket della licenza, data di fine validità del ticket della licenza, stato corrente del ticket della licenza, versione intestazione ticket, versione della licenza, identificatore certificato di firma intestazione ticket, checksum del file chiave, numero di serie firmatario intestazione ticket, token di autenticazione.

- - Informazioni sull'hardware installato nel computer; tipo, nome, nome del modello, versione firmware, parametri dei dispositivi integrati e collegati.

- Informazioni su dispositivo: ID dispositivo.

- Informazioni sul funzionamento del componente Controllo Web:
versione del componente, motivo della categorizzazione, informazioni aggiuntive sul motivo della categorizzazione, URL categorizzato, indirizzo IP host dell'oggetto bloccato/categorizzato.

Nota: in base alle impostazioni di Kaspersky Security Center, è possibile partecipare a Kaspersky Private Security Network anziché a Kaspersky Security Network. Kaspersky Endpoint Security invia una notifica quando passa da Kaspersky Private Security Network a Kaspersky Security Network e richiede all'utente di accettare i termini dell'Informativa su Kaspersky Security Network. Per informazioni dettagliate sulla partecipazione a Kaspersky Private Security Network, vedere la Guida di Kaspersky Security Center.

Infrastruttura di Kaspersky Security Network

Kaspersky Endpoint Security supporta le seguenti soluzioni infrastrutturali di Kaspersky Security Network:

- *KSN Globale* è la soluzione utilizzata dalla maggior parte delle applicazioni Kaspersky. I partecipanti a KSN ricevono informazioni da Kaspersky Security Network e inviano a Kaspersky informazioni sugli oggetti rilevati nel computer dell'utente che devono essere sottoposti a ulteriori analisi da parte degli analisti di Kaspersky e inclusi nei database statistici e di reputazione di Kaspersky Security Network.

- *KSN Privato* è una soluzione che consente agli utenti dei computer che ospitano Kaspersky Endpoint Security o altre applicazioni Kaspersky di ottenere l'accesso ai database di reputazione di Kaspersky Security Network e ad altre statistiche senza inviare i dati a Kaspersky Security Network dai propri computer. KSN Privato è progettato per i clienti aziendali che non sono in grado di partecipare a Kaspersky Security Network per uno dei seguenti motivi:

  - Le workstation locali non sono connesse a Internet.

  - La trasmissione dei dati al di fuori del paese o al di fuori della LAN aziendale è vietata dalla legge o limitata dai criteri di protezione aziendali.

Per impostazione predefinita, Kaspersky Security Center utilizza KSN Globale. È possibile configurare l'utilizzo di KSN Privato in Kaspersky Security Center Administration Console (MMC) e Kaspersky Security Center Web Console. Non è possibile configurare l'utilizzo di KSN Privato in Kaspersky Security Center Cloud Console.

Proxy KSN

I computer gestiti da Kaspersky Security Center Administration Server possono interagire con Kaspersky Security Network tramite il servizio proxy KSN.

Il servizio proxy KSN offre le seguenti funzionalità:

- Il computer dell'utente può interrogare KSN e inviare informazioni a KSN anche senza l'accesso diretto a Internet.
- Il servizio proxy KSN memorizza nella cache i dati elaborati, riducendo così il carico sul canale di comunicazione di rete esterno e accelerando la ricezione delle informazioni richieste dal computer dell'utente.

Per ulteriori informazioni sul servizio proxy KSN, consultare la Guida di Kaspersky Security Center.

Nota: Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Verificare l'integrità dei componenti dell'applicazione

Kaspersky Endpoint Security contiene vari moduli binari sotto forma di librerie di collegamento dinamico, file eseguibili, file di configurazione e file di interfaccia. Utenti malintenzionati potrebbero sostituire uno o più file o moduli eseguibili dell'applicazione con altri file contenenti codice dannoso. Per impedirlo, Kaspersky Endpoint Security è in grado di verificare l'integrità dei componenti dell'applicazione. L'applicazione controlla i moduli e i file per rilevare eventuali modifiche non autorizzate o file danneggiati. Se il file o il modulo di un'applicazione contiene un checksum non corretto, viene considerato danneggiato. L'applicazione controlla i moduli e i file per rilevare eventuali modifiche non autorizzate o file danneggiati. Se il file o il modulo di un'applicazione contiene un checksum non corretto, viene considerato danneggiato.

L'integrità dei componenti dell'applicazione viene verificata utilizzando l'utilità integrity_checker disponibile nella directory /Library/Application Support/Kaspersky Lab/KAV/Binaries. Questa utility verifica l'integrità del file manifesto contenente un elenco dei file dell'applicazione la cui integrità è fondamentale per il corretto funzionamento del componente dell'applicazione.

Il file manifesto integrity_check.xml, protetto dalla firma crittografica di Kaspersky, si trova nella stessa directory dell'utility integrity_checker (/Library/Application Support/Kaspersky Lab/KAV/Binaries).

Nota: sono necessari i privilegi dell'account utente root per eseguire l'utility integrity_checker.

È possibile eseguire il controllo integrità utilizzando l'utility installata insieme all'applicazione o utilizzando l'utility in un CD certificato.

Per verificare l'integrità dei componenti dell'applicazione, eseguire il comando seguente:

```
sudo "/Library/Application Support/Kaspersky Lab/KAV/Binaries/integrity_checker"
```

Per impostazione predefinita, l'utility utilizza il file integrity_check.xml che si trova nella directory /Library/Application Support/Kaspersky Lab/KAV/Binaries.

Per visualizzare la Guida per le impostazioni dell'utility, eseguire il seguente comando:

```
--help
```

Il risultato del controllo di ciascun file manifesto viene visualizzato accanto al nome del file manifesto nel seguente formato:

- `SUCCEEDED`: l'integrità dei file è confermata (il codice restituito è `0`)
- `FAILED`: l'integrità dei file non è confermata (il codice restituito è diverso da `0`)

Gestire l'applicazione tramite Kaspersky Security Center Administration Console

Kaspersky Security Center è progettato per la gestione centralizzata della sicurezza della rete aziendale. Per informazioni dettagliate su Kaspersky Security Center, vedere la Guida di Kaspersky Security Center.

È inoltre possibile gestire Kaspersky Endpoint Security tramite l'interfaccia utente grafica dell'applicazione, Kaspersky Security Center Web Console e Cloud Console e la riga di comando.

Distribuire Kaspersky Endpoint Security in una rete aziendale

1. Distribuire *Administration Server* nella rete.

   Administration Server è un componente di Kaspersky Security Center che consente di archiviare in modo centralizzato le informazioni su tutte le applicazioni Kaspersky installate all'interno della rete aziendale e di gestire tali applicazioni.

2. Installare *Administration Console* nella workstation dell'amministratore di Kaspersky Security Center.

   Administration Console è un componente di Kaspersky Security Center che offre un'interfaccia utente per i servizi amministrativi di Administration Server e *Network Agent*. Network Agent coordina l'interazione tra Administration Server e Kaspersky Endpoint Security installati nei computer all'interno della rete aziendale.

3. Installare il plug-in di amministrazione di Kaspersky Endpoint Security nella workstation dell'amministratore di Kaspersky Security Center.

   Un *plug-in di amministrazione* è un componente dedicato che fornisce un'interfaccia per la gestione delle applicazioni Kaspersky tramite Administration Console. Ogni applicazione dispone del proprio plug-in di amministrazione. Il plug-in di amministrazione viene fornito per tutte le applicazioni Kaspersky che possono essere gestite da Kaspersky Security Center.

4. Installare Network Agent nei computer Mac remoti in uno dei seguenti modi:

   - In locale
   - Utilizzo in remoto di Apple Remote Desktop
   - In remoto tramite Kaspersky Security Center
   - In remoto utilizzando il protocollo SSH

   Nota: per gestire Kaspersky Endpoint Security for Mac 12.2.1 tramite Kaspersky Security Center, è necessario installare Network Agent versione 15 nei computer remoti.

5. Installare Kaspersky Endpoint Security nei computer Mac remoti in uno dei seguenti modi:

   - In locale
   - Utilizzo in remoto di Apple Remote Desktop
   - In remoto utilizzando il protocollo SSH
   - In remoto tramite Kaspersky Security Center

   Importante: se Kaspersky Internet Security for Mac o un software anti-malware di terze parti è installato nei computer remoti, disinstallarlo prima di installare Kaspersky Endpoint Security.

Per informazioni dettagliate su come distribuire Administration Server e installare Administration Console, vedere la Guida di Kaspersky Security Center.

Aggiornare Kaspersky Endpoint Security 11.1 o versione successiva alla versione 12.2.1

Nota: per gestire Kaspersky Endpoint Security for Mac 12.2.1 tramite Kaspersky Security Center, è necessario installare Network Agent versione 15 nei computer remoti.

È possibile aggiornare Kaspersky Endpoint Security gestito tramite Kaspersky Security Center 11.1 o versione successiva alla versione 12.2.1 in uno dei seguenti modi:

- Aggiornare contemporaneamente Kaspersky Endpoint Security alla versione 12.2.1 e Network Agent alla versione 15 nei computer remoti.
- Aggiornare prima Network Agent alla versione 15, quindi aggiornare Kaspersky Endpoint Security alla versione 12.2.1.

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

- Per aggiornare Kaspersky Endpoint Security alla versione 12.2.1, è richiesto macOS 14 o versione successiva.
- Per applicare il nuovo profilo di configurazione è necessario scaricare l'archivio KES_11.3_profile.zip dal sito Web dell'Assistenza tecnica.
- Dopo l'aggiornamento di Kaspersky Endpoint Security alla versione 12.2.1, potrebbero essere visualizzati due elementi Kaspersky Filter e Kaspersky Monitor nelle impostazioni di rete.
- Se si dispone di Kaspersky Endpoint Security 11.0.1 o versione precedente, per aggiornare l'applicazione alla versione 12.2.1, è necessario disinstallare l'applicazione e aggiornare macOS alla versione 14 o successiva. Sarà quindi possibile installare Kaspersky Endpoint Security versione 12.2.1.

Nota: Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Prepararsi all'installazione remota di Kaspersky Endpoint Security

Questa sezione contiene informazioni sull'installazione del plug-in di amministrazione di Kaspersky Endpoint Security nella workstation dell'amministratore di Kaspersky Security Center e sull'installazione di Network Agent nel computer remoto.

L'installazione del plug-in di amministrazione di Kaspersky Endpoint Security e Network Agent è un prerequisito per l'installazione di Kaspersky Endpoint Security tramite Kaspersky Security Center.

Installare il plug-in di amministrazione di Kaspersky Endpoint Security

Il plug-in di amministrazione di Kaspersky Endpoint Security offre un'interfaccia per la gestione di Kaspersky Endpoint Security tramite Administration Console.

Installare il plug-in di amministrazione di Kaspersky Endpoint Security

1. Nella workstation dell'amministratore di Kaspersky Security Center decomprimere l'archivio con i file del pacchetto di installazione di Kaspersky Endpoint Security.
2. Aprire la cartella con i file del pacchetto di installazione di Kaspersky Endpoint Security.
3. Fare doppio clic su klcfginst.exe.

   Verrà avviata l'installazione del plug-in di amministrazione di Kaspersky Endpoint Security.

Importante: prima di installare il plug-in di amministrazione di Kaspersky Endpoint Security, chiudere Administration Console nella workstation dell'amministratore di Kaspersky Security Center.

Installare Network Agent in locale

Network Agent coordina l'interazione tra Administration Server e Kaspersky Endpoint Security installati nei computer all'interno della rete aziendale.

Installare Network Agent in locale

1. Nel computer remoto aprire la cartella con il kit di distribuzione di Network Agent.
2. Aprire il kit di distribuzione di Network Agent (file DMG).

   Verrà visualizzata una finestra con il contenuto del kit di distribuzione.
3. Nella finestra con il contenuto del kit di distribuzione fare doppio clic su **Kaspersky Network Agent**.

4. Confermare che si desidera installare Network Agent facendo clic su **Continua**.
5. Nella finestra **Introduzione** fare clic su **Continua**.
6. Nella finestra **Licenza** leggere il testo del Contratto di licenza con l'utente finale di Network Agent che intercorre tra l'utente e AO Kaspersky Lab: Eseguire le seguenti operazioni:
   - Per accettare tutte le condizioni del contratto e proseguire con l'installazione, fare clic su **Continua**.
   - Per stampare il testo del contratto, fare clic su **Stampa**.
   - Per salvare il contratto come file di testo, fare clic su **Salva**.
7. Nella finestra di conferma eseguire una delle seguenti opzioni:
   - Per procedere con l'installazione di Network Agent, fare clic su **Accetta**.
   - Per tornare al testo del Contratto di licenza con l'utente finale, fare clic su **Leggi licenza**.
   - Per annullare l'installazione, fare clic su **Rifiuta**.
8. Nella finestra **Impostazioni** eseguire le seguenti operazioni:
   a. Nel campo **Server** specificare l'indirizzo IP o il nome DNS del server in cui è installato Kaspersky Security Center.
   b. Nel campo **Porta** specificare il numero di porta per una connessione non crittografata al server.
   c. Nel campo **Porta SSL** specificare il numero di porta per una connessione SSL al server.
   d. Se si desidera avviare Network Agent subito dopo l'installazione, selezionare la casella di controllo **Esegui dopo l'installazione**.

   Se non si desidera utilizzare SSL per la connessione al server, deselezionare la casella **Usa SSL**. Per continuare con l'installazione, fare clic su **Continua**.
9. Nella finestra **Tipo di installazione** leggere le informazioni sul disco in cui verrà installato Network Agent.

   Per installare Network Agent utilizzando le impostazioni consigliate, fare clic su **Installa** e immettere la password dell'amministratore per confermare la scelta.

   Attendere il completamento dell'installazione dei componenti dell'applicazione da parte di Network Agent.
10. Fare clic su **Chiudi** per chiudere il programma di installazione.

Installare Network Agent tramite Apple Remote Desktop

1. In un computer remoto scegliere **menu Apple** > **Impostazioni di Sistema** > **Generale** > **Condivisione**.
2. Selezionare la casella di controllo **Gestione remota**.
3. In un altro Mac che si desidera impostare come server, installare Apple Remote Desktop. Per ulteriori informazioni su Apple Remote Desktop, fare riferimento al Supporto Apple.
4. Aprire Apple Remote Desktop.

5. Nella finestra **Desktop remoto** fare clic su **Scanner** a sinistra e selezionare i dispositivi in cui si desidera installare Network Agent.

6. Fare clic su **Copia**.

7. Fare clic su + e selezionare i file di installazione di Network Agent: il file DMG, il file KUD e il file SH.

8. Nel menu a comparsa **Place items in (Colloca elementi in)** scegliere **Top folder of the disk (Cartella principale del disco)**.

9. Fare clic su **Copia**.

10. Dopo la copia dei file, fare clic su **Unix**.

11. Immettere il seguente comando:

    ```
    cd /;
    ./install.sh --accept_eula -r <indirizzo Administration Server>
    ```

    dove `<indirizzo Administration Server>` è il nome DNS o l'indirizzo IP di Kaspersky Security Center Administration Server.

    Nota: inserendo questo comando si accetta il Contratto di licenza con l'utente finale.

12. Scegliere di eseguire il comando come **Utente** e digitare "root" nel campo.

13. Fare clic su **Invia**.

L'installazione di Network Agent viene avviata nei dispositivi selezionati.

Installare Network Agent tramite Kaspersky Security Center

Kaspersky Security Center installa Network Agent in un computer client utilizzando una connessione SSH.

Prima di installare Network Agent in un computer client, verificare che siano soddisfatte le seguenti condizioni:

- Kaspersky Security Center Administration Server è distribuito nella rete aziendale.
- Administration Console è installata nella workstation dell'amministratore di Kaspersky Security Center.
- L'accesso remoto è abilitato nei computer remoti.
- Nel computer remoto viene creato un account amministratore dedicato che verrà utilizzato per eseguire l'attività di installazione remota. È possibile utilizzare un account di dominio per l'installazione.
- La password sudo è disabilitata per l'account dedicato.

Creare un pacchetto di installazione di Network Agent

1. Avviare Kaspersky Security Center Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nell'albero della console selezionare la cartella **Avanzate** e quindi la sottocartella **Installazione remota** e **Pacchetti di installazione**.

4. Nell'area di lavoro fare clic su **Crea pacchetto di installazione**.

5. Nella finestra **Selezionare il tipo di pacchetto di installazione** fare clic su **Creare un pacchetto di installazione per un'applicazione Kaspersky**.

6. Nella finestra **Definizione del nome del pacchetto di installazione** digitare il nome del nuovo pacchetto di installazione nel campo **Nome** e fare clic su **Avanti**.

7. Nella finestra **Selezione del pacchetto di distribuzione per l'installazione** fare clic su **Sfoglia**.

   Verrà visualizzata la finestra per selezionare un file per la creazione del pacchetto di installazione.

8. Aprire la cartella con i contenuti del pacchetto di installazione di Network Agent e selezionare il file klnagent.kud.

   Nella finestra **Selezione del pacchetto di distribuzione per l'installazione** vengono visualizzati il nome e la versione dell'applicazione da installare in remoto tramite il file aggiunto.

9. Fare clic su **Avanti**.

   Il pacchetto di installazione di Kaspersky Endpoint Security viene creato con le impostazioni specificate.

10. Nell'ultima finestra della procedura guidata fare clic su **Fine** per chiudere la Creazione guidata nuovo pacchetto.

Creare un'attività per l'installazione remota di Network Agent in un computer client

1. Avviare Kaspersky Security Center Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Selezionare la cartella **Attività**.

4. Nell'area di lavoro avviare la Creazione guidata nuova attività facendo clic su **Nuova attività**.

5. Seguire i passaggi della Creazione guidata nuova attività illustrati di seguito per creare un'attività per l'installazione remota di Kaspersky Endpoint Security nel computer client.

Per procedere al passaggio successivo della procedura guidata, fare clic su **Avanti**. Per tornare al passaggio precedente della procedura guidata, fare clic su ←. Per uscire dalla procedura guidata in qualsiasi passaggio, fare clic su **Annulla**.

Nota: l'aspetto dei pulsanti può variare in base alla versione di Windows.

Passaggio 1. Selezionare il tipo di attività

1. Nella finestra **Selezionare il tipo di attività** ingrandire il nodo **Kaspersky Security Center Administration Server**.

2. Selezionare l'attività **Installa l'applicazione in remoto**.

Passaggio 2. Selezionare il pacchetto di installazione

Nella finestra **Selezionare il pacchetto di installazione** eseguire una delle seguenti operazioni:

- Se il pacchetto di installazione di Network Agent con le impostazioni richieste è stato creato precedentemente, selezionarlo nell'elenco dei pacchetti di installazione nella parte superiore della finestra **Selezionare il pacchetto di installazione**.
- Se il pacchetto di installazione richiesto non è ancora stato creato, fare clic su **Nuovo** per avviare la Creazione guidata nuovo pacchetto.

Passaggio 3. Configurare le impostazioni di installazione

Nella finestra **Impostazioni** eseguire le seguenti operazioni:

1. Selezionare la casella di controllo **Utilizzo delle risorse del sistema operativo tramite Administration Server**.
2. Deselezionare tutte le altre caselle di controllo.

Passaggio 4. Selezionare un gruppo di amministrazione a cui aggiungere i computer dopo l'installazione

Nella finestra **Spostare nell'elenco dei dispositivi gestiti** selezionare un gruppo in cui verranno spostati i computer dopo l'installazione, se necessario.

Passaggio 5. Definire la modalità di selezione dei computer client per cui verrà creata l'attività

Nella finestra **Selezionare i dispositivi a cui assegnare l'attività** selezionare il metodo che si desidera utilizzare per specificare i computer client:

- Per scegliere tra i computer rilevati nella rete da Administration Server, selezionare l'opzione **Selezionare i dispositivi della rete rilevati da Administration Server**.
- Per specificare gli indirizzi IP dei computer manualmente o per importare gli indirizzi IP dei computer da un file, selezionare l'opzione **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**.
- Per creare un'attività per una selezione di dispositivi in base a un criterio preimpostato, selezionare l'opzione **Assegnare un'attività a una selezione di dispositivi**.
- Per selezionare i computer da un gruppo di amministrazione specifico, selezionare l'opzione **Assegnare un'attività a un gruppo di amministrazione**.

Passaggio 6. Selezionare i computer client

Nella finestra visualizzata (**Seleziona dispositivi**, **Selezione dispositivi** o **Seleziona gruppo di amministrazione**, a seconda dell'opzione selezionata nel passaggio precedente), selezionare i computer client, specificare gli indirizzi IP dei computer, specificare una selezione di computer o selezionare il gruppo di amministrazione a cui verrà applicata l'attività.

Passaggio 7. Selezionare l'account per l'esecuzione dell'attività

1. Nella finestra **Selezione di un account per l'esecuzione dell'attività** selezionare la casella **Account richiesto (Network Agent non utilizzato)**.
2. Fare clic su **Aggiungi** > **Account**.

   Verrà visualizzata la finestra **Account**.

3. Immettere il nome utente e la password dell'account amministratore dedicato di un computer remoto.

4. Fare clic su **OK**.

Passaggio 8. Configurare la pianificazione attività

1. Nella finestra **Configurare la pianificazione delle attività** selezionare la modalità di avvio nell'elenco a discesa **Avvio pianificato**.

2. Se necessario, configurare l'avvio automatico di un'attività pianificata (specificando la data e l'ora di inizio dell'attività).

3. Se si desidera eseguire attività che l'applicazione non è stata in grado di avviare in base alla pianificazione (ad esempio perché il computer era spento all'ora pianificata), selezionare la casella **Esegui attività non effettuate**.

   Kaspersky Endpoint Security avvia l'attività non appena viene eliminato l'ostacolo che impedisce l'avvio dell'attività.

Passaggio 9. Specificare il nome dell'attività

Nel campo **Nome** della finestra **Definire il nome dell'attività** immettere il nome dell'attività che si intende creare.

Passaggio 10. Completare la creazione dell'attività

Nella finestra **Completare la creazione dell'attività** eseguire le seguenti operazioni:

1. Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella **Esegui l'attività al termine della procedura guidata**.

2. Fare clic su **Fine** per chiudere la procedura guidata.

Installare Network Agent tramite il protocollo SSH

Un modo per installare Network Agent in un computer remoto consiste nell'utilizzo del protocollo SSH.

Accertarsi che i seguenti requisiti siano soddisfatti:

- Kaspersky Security Center Administration Server è distribuito nella rete aziendale.
- Administration Console è installata nella workstation dell'amministratore di Kaspersky Security Center.
- Il pacchetto di installazione di Network Agent viene creato e memorizzato in una cartella condivisa di Administration Server.
- L'accesso remoto è abilitato nel computer remoto.
- L'account del computer utilizzato per installare Network Agent è incluso in sudoers.

Per informazioni dettagliate sui pacchetti di installazione, vedere la Guida di Kaspersky Security Center.

Installare Network Agent tramite il protocollo SSH

1. Avviare il client SSH nella workstation dell'amministratore.

2. Connettersi al computer remoto.

3. Collegare la cartella condivisa di Administration Server come unità di rete nel computer remoto. A tale scopo, immettere i seguenti comandi nel client SSH:

```
mkdir /Volumes/KLSHARE
mount_smbfs //<account amministratore>:<password>@<indirizzo IP Administration Server>/KLSHARE /Volumes/KLSHARE
```

Descrizioni dei parametri:

- `<account amministratore>` – Nome dell'account amministratore in Administration Server.
- `<password>` – Password dell'amministratore in Administration Server.
- `<indirizzo IP di Administration Server>` – indirizzo IP del server che ospita Kaspersky Security Center.

4. Eseguire lo script di installazione. A tale scopo, immettere il seguente comando nel client SSH:

```
cd /Volumes/KLSHARE/<cartella_pacchetto_klnagent>
```

dove `<cartella_pacchetto_klnagent>` è la cartella in cui si trova il pacchetto di installazione di Network Agent.

```
sudo ./install.sh --accept_eula [-r <server>] [-p <numero di porta>] [-s use_ssl 0|1] [-l <numero della porta SSL>] [-x use_proxy 0|1] [-a <proxy>] [-n <nome utente proxy>] [-w <password proxy>]
```

Descrizioni dei parametri:

- `<server>` – Indirizzo IP o nome DNS del server in cui è installato Kaspersky Security Center.
- `<numero di porta>` – Numero della porta che verrà utilizzata per stabilire una connessione non crittografata ad Administration Server. La porta 14000 è utilizzata per impostazione predefinita.
- `use_ssl 0|1` – Parametro che stabilisce se durante la connessione tra Network Agent e Administration Server verrà utilizzata la crittografia. Se il valore è "0", verrà utilizzata una connessione non crittografata. Se il valore è "1", la connessione verrà stabilita tramite il protocollo SSL (valore predefinito).
- `<numero di porta SSL>` – Numero della porta che verrà utilizzata per stabilire una connessione crittografata ad Administration Server utilizzando il protocollo SSL. La porta 13000 è utilizzata per impostazione predefinita.
- `use_proxy 0|1` – Parametro che definisce se durante la connessione a Internet verrà utilizzato un server proxy. Se il valore è "0", non verrà utilizzato un server proxy. Se il valore è "1", la connessione verrà stabilita tramite un server proxy (valore predefinito).
- `<proxy>` – L'indirizzo IP o il nome DNS del server proxy.
- `<nome utente proxy>` – Account utente per la connessione al server proxy.
- `<password proxy>` – Password per la connessione al server proxy.

Importante: sono necessari i diritti di amministratore per l'esecuzione di questo comando.

5. Disconnettere l'unità di rete nel computer remoto. A tale scopo, immettere il seguente comando nel client SSH:

```
umount /Volumes/KLSHARE
```

6. Controllare se Network Agent funziona correttamente nel computer remoto. A tale scopo, immettere i seguenti comandi nel client SSH:

```
cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
sudo ./klnagchk
```

In caso di esito positivo, Network Agent funziona correttamente.

Disinstallare Network Agent in locale

1. Nel computer remoto aprire la cartella con il kit di distribuzione di Network Agent.
2. Aprire il kit di distribuzione di Network Agent (file DMG).

   Verrà visualizzata una finestra con il contenuto del kit di distribuzione.
3. Nella finestra con il contenuto del kit di distribuzione fare doppio clic su **Programma di disinstallazione di Network Agent**.
4. Nella finestra **Introduzione** fare clic su **Continua**.
5. Nella finestra **Informazioni** fare clic su **Disinstalla**.
6. Quando vengono richieste le credenziali di amministratore, immettere il nome e la password dell'amministratore e confermare che si desidera disinstallare Network Agent.

   Viene avviata la disinstallazione di Network Agent.
7. Leggere le informazioni sulla disinstallazione e fare clic su **Fine** per chiudere il programma di disinstallazione.

Network Agent è stato rimosso dal computer remoto.

Gestire Network Agent dalla riga di comando

Questa sezione contiene informazioni su come gestire Network Agent tramite la riga di comando in un computer client.

È possibile interrompere Network Agent e avviarlo nuovamente utilizzando la riga di comando in un computer client.

È inoltre possibile connettere un computer remoto ad Administration Server manualmente utilizzando l'utilità klmover e verificare la connessione tra il computer remoto e Administration Server utilizzando l'utilità klnagchk.

È possibile disinstallare Network Agent.

Avviare/interrompere Network Agent in un computer remoto

È possibile interrompere Network Agent e avviarlo nuovamente in un computer client utilizzando la riga di comando.

Interrompere Network Agent

Nel computer remoto avviare l'utilità launchctl con il comando unload dalla riga di comando.

Sintassi del comando:

```
sudo launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Avviare Network Agent

Nel computer remoto avviare l'utilità launchctl con il comando load dalla riga di comando.

Sintassi del comando:

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

Importante: sono necessari i diritti di amministratore per l'interruzione e l'avvio di Network Agent.

Controllare manualmente la connessione tra un computer client e Administration Server. Utilità klnagchk

Controllare la connessione tra un computer remoto e Administration Server.

Nel computer remoto eseguire l'utilità klnagchk dalla riga di comando.

L'utilità klnagchk è inclusa nel kit di distribuzione di Network Agent.

In seguito all'installazione di Network Agent, l'utilità klnagchk viene collocata nella cartella /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

A seconda dei parametri specificati, l'utilità klnagchk esegue le seguenti operazioni se eseguita dalla riga di comando:

- Visualizza le impostazioni specificate per la connessione tra Network Agent installato nel computer remoto e Administration Server oppure le salva in un file.
- Salva le statistiche di Network Agent (dall'ultimo avvio di Network Agent) e i risultati dell'esecuzione dell'utilità in un file oppure visualizza queste informazioni.
- Prova a stabilire una connessione tra Network Agent e Administration Server.
- Se l'utilità non è in grado di stabilire una connessione, invia un pacchetto ICMP per verificare lo stato del computer in cui è installato Administration Server.

Prima di eseguire l'utilità, accedere a /Library/Application Support/Kaspersky Lab/klnagent/Binaries nella riga di comando.

Sintassi del comando:

```
sudo ./klnagchk [-logfile <nome file>] [-sp] [-savecert <percorso del file di
certificato>] [-restart]
```

Importante: sono necessari i diritti di amministratore per l'esecuzione dell'utilità.

Descrizioni dei parametri

`-logfile <nome del file>` – Salvare le impostazioni della connessione tra Network Agent e Administration Server e i risultati dell'esecuzione dell'utilità in un file. Se questo parametro non è specificato, le impostazioni della connessione al server, i risultati dell'esecuzione e i messaggi di errore vengono visualizzati.

`-sp` – Consente di visualizzare la password per l'autenticazione del server proxy o di salvarla in un file. Questo parametro viene utilizzato se Network Agent si connette ad Administration Server tramite un server proxy. Per impostazione predefinita, questo parametro non viene utilizzato.

`-savecert <nome file>` – Consente di salvare il certificato per l'autenticazione in Administration Server in un file specificato.

`-restart` – Consente di riavviare Network Agent dopo l'interruzione dell'esecuzione dell'utilità.

Esempio:
sudo ./klnagchk -logfile klnagchk.log -sp

Connettere manualmente un computer remoto ad Administration Server. Utilità klmover

Connettere un computer remoto ad Administration Server

Nel computer remoto eseguire l'utilità klmover dalla riga di comando.

L'utilità klmover è inclusa nel pacchetto di installazione di Network Agent.

In seguito all'installazione di Network Agent, l'utilità klmover viene collocata nella cartella /Library/Application Support/Kaspersky Lab/klnagent/Binaries.

A seconda dei parametri specificati, l'utilità klmover esegue le seguenti operazioni se eseguita dalla riga di comando:

- Connette Network Agent ad Administration Server con i parametri specificati.
- Salva i risultati dell'esecuzione dell'utilità in un file o provvede alla relativa visualizzazione.

Prima di eseguire l'utilità, accedere a /Library/Application Support/Kaspersky Lab/klnagent/Binaries nella riga di comando.

Sintassi della riga di comando:

```
sudo ./klmover [-logfile <nome file>] [-address <indirizzo server>] [-pn <numero di
porta>] [-ps <numero di porta SSL>] [-nossl] [-cert <percorso del file di certificato>]
[-silent] [-dupfix]
```

Importante: sono necessari i diritti di amministratore per l'esecuzione dell'utilità.

Descrizioni dei parametri

`-logfile <nome del file>` – Consente di salvare i risultati dell'esecuzione in un file. Se questo parametro non è specificato, i risultati dell'esecuzione e i messaggi di errore vengono visualizzati.

`-address <indirizzo del server>` – Indirizzo utilizzato da Network Agent per connettersi ad Administration Server. È possibile specificare l'indirizzo IP o il nome DNS del server.

Nota: è inoltre possibile utilizzare il comando con questo parametro per modificare l'indirizzo dell'Administration Server a cui sono connessi i computer remoti.

`-pn <numero di porta>` – Numero della porta che verrà utilizzata per stabilire una connessione non crittografata ad Administration Server. La porta 14000 è utilizzata per impostazione predefinita.

`-ps <numero di porta SSL>` – Numero della porta che verrà utilizzata per stabilire una connessione crittografata ad Administration Server tramite il protocollo SSL. La porta 13000 è utilizzata per impostazione predefinita.

`-nossl` – Utilizzare una connessione non crittografata ad Administration Server. Se questo parametro non è specificato, Network Agent stabilirà una connessione sicura ad Administration Server tramite il protocollo SSL crittografato.

`-cert <percorso del file di certificato>` – Utilizzare il file di certificato specificato per l'autenticazione in un nuovo Administration Server. Se questo parametro non è specificato, Network Agent riceverà un certificato alla prima connessione ad Administration Server.

`-silent` – Eseguire l'utilità in modalità automatica.

`-dupfix` – Questo parametro viene utilizzato se Network Agent è stato installato in modo diverso dai metodi descritti in questa Guida, ad esempio, se è stato recuperato da un'immagine del disco in cui è installato Network Agent. Se l'identificazione automatica di Network Agent provoca la duplicazione delle icone del computer originale e degli altri computer in Administration Console, provare a riconnettere i computer duplicati.

Nota: durante l'esecuzione dell'utilità klmover, è consigliabile specificare i valori per tutti i parametri.

Esempio:
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001

Il computer remoto connesso ad Administration Server tramite Network Agent si chiama *computer client*.

Disinstallare Network Agent

Sintassi del comando:

```
sudo '/Library/Application Support/Kaspersky Lab/klnagent/Binaries/UninstallScript'
```

Installare e disinstallare Kaspersky Endpoint Security

Questa sezione descrive l'installazione e la disinstallazione remota di Kaspersky Endpoint Security in un computer client.

È inoltre possibile installare o disinstallare Kaspersky Endpoint Security in locale o tramite Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console.

Installare l'applicazione tramite il protocollo SSH

Prima di installare Kaspersky Endpoint Security in un computer remoto, verificare che siano soddisfatte le seguenti condizioni:

- Kaspersky Security Center Administration Server è distribuito nella rete aziendale.
- Administration Console è installata nella workstation dell'amministratore di Kaspersky Security Center.
- È stato creato un pacchetto di installazione per Kaspersky Endpoint Security che si trova in una cartella condivisa in Administration Server.
- Un file chiave per Kaspersky Endpoint Security viene memorizzato nella cartella condivisa in Administration Server (facoltativo).
- L'accesso remoto è abilitato nel computer remoto.
- L'account del computer utilizzato per installare l'applicazione è incluso in sudoers.

Installare Kaspersky Endpoint Security in un computer client utilizzando il protocollo SSH

1. Avviare il client SSH nella workstation dell'amministratore di Kaspersky Security Center.
2. Connettersi al computer remoto.
3. Collegare la cartella condivisa di Administration Server come unità di rete nel computer remoto. A tale scopo, immettere i seguenti comandi nel client SSH:
   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<account amministratore>:<password>@<indirizzo IP Administration Server>/KLSHARE /Volumes/KLSHARE
   ```
   Descrizioni dei parametri:
   - `<account amministratore>` – Nome dell'account amministratore in Administration Server.
   - `<password>` – Password dell'amministratore in Administration Server.
   - `<indirizzo IP di Administration Server>` – indirizzo IP del server che ospita Kaspersky Security Center.
4. Eseguire lo script di installazione. A tale scopo, immettere i seguenti comandi nel client SSH:
   ```
   cd /Volumes/KLSHARE/<cartella pacchetto KES>
   ./install.sh --accept_eula
   ```

dove `<cartella pacchetto KES>` è la cartella in cui si trova il pacchetto di installazione di Kaspersky Endpoint Security.

Importante: sono necessari i diritti di amministratore per l'esecuzione di questo comando.

5. Disconnettere l'unità di rete nel computer remoto. A tale scopo, immettere il seguente comando nel client SSH:
   `umount /Volumes/KLSHARE`

Installare l'applicazione tramite Kaspersky Security Center

Prima di installare Kaspersky Endpoint Security in un computer client, verificare che siano soddisfatte le seguenti condizioni:

- Kaspersky Security Center Administration Server è distribuito nella rete aziendale.
- Administration Console è installata nella workstation dell'amministratore di Kaspersky Security Center.
- Network Agent è installato nel computer client.
- È stato creato un pacchetto di installazione per Kaspersky Endpoint Security che è archiviato nella cartella condivisa di Administration Server.
- Un file chiave per Kaspersky Endpoint Security viene memorizzato nella cartella condivisa in Administration Server (facoltativo).
- Il computer client viene aggiunto al gruppo di amministrazione **Dispositivi gestiti** in Administration Server (facoltativo).

Per informazioni dettagliate sui gruppi di amministrazione in Administration Server, vedere la Guida di Kaspersky Security Center.

Per installare Kaspersky Endpoint Security in un computer client utilizzando Kaspersky Security Center, è necessario creare e avviare l'attività **Installa l'applicazione in remoto**.

Creare un'attività per l'installazione remota di Kaspersky Endpoint Security in un computer client

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Selezionare la cartella **Attività**.
4. Nell'area di lavoro avviare la Creazione guidata nuova attività facendo clic su **Nuova attività**.
5. Seguire i passaggi della Creazione guidata nuova attività illustrati di seguito per creare un'attività per l'installazione remota di Kaspersky Endpoint Security nel computer client.

Per procedere al passaggio successivo della procedura guidata, fare clic su **Avanti**. Per tornare al passaggio precedente della procedura guidata, fare clic su ←. Per uscire dalla procedura guidata in qualsiasi passaggio, fare clic su **Annulla**.

Nota: l'aspetto dei pulsanti può variare in base alla versione di Windows.

Passaggio 1. Selezionare il tipo di attività

1. Nella finestra **Selezionare il tipo di attività** ingrandire il nodo **Kaspersky Security Center Administration Server**.
2. Selezionare l'attività **Installa l'applicazione in remoto**.

Passaggio 2. Selezionare il pacchetto di installazione

Nella finestra **Selezionare il pacchetto di installazione** eseguire una delle seguenti operazioni:

- Se il pacchetto di installazione di Kaspersky Endpoint Security con le impostazioni richieste è stato creato precedentemente, selezionarlo nell'elenco dei pacchetti di installazione nella parte superiore della finestra **Selezionare il pacchetto di installazione**.
- Se il pacchetto di installazione richiesto non è ancora stato creato, fare clic su **Nuovo** per avviare la Creazione guidata nuovo pacchetto.

Passaggio 3. Installare applicazioni aggiuntive

Nella finestra **Avanzate** selezionare le caselle di controllo **Installa Network Agent con questa applicazione** e **<nome del pacchetto di installazione di Network Agent>** se si desidera installare Network Agent anche nel computer client.

Nota: il pacchetto di installazione per Network Agent deve essere creato preventivamente. Se non è stata creata, fare clic su **Crea** per avviare la Creazione guidata nuovo pacchetto.

Passaggio 4. Configurare le impostazioni di installazione

Nella finestra **Impostazioni** configurare l'installazione remota dell'applicazione.

Passaggio 5. Selezionare un gruppo di amministrazione a cui aggiungere i computer dopo l'installazione

Nella finestra **Spostare nell'elenco dei dispositivi gestiti** selezionare un gruppo in cui verranno spostati i computer dopo l'installazione, se necessario.

Nota: se nel passaggio 3 si seleziona l'installazione di Network Agent, verrà visualizzata la finestra **Sposta nell'elenco dei dispositivi gestiti**.

Passaggio 6. Definire la modalità di selezione dei computer client per cui verrà creata l'attività

Nella finestra **Selezionare i dispositivi a cui assegnare l'attività** selezionare il metodo che si desidera utilizzare per specificare i computer client:

- Per scegliere tra i computer rilevati nella rete da Administration Server, selezionare l'opzione **Selezionare i dispositivi della rete rilevati da Administration Server**.
- Per specificare gli indirizzi IP dei computer manualmente o per importare gli indirizzi IP dei computer da un file, selezionare l'opzione **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**.
- Per creare un'attività per una selezione di dispositivi in base a un criterio preimpostato, selezionare l'opzione **Assegnare un'attività a una selezione di dispositivi**.
- Per selezionare i computer da un gruppo di amministrazione specifico, selezionare l'opzione **Assegnare un'attività a un gruppo di amministrazione**.

Passaggio 7. Selezionare i computer client

Nella finestra visualizzata (**Seleziona dispositivi**, **Selezione dispositivi** o **Seleziona gruppo di amministrazione**, a seconda dell'opzione selezionata nel passaggio precedente), selezionare i computer client, specificare gli indirizzi IP dei computer, specificare una selezione di computer o selezionare il gruppo di amministrazione a cui verrà applicata l'attività.

Passaggio 8. Selezionare l'account per l'esecuzione dell'attività

Nella finestra **Selezione di un account per l'esecuzione dell'attività** selezionare la casella **Nessun account richiesto (Network Agent installato)**.

Si presume che sia stato installato Network Agent prima di avviare questa procedura guidata.

Passaggio 9. Configurare la pianificazione attività

1. Nella finestra **Configurare la pianificazione delle attività** selezionare la modalità di avvio nell'elenco a discesa **Avvio pianificato**.
2. Se necessario, configurare l'avvio automatico di un'attività pianificata (specificando la data e l'ora di inizio dell'attività).
3. Se si desidera eseguire attività che l'applicazione non è stata in grado di avviare in base alla pianificazione (ad esempio perché il computer era spento all'ora pianificata), selezionare la casella **Esegui attività non effettuate**.

   Kaspersky Endpoint Security avvia l'attività non appena viene eliminato l'ostacolo che impedisce l'avvio dell'attività.

Passaggio 10. Specificare il nome dell'attività

Nel campo **Nome** della finestra **Definire il nome dell'attività** immettere il nome dell'attività che si intende creare.

Passaggio 11. Completare la creazione dell'attività

Nella finestra **Completare la creazione dell'attività** eseguire le seguenti operazioni:

1. Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella **Esegui l'attività al termine della procedura guidata**.
2. Fare clic su **Fine** per chiudere la procedura guidata.

L'attività creata viene visualizzata nell'area di lavoro della cartella **Attività**.

Creare pacchetto di installazione

Quando si crea l'attività **Installa l'applicazione in remoto**, è possibile utilizzare un pacchetto di installazione esistente o crearne uno nuovo. Per visualizzare l'elenco dei pacchetti di installazione creati, fare clic su **Avanzate** > **Installazione remota** > **Pacchetti di installazione**.

Creare un pacchetto di installazione in Kaspersky Security Center

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nell'albero della console selezionare la cartella **Avanzate** e quindi la sottocartella **Installazione remota** e **Pacchetti di installazione**.
4. Nell'area di lavoro fare clic su **Crea pacchetto di installazione**.
5. Nella finestra **Selezionare il tipo di pacchetto di installazione** fare clic su **Creare un pacchetto di installazione per un'applicazione Kaspersky**.
6. Nella finestra **Definizione del nome del pacchetto di installazione** digitare il nome del nuovo pacchetto di installazione nel campo **Nome** e fare clic su **Avanti**.
7. Nella finestra **Selezione del pacchetto di distribuzione per l'installazione** fare clic su **Sfoglia**.

   Verrà visualizzata la finestra per selezionare un file per la creazione del pacchetto di installazione.
8. Aprire la cartella con i contenuti del pacchetto di installazione di Kaspersky Endpoint Security e selezionare il file kesmac.kud.

   Nella finestra **Selezione del pacchetto di distribuzione per l'installazione** vengono visualizzati il nome e la versione dell'applicazione da installare in remoto tramite il file aggiunto.
9. Selezionare la casella di controllo **Copia aggiornamenti dall'archivio al pacchetto di installazione** per copiare gli aggiornamenti dell'applicazione dall'archivio di Kaspersky Security Center nel pacchetto di installazione, se necessario, e fare clic su **Avanti**.

   Verrà avviato il caricamento del pacchetto di installazione in Administration Server. Al termine del caricamento, verrà visualizzata la finestra **Tipo di installazione**.
10. Nella finestra **Tipo di installazione**, nella sezione **Pacchetti da installare**, selezionare o deselezionare le caselle accanto ai nomi dei componenti che si desidera ignorare durante l'installazione nel computer client e fare clic su **Avanti**.

    Il pacchetto di installazione di Kaspersky Endpoint Security viene creato con le impostazioni specificate.
11. Nell'ultima finestra della procedura guidata fare clic su **Fine** per completare la Creazione guidata nuovo pacchetto.

Disinstallare l'applicazione tramite Kaspersky Security Center

Prima di rimuovere Kaspersky Endpoint Security da un computer client tramite Kaspersky Security Center, verificare che siano soddisfatte le seguenti condizioni:

- Kaspersky Security Center Administration Server è distribuito nella rete aziendale.
- Administration Console è installata nella workstation dell'amministratore di Kaspersky Security Center.
- Network Agent è installato nel computer client.

Per disinstallare Kaspersky Endpoint Security dal computer client tramite Kaspersky Security Center, è necessario creare e avviare l'attività **Disinstalla l'applicazione in remoto**.

Importante: la rimozione di Kaspersky Endpoint Security da un computer client può comportare il rischio di infezione.

Creare un'attività per la disinstallazione remota di Kaspersky Endpoint Security da un computer client

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Selezionare la cartella **Attività**.
4. Nell'area di lavoro avviare la Creazione guidata nuova attività facendo clic su **Nuova attività**.
5. Seguire i passaggi della Creazione guidata nuova attività illustrati di seguito per creare un'attività per la disinstallazione remota di Kaspersky Endpoint Security dal computer client.

Per procedere al passaggio successivo della procedura guidata, fare clic su **Avanti**. Per tornare al passaggio precedente della procedura guidata, fare clic su ←. Per uscire dalla procedura guidata in qualsiasi passaggio, fare clic su **Annulla**.

Nota: l'aspetto dei pulsanti può variare in base alla versione di Windows.

Passaggio 1. Selezionare il tipo di attività

1. Nella finestra **Selezionare il tipo di attività** ingrandire il nodo **Kaspersky Security Center Administration Server**.
2. Espandere il nodo figlio **Avanzate**.
3. Selezionare l'attività **Disinstalla l'applicazione in remoto**.

Passaggio 2. Selezionare l'applicazione da disinstallare

Nella finestra **Selezionare l'applicazione da disinstallare** selezionare **Disinstalla applicazione supportata da Kaspersky Security Center**.

Passaggio 3. Configurare le impostazioni di disinstallazione

Nella finestra **Impostazioni** eseguire le seguenti operazioni:

1. Nell'elenco a discesa **Applicazione da disinstallare** selezionare **Kaspersky Endpoint Security for Mac 12.2.1**.
2. Fare clic su **Avanti**.
3. Configurare la disinstallazione remota dell'applicazione.

Passaggio 4. Selezione dell'opzione per il riavvio del sistema operativo

Nella finestra **Selezione dell'opzione per il riavvio del sistema operativo** selezionare l'opzione **Non riavviare il dispositivo**.

Passaggio 5. Definire la modalità di selezione dei computer client per cui verrà creata l'attività

Nella finestra **Selezionare i dispositivi a cui assegnare l'attività** selezionare il metodo che si desidera utilizzare per specificare i computer client:

- Per scegliere tra i computer rilevati nella rete da Administration Server, selezionare l'opzione **Selezionare i dispositivi della rete rilevati da Administration Server**.
- Per specificare gli indirizzi IP dei computer manualmente o per importare gli indirizzi IP dei computer da un file, selezionare l'opzione **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**.
- Per creare un'attività per una selezione di dispositivi in base a un criterio preimpostato, selezionare l'opzione **Assegnare un'attività a una selezione di dispositivi**.
- Per selezionare i computer da un gruppo di amministrazione specifico, selezionare l'opzione **Assegnare un'attività a un gruppo di amministrazione**.

Passaggio 6. Selezionare i computer client

Nella finestra visualizzata (**Seleziona dispositivi**, **Selezione dispositivi** o **Seleziona gruppo di amministrazione**, a seconda dell'opzione selezionata nel passaggio precedente), selezionare i computer client, specificare gli indirizzi IP dei computer, specificare una selezione di computer o selezionare il gruppo di amministrazione a cui verrà applicata l'attività.

Passaggio 7. Selezionare l'account per l'esecuzione dell'attività

Nella finestra **Selezione di un account per l'esecuzione dell'attività** selezionare la casella **Nessun account richiesto (Network Agent installato)**.

Si presume che sia stato installato Network Agent prima di avviare questa procedura guidata.

Passaggio 8. Configurare la pianificazione attività

1. Nella finestra **Configurare la pianificazione delle attività** selezionare la modalità di avvio nell'elenco a discesa **Avvio pianificato**.
2. Se necessario, configurare l'avvio automatico di un'attività pianificata (specificando la data e l'ora di inizio dell'attività).
3. Se si desidera eseguire attività che l'applicazione non è stata in grado di avviare in base alla pianificazione (ad esempio perché il computer era spento all'ora pianificata), selezionare la casella **Esegui attività non effettuate**.

   Kaspersky Endpoint Security avvia l'attività non appena viene eliminato l'ostacolo che impedisce l'avvio dell'attività.

Passaggio 9. Specificare il nome dell'attività

Nel campo **Nome** della finestra **Definire il nome dell'attività** immettere il nome dell'attività che si intende creare.

Passaggio 10. Completare la creazione dell'attività

Nella finestra **Completare la creazione dell'attività** eseguire le seguenti operazioni:

1. Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella **Esegui l'attività al termine della procedura guidata**.

2. Fare clic su **Fine** per chiudere la procedura guidata.

L'attività creata viene visualizzata nell'area di lavoro della cartella **Attività**.

Avviare e interrompere l'applicazione tramite Kaspersky Security Center

È possibile avviare o interrompere Kaspersky Endpoint Security in un computer selezionato nell'elenco dei dispositivi gestiti tramite Kaspersky Security Center.

Avviare o interrompere Kaspersky Endpoint Security tramite Kaspersky Security Center

1. Avviare Kaspersky Security Center Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nella struttura della console fare clic su **Dispositivi gestiti**.

4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.

5. Selezionare la scheda **Dispositivi**.

6. Selezionare il computer dall'elenco dei computer client.

7. Aprire la finestra **Proprietà: <Nome computer>** in uno dei seguenti modi:

   - Fare doppio clic sul nome del computer client.

   - Fare clic con il pulsante destro del mouse sul computer client, quindi selezionare **Proprietà** dal menu di scelta rapida.

8. Selezionare la sezione **Applicazioni**.

9. Nell'elenco **Applicazioni Kaspersky installate nel dispositivo** fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida della voce **Kaspersky Endpoint Security for Mac 12.2.1** ed eseguire una delle seguenti operazioni:

   - Per avviare l'applicazione, selezionare la voce **Avvia**.
   - Per interrompere l'applicazione, selezionare la voce **Arresta**.

Importante: in seguito all'interruzione di Kaspersky Endpoint Security, il computer client continua a funzionare in modalità non protetta, che può comportare il rischio di infezione.

Creare e gestire le attività

Questa sezione descrive come utilizzare Kaspersky Security Center per creare e configurare le attività che Kaspersky Endpoint Security esegue in un computer client o in un gruppo di computer.

Un'attività è un set di azioni configurabili che Kaspersky Endpoint Security esegue in un computer client.

In Kaspersky Security Center è possibile creare le seguenti attività:

- Aggiungi chiave
- Scansione rapida
- Rollback
- Scansione
- Aggiornamento

È possibile eseguire le seguenti azioni sulle attività:

- Avviare e interrompere le attività.
- Configurare le impostazioni delle attività.
- Monitorare lo stato di avanzamento di un'attività.
- Copiare e spostare le attività da un gruppo all'altro.
- Eliminare le attività.
- Importare ed esportare le attività.

Per ulteriori informazioni sulle attività, vedere la Guida di Kaspersky Security Center.

Creare le attività

Quando si gestisce Kaspersky Endpoint Security tramite Kaspersky Security Center, è possibile creare i seguenti tipi di attività:

- Attività locali. *Un'attività locale* è un'attività per l'esecuzione in un computer client separato.
- Attività di gruppo. *Un'attività di gruppo* è un'attività per l'esecuzione nei computer in un gruppo di amministrazione.
- Attività per un set arbitrario di computer. È possibile creare un'attività da eseguire in qualsiasi computer indipendentemente dal fatto che questo appartenga a un gruppo di amministrazione o a una selezione di computer.

Creare un'attività locale per un computer client separato

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.
5. Nell'area di lavoro selezionare la scheda **Dispositivi**.
6. Selezionare il computer dall'elenco dei computer client.
7. Aprire la finestra **Proprietà: <Nome computer>** in uno dei seguenti modi:
   - Fare doppio clic sul nome del computer client.
   - Fare clic con il pulsante destro del mouse sul computer client, quindi selezionare **Proprietà** dal menu di scelta rapida.
8. Nella finestra **Proprietà: <Nome computer>** selezionare la sezione **Attività**.

   L'elenco delle attività di sistema e personalizzate per il computer client selezionato verrà visualizzato nell'area di lavoro sulla destra.
9. Fare clic su **Aggiungi** nella parte inferiore dell'area di lavoro.

   Verrà avviata la Creazione guidata nuova attività.
10. Seguire i passaggi della Creazione guidata nuova attività per creare un'attività locale per un computer client separato.

Creare un'attività per i computer client in un gruppo di amministrazione

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.
5. Nell'area di lavoro selezionare la scheda **Attività**.

6. Nell'area di lavoro avviare la Creazione guidata nuova attività facendo clic su **Nuova attività**.

7. Seguire i passaggi della Creazione guidata nuova attività per creare un'attività per i computer client inclusi nel gruppo di amministrazione.

Per informazioni dettagliate su come creare attività di gruppo, vedere la Guida di Kaspersky Security Center.

Creare un'attività per un set arbitrario di computer

1. Avviare Kaspersky Security Center Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nella struttura della console fare clic su **Attività**.

4. Nell'area di lavoro avviare la Creazione guidata nuova attività facendo clic su **Nuova attività**.

5. Seguire i passaggi della Creazione guidata nuova attività per creare un'attività per un set arbitrario di computer.

Per procedere al passaggio successivo della procedura guidata, fare clic su **Avanti**. Per tornare al passaggio precedente della procedura guidata, fare clic su ←. Per uscire dalla procedura guidata in qualsiasi passaggio, fare clic su **Annulla**.

Nota: l'aspetto dei pulsanti può variare in base alla versione di Windows.

Passaggio 1. Selezionare un'applicazione e definire il tipo di attività

1. Nella finestra **Selezionare il tipo di attività** ingrandire il nodo **Kaspersky Endpoint Security for Mac 12.2.1**.

2. Selezionare il tipo di attività che si desidera creare:

   - Per creare un'attività per l'aggiunta di una chiave, selezionare **Aggiungi chiave**.
   - Per creare un'attività di scansione delle aree critiche, selezionare **Scansione rapida**.
   - Per creare un'attività per il rollback dell'aggiornamento più recente, selezionare **Rollback**.
   - Per creare un'attività di scansione anti-malware, selezionare **Scansione**.
   - Per creare un'attività di aggiornamento, selezionare **Aggiornamento**.

Passaggio 2. Configurare le impostazioni per il tipo di attività selezionato

I contenuti della finestra delle impostazioni possono variare a seconda del tipo di attività selezionato durante il passaggio precedente. Questa finestra non viene visualizzata per l'attività di rollback.

Attivazione dell'applicazione

Nella finestra **Attivazione dell'applicazione** eseguire le seguenti operazioni:

1. Selezionare un codice di attivazione o una chiave dall'archivio di Kaspersky Security Center o aggiungere un file chiave archiviato nel computer.

2. Per aggiungere la chiave specificata come chiave di riserva, selezionare la casella **Aggiungi come chiave di riserva**.

   La chiave di riserva diventa attiva allo scadere della chiave attiva corrente.

Le informazioni sulla chiave specificata (chiave, tipo di chiave e data di scadenza della chiave) sono visualizzate nella finestra **Attivazione dell'applicazione**.

Aggiornamento

La principale sorgente degli aggiornamenti per Kaspersky Endpoint Security sono i server degli aggiornamenti dedicati di Kaspersky. Kaspersky Endpoint Security può inoltre utilizzare i punti di distribuzione, le cartelle locali o altri server Web come *sorgente degli aggiornamenti*.

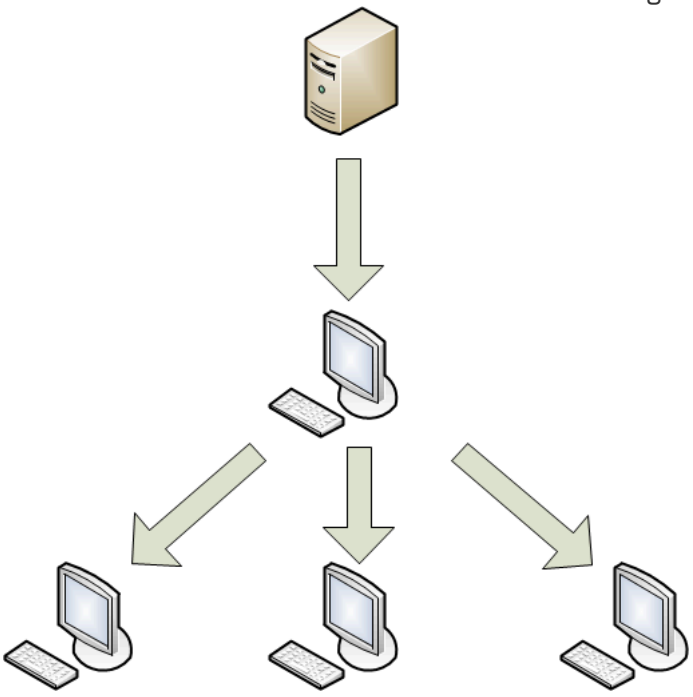
È possibile inserire gli aggiornamenti scaricati in una cartella locale per aggiornare i database dell'applicazione e i moduli di Kaspersky Endpoint Security in altri computer della rete aziendale per ridurre la quantità di traffico Internet.

È possibile configurare la distribuzione degli aggiornamenti come segue:

1. Uno dei computer della rete riceve un pacchetto di aggiornamenti di Kaspersky Endpoint Security dai server degli aggiornamenti di Kaspersky o da una sorgente degli aggiornamenti diversa. Gli aggiornamenti recuperati vengono collocati in una cartella locale condivisa.

   Nota: la cartella locale condivisa deve essere creata in anticipo.

2. Altri computer della rete fanno riferimento alla cartella locale condivisa come sorgente degli aggiornamenti.



Distribuzione degli aggiornamenti tramite un computer locale

Se necessario, modificare le impostazioni dell'attività di aggiornamento nella finestra **Aggiornamento**:

1. Per disabilitare gli aggiornamenti dei moduli dell'applicazione, deselezionare la casella **Aggiorna moduli dell'applicazione**.

2. Per modificare le sorgenti degli aggiornamenti:

   a. Fare clic su **Impostazioni**.

   Verrà visualizzata la finestra **Impostazioni: Aggiornamento**.

   b. Selezionare le caselle accanto alle sorgenti degli aggiornamenti da utilizzare.

3. Per specificare una sorgente degli aggiornamenti diversa, fare clic su **Aggiungi**.

   Verrà visualizzata la finestra **Sorgente degli aggiornamenti**.

   a. Specificare l'indirizzo Web della sorgente degli aggiornamenti o il percorso di una cartella locale o di rete che è una sorgente degli aggiornamenti e fare clic su **OK**.

   b. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Impostazioni: Aggiornamento**.

Scansione e Scansione rapida

Per impostazione predefinita, Kaspersky Endpoint Security utilizza il livello di sicurezza **Consigliato**, richiede all'utente di selezionare un'azione se viene rilevato un oggetto infetto dopo la scansione, ed esamina i seguenti oggetti:

- Tutte le unità rimovibili
- Tutte le unità interne

- Tutte le unità di rete
- Memoria

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Se necessario, modificare le impostazioni di scansione nella finestra **Scansione**:

1. Selezionare uno dei livelli di protezione preimpostati o personalizzare le impostazioni di protezione.
2. Specificare l'azione eseguita da Kaspersky Endpoint Security in caso di rilevamento di un oggetto infetto.
3. Definire un ambito di scansione.

Passaggio 3. Definire la modalità di selezione dei computer client per cui verrà creata l'attività

Nota: questo passaggio non è attinente alle attività di gruppo o locali.

Nella finestra **Selezionare i dispositivi a cui assegnare l'attività** selezionare il metodo che si desidera utilizzare per specificare i computer client:

- Per scegliere tra i computer rilevati nella rete da Administration Server, selezionare l'opzione **Selezionare i dispositivi della rete rilevati da Administration Server**.
- Per specificare gli indirizzi IP dei computer manualmente o per importare gli indirizzi IP dei computer da un file, selezionare l'opzione **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**.
- Per creare un'attività per una selezione di dispositivi in base a un criterio preimpostato, selezionare l'opzione **Assegnare un'attività a una selezione di dispositivi**.
- Per selezionare i computer da un gruppo di amministrazione specifico, selezionare l'opzione **Assegnare un'attività a un gruppo di amministrazione**.

Passaggio 4. Selezionare i computer client

Nota: questo passaggio non è attinente alle attività di gruppo o locali.

Nella finestra visualizzata (**Seleziona dispositivi**, **Selezione dispositivi** o **Seleziona gruppo di amministrazione**, a seconda dell'opzione selezionata nel passaggio precedente), selezionare i computer client, specificare gli indirizzi IP dei computer, specificare una selezione di computer o selezionare il gruppo di amministrazione a cui verrà applicata l'attività.

Passaggio 5. Configurare la pianificazione attività

1. Nella finestra **Configurare la pianificazione delle attività** selezionare la modalità di avvio nell'elenco a discesa **Avvio pianificato**.
2. Se necessario, configurare l'avvio automatico di un'attività pianificata (specificando la data e l'ora di inizio dell'attività).

3. Se si desidera eseguire attività che l'applicazione non è stata in grado di avviare in base alla pianificazione (ad esempio perché il computer era spento all'ora pianificata), selezionare la casella **Esegui attività non effettuate**.

   Kaspersky Endpoint Security avvia l'attività non appena viene eliminato l'ostacolo che impedisce l'avvio dell'attività.

4. Se si desidera che Kaspersky Security Center determini automaticamente l'intervallo tra gli avvii dell'attività in diversi computer, selezionare la casella **Usa automaticamente il ritardo casuale per l'avvio delle attività**.

   Questo consente di ridurre il carico su Kaspersky Security Center Administration Server.

5. Per impostare l'intervallo tra gli avvii dell'attività in diversi computer manualmente, selezionare la casella **Usa ritardo casuale per l'avvio dell'attività con un intervallo di (min)** e specificare il numero di minuti.

   Questo consente di ridurre il carico su Kaspersky Security Center Administration Server.

Passaggio 6. Specificare il nome dell'attività

Nel campo **Nome** della finestra **Definire il nome dell'attività** immettere il nome dell'attività che si intende creare.

Passaggio 7. Completare la creazione dell'attività

Nella finestra **Completare la creazione dell'attività** eseguire le seguenti operazioni:

1. Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella **Esegui l'attività al termine della procedura guidata**.

2. Fare clic su **Fine** per chiudere la procedura guidata.

Avviare e interrompere manualmente le attività

Le attività pianificate vengono avviate e interrotte automaticamente in base a una pianificazione. Tuttavia, è possibile avviare un'attività manualmente in qualsiasi momento.

Nota: le attività vengono avviate in un computer client solo se Network Agent è in esecuzione. Se l'esecuzione di Network Agent viene interrotta, vengono interrotte tutte le attività attive.

Avviare e interrompere manualmente le attività

1. Aprire l'elenco delle attività contenente l'attività che si desidera avviare o interrompere.

2. Selezionare l'attività che si desidera avviare o interrompere.

3. Avviare o interrompere l'attività in uno dei seguenti modi:

   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Avvia** o **Arresta**.

   - Nell'area di lavoro fare clic su **Avvia** o **Arresta**.

   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**. Nella finestra visualizzata fare clic su **Avvia** o **Arresta**.

Importare ed esportare le attività

È possibile esportare attività di gruppo e attività per un set arbitrario di computer in un file.

Esportare un'attività

1. Selezionare l'elenco delle attività da cui si desidera esportare l'attività:
   - Selezionare il gruppo di amministrazione e quindi aprire la scheda **Attività**.
   - Nella struttura della console fare clic su **Attività**.
2. Fare clic con il pulsante destro del mouse sull'attività che si desidera esportare e, nel menu di scelta rapida dell'attività, selezionare **Tutte le attività** > **Esporta**.
3. Nella finestra **Salva con nome** specificare il nome del file e la posizione in cui verrà salvata l'attività esportata.
4. Fare clic su **Salva**.

Importare un'attività

1. Selezionare l'elenco delle attività in cui si desidera importare l'attività:
   - Selezionare il gruppo di amministrazione e quindi aprire la scheda **Attività**.
   - Nella struttura della console fare clic su **Attività**.
2. Importare l'attività in uno dei seguenti modi:
   - Nel menu di scelta rapida dell'elenco attività selezionare **Tutte le attività** > **Importa**.
   - Fare clic su **Importa attività da file**.
3. Nella finestra **Apri** specificare il percorso del file dell'attività che si desidera importare.
4. Fare clic su **Apri**.

   L'attività viene visualizzata nell'elenco delle attività.

Visualizzare le attività

È possibile visualizzare l'elenco delle attività create per un computer specifico, per i computer in un determinato gruppo di amministrazione o l'elenco di tutte le attività non locali.

Visualizzare le attività per un determinato gruppo di amministrazione

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.

4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.

5. Nell'area di lavoro selezionare la scheda **Attività**.

Verrà visualizzato l'elenco delle attività per i computer nel gruppo di amministrazione selezionato.

Visualizzare le attività locali

1. Avviare Kaspersky Security Center Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nella struttura della console fare clic su **Dispositivi gestiti**.

4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.

5. Nell'area di lavoro selezionare la scheda **Dispositivi**.

6. Selezionare il computer dall'elenco dei computer client.

7. Aprire la finestra **Proprietà: <Nome computer>** in uno dei seguenti modi:

   - Fare doppio clic sul nome del computer client.

   - Fare clic con il pulsante destro del mouse sul computer client, quindi selezionare **Proprietà** dal menu di scelta rapida.

8. Nella finestra **Proprietà: <Nome computer>** selezionare la sezione **Attività**.

L'elenco delle attività di sistema e personalizzate per il computer client selezionato verrà visualizzato nell'area di lavoro sulla destra.

Visualizzare le attività non locali

1. Avviare Kaspersky Security Center Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nella struttura della console fare clic su **Attività**.

Verrà visualizzato l'elenco delle attività non locali create per i computer che possono far parte o meno dei gruppi di amministrazione.

Gestire impostazioni specifiche delle attività

Visualizzare le impostazioni di un'attività locale

1. Aprire l'elenco delle attività locali.
2. Selezionare un'attività nell'elenco e aprire le impostazioni dell'attività in uno dei seguenti modi:
   - Fare doppio clic sul nome dell'attività.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**.

Visualizzare le impostazioni di un'attività di gruppo

1. Aprire l'elenco delle attività di gruppo per un gruppo di amministrazione.
2. Selezionare un'attività nell'elenco e aprire le impostazioni dell'attività in uno dei seguenti modi:
   - Fare doppio clic sul nome dell'attività.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura attività** nell'area di lavoro.

Visualizzare le impostazioni di un'attività non locale

1. Aprire l'elenco delle attività non locali.
2. Selezionare un'attività nell'elenco e aprire le impostazioni dell'attività in uno dei seguenti modi:
   - Fare doppio clic sul nome dell'attività.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**.
   - Fare clic sul collegamento **Configura attività** nell'area di lavoro.

Per ulteriori informazioni sulle attività, vedere la Guida di Kaspersky Security Center.

Per attività locali, attività di gruppo o attività per un set arbitrario di computer

Configurare le impostazioni dell'attività Aggiungi chiave

1. Aprire la finestra con le impostazioni dell'attività **Aggiungi chiave**.
2. Selezionare la sezione **Attivazione dell'applicazione**.

3. Se necessario, aggiungere un'altra chiave in uno dei seguenti modi:

   - Per selezionare una chiave o un codice di attivazione tra i codici di attivazione aggiunti all'archivio di Kaspersky Security Center:

     a. Selezionare l'opzione **Chiave o codice di attivazione**.

     b. Fare clic su **Sfoglia**.

     Verrà visualizzata la finestra **Chiavi e codici di attivazione nell'archivio di Kaspersky Security Center**.

     c. Selezionare una chiave o un codice di attivazione.

     d. Fare clic su **OK**.

   - Per aggiungere un file chiave:

     a. Selezionare l'opzione **File chiave**.

     b. Fare clic su **Aggiungi**.

     Verrà visualizzata la finestra di selezione file.

     c. Selezionare un file chiave.

     d. Fare clic su **Apri**.

   Nota: la chiave corrente viene eliminata quando viene aggiunta un'altra chiave.

4. Per aggiungere la chiave specificata come chiave di riserva, selezionare la casella **Aggiungi come chiave di riserva**.

   La chiave di riserva diventa attiva allo scadere della chiave corrente.

   Nota: la data di scadenza della chiave di riserva deve essere successiva alla data di scadenza della chiave corrente.

5. Salvare le modifiche in uno dei seguenti modi:

   - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome attività>** dopo il salvataggio delle modifiche.
   - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome attività>** dopo il salvataggio delle modifiche.

Gestire le impostazioni delle attività Scansione rapida

1. Aprire la finestra con le impostazioni dell'attività **Scansione rapida**.
2. Selezionare la sezione **Scansione rapida**.
3. Per modificare il livello di protezione con cui Kaspersky Endpoint Security esegue l'attività Scansione rapida, eseguire una delle seguenti operazioni nella sezione **Livello di sicurezza**:

   - Selezionare un livello di sicurezza preimpostato spostando il dispositivo di scorrimento verso l'alto o verso il basso.

È possibile selezionare uno dei seguenti livelli di protezione:

- **Protezione massima**. Kaspersky Endpoint Security esegue il monitoraggio di livello più elevato dei file aperti, salvati o eseguiti.
- **Consigliato**. Kaspersky Endpoint Security monitora i file con le impostazioni consigliate da Kaspersky.

  Questo è il livello di sicurezza predefinito.
- **Velocità massima**. Kaspersky Endpoint Security monitora un set minimo di file. È possibile selezionare questo livello di sicurezza se si desidera utilizzare altre applicazioni che richiedono risorse di memoria significative.

- Configurare manualmente le impostazioni di protezione:

  a. Fare clic su **Impostazioni**.

  Verrà visualizzata la finestra **Impostazioni: Scansione**.

  b. Nella scheda **Generali** della sezione **Tipi di file** i tipi di file che devono essere esaminati da Kaspersky Endpoint Security durante l'esecuzione dell'attività Scansione rapida.

  c. Nella scheda **Generali** della sezione **Ottimizzazione** configurare le impostazioni delle prestazioni di scansione.

  d. Nella scheda **Generali** della sezione **File compositi** selezionare i file compositi che devono essere analizzati da Kaspersky Endpoint Security per rilevare eventuali oggetti.

  e. Nella scheda **Avanzate** della sezione **Impostazioni avanzate** configurare l'utilizzo della tecnologia iSwift e il salvataggio delle informazioni sugli oggetti rilevati nelle statistiche dell'applicazione.

  f. Nella scheda **Avanzate** della sezione **Analizzatore euristico** configurare l'utilizzo dell'analizzatore euristico e selezionare il livello di protezione che deve essere applicato da quest'ultimo durante le scansioni anti-malware.

  g. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Impostazioni: Scansione**.

  Il livello di sicurezza diventa **Personalizzato**.

- Per ripristinare le impostazioni predefinite, fare clic su **Predefinito**.

  Il livello di sicurezza diventa **Consigliato**.

4. Se necessario, nella sezione **Azione** selezionare l'azione che Kaspersky Endpoint Security deve eseguire se viene rilevato un oggetto infetto.

5. Per specificare un ambito della scansione, nella sezione **Ambito della scansione** fare clic su **Impostazioni** ed eseguire le seguenti operazioni nella finestra **Ambito della scansione**:

   a. Se si desidera che Kaspersky Endpoint Security esamini la memoria del computer, selezionare la casella di controllo **Memoria**.

   b. Se si desidera che Kaspersky Endpoint Security esamini gli oggetti di avvio, selezionare la casella di controllo **Voci di accesso**.

   c. Se si desidera che Kaspersky Endpoint Security esamini altri file o cartelle, fare clic su **Aggiungi** e specificare un file, una cartella o una maschera dei nomi di una cartella o di un file.

   d. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Ambito della scansione**.

6. Salvare le modifiche in uno dei seguenti modi:

   - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome attività>** dopo il salvataggio delle modifiche.

   - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome attività>** dopo il salvataggio delle modifiche.

Configurare le impostazioni dell'attività Scansione

1. Aprire la finestra con le impostazioni dell'attività **Scansione**.

2. Selezionare la sezione **Scansione**.

3. Per modificare il livello di protezione con cui Kaspersky Endpoint Security esegue l'attività Scansione, eseguire una delle seguenti operazioni nella sezione **Livello di sicurezza**:

   - Selezionare un livello di sicurezza preimpostato spostando il dispositivo di scorrimento verso l'alto o verso il basso.

     È possibile selezionare uno dei seguenti livelli di protezione:

     - **Protezione massima**. Kaspersky Endpoint Security esegue il monitoraggio di livello più elevato dei file aperti, salvati o eseguiti.

     - **Consigliato**. Kaspersky Endpoint Security monitora i file con le impostazioni consigliate da Kaspersky.

       Questo è il livello di sicurezza predefinito.

     - **Velocità massima**. Kaspersky Endpoint Security monitora un set minimo di file. È possibile selezionare questo livello di sicurezza se si desidera utilizzare altre applicazioni che richiedono risorse di memoria significative.

   - Configurare manualmente le impostazioni di protezione:

     a. Fare clic su **Impostazioni**.

        Verrà visualizzata la finestra **Impostazioni: Scansione**.

     b. Nella scheda **Generali** della sezione **Tipi di file** i tipi di file che devono essere esaminati da Kaspersky Endpoint Security durante l'esecuzione dell'attività Scansione.

     c. Nella scheda **Generali** della sezione **Ottimizzazione** configurare le impostazioni delle prestazioni di scansione.

     d. Nella scheda **Generali** della sezione **File compositi** selezionare i file compositi che devono essere analizzati da Kaspersky Endpoint Security per rilevare eventuali oggetti.

     e. Nella scheda **Avanzate** della sezione **Impostazioni avanzate** configurare l'utilizzo della tecnologia iSwift e il salvataggio delle informazioni sugli oggetti rilevati nelle statistiche dell'applicazione.

     f. Nella scheda **Avanzate** della sezione **Analizzatore euristico** configurare l'utilizzo dell'analizzatore euristico e selezionare il livello di protezione che deve essere applicato da quest'ultimo durante le scansioni anti-malware.

     g. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Impostazioni: Scansione**.

        Il livello di sicurezza diventa **Personalizzato**.

- Per ripristinare le impostazioni predefinite, fare clic su **Predefinito**.

  Il livello di sicurezza diventa **Consigliato**.

4. Se necessario, nella sezione **Azione** selezionare l'azione che Kaspersky Endpoint Security deve eseguire se viene rilevato un oggetto infetto.

5. Per specificare un ambito della scansione, nella sezione **Ambito della scansione** fare clic su **Impostazioni** ed eseguire le seguenti operazioni nella finestra **Ambito della scansione**:

   a. Se si desidera che Kaspersky Endpoint Security esamini tutte le unità rimovibili, selezionare la casella **Tutti i dischi rimovibili**.

   b. Se si desidera che Kaspersky Endpoint Security esamini tutte le unità interne, selezionare la casella di controllo **Tutti i dischi interni**.

   c. Se si desidera che Kaspersky Endpoint Security esamini tutte le unità di rete, selezionare la casella di controllo **Tutti i dischi di rete**.

   d. Se si desidera che Kaspersky Endpoint Security esamini la memoria del computer, selezionare la casella di controllo **Memoria**.

   e. Se si desidera che Kaspersky Endpoint Security esamini gli oggetti di avvio, selezionare la casella di controllo **Voci di accesso**.

   f. Se si desidera che Kaspersky Endpoint Security esamini altri file o cartelle, fare clic su **Aggiungi** e specificare un file, una cartella o una maschera dei nomi di una cartella o di un file.

   g. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Ambito della scansione**.

6. Salvare le modifiche in uno dei seguenti modi:

   - Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome attività>** dopo il salvataggio delle modifiche.

   - Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome attività>** dopo il salvataggio delle modifiche.

Gestire le impostazioni dell'attività Aggiornamento

1. Aprire la finestra con le impostazioni dell'attività **Aggiornamento**.

2. Selezionare la sezione **Aggiornamento**.

3. Se si desidera che Kaspersky Endpoint Security aggiorni i moduli dell'applicazione insieme ai database dell'applicazione, selezionare la casella **Aggiorna moduli dell'applicazione**.

4. Per selezionare una sorgente degli aggiornamenti:

   a. Fare clic su **Impostazioni**.

   Verrà visualizzata la finestra **Impostazioni: Aggiornamento**.

b. Specificare la sorgente degli aggiornamenti in uno dei seguenti modi:

- Se si desidera che l'applicazione scarichi gli aggiornamenti da Administration Server, selezionare la casella **Kaspersky Security Center**.
- Se si desidera che l'applicazione scarichi gli aggiornamenti dai server di aggiornamento di Kaspersky, selezionare la casella **Server degli aggiornamenti Kaspersky**.
- Per aggiungere una sorgente degli aggiornamenti diversa, fare clic su **Aggiungi** e immettere nella finestra visualizzata il percorso della sorgente degli aggiornamenti.

  Per impostazione predefinita, Kaspersky Endpoint Security scarica gli aggiornamenti dai server di aggiornamento di Kaspersky.

c. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Impostazioni: Aggiornamento**.

5. Salvare le modifiche in uno dei seguenti modi:

- Fare clic su **Applica** per rimanere nella finestra **Proprietà: <Nome attività>** dopo il salvataggio delle modifiche.
- Fare clic su **OK** per chiudere la finestra **Proprietà: <Nome attività>** dopo il salvataggio delle modifiche.

Solo per attività locali

Gestire le impostazioni dell'attività Protezione Minacce File

1. Aprire l'elenco di attività locali per un computer client.
2. Nell'elenco di attività locali selezionare l'attività Protezione Minacce File e aprire le relative proprietà in uno dei seguenti modi:

- Fare doppio clic sul nome dell'attività.
- Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**.
- Fare clic su **Proprietà**.

3. Selezionare la sezione **Protezione minacce file**.
4. Se necessario, configurare le seguenti impostazioni:

- Abilitare o disabilitare Protezione Minacce File nel computer client.
- Per selezionare uno dei livello di sicurezza preimpostati, utilizzare il dispositivo di scorrimento nella sezione **Livello di sicurezza**.

- Per configurare manualmente le impostazioni di protezione fare clic su **Impostazioni** e, nella finestra **Impostazioni: Protezione minacce file** visualizzata, eseguire le seguenti operazioni:

  a. Nella scheda **Generali** della sezione **Tipi di file** selezionare i tipi di file che devono essere esaminati da Kaspersky Endpoint Security quando vengono aperti, eseguiti o salvati.

  b. Nella scheda **Generali**, nella sezione **Ottimizzazione**, configurare le impostazioni delle prestazioni di scansione e selezionare la tecnologia di scansione, quindi selezionare se Kaspersky Endpoint Security ignorerà la scansione del volume di sistema di sola lettura nei computer client.

  c. Nella scheda **Generali** della sezione **File compositi** selezionare quali file compositi devono essere esaminati alla ricerca di oggetti rilevabili e impostare una restrizione sulla scansione degli oggetti di grandi dimensioni.

  d. Nella scheda **Ambito della protezione** specificare i file o le cartelle che devono essere esaminati da Protezione Minacce File.

  Per impostazione predefinita, vengono esaminati tutti gli oggetti nelle unità rimovibili, interne e di rete connesse al computer client. È possibile aggiungere un oggetto all'ambito di protezione, modificare un oggetto nell'elenco, disabilitare temporaneamente la scansione di un oggetto nell'elenco o rimuovere un oggetto dall'elenco.

  e. Nella scheda **Avanzate**, nella sezione **Modalità di scansione**, selezionare la modalità Protezione Minacce File.

  f. Nella scheda **Avanzate** della sezione **Sospendi attività** abilitare o disabilitare la sospensione pianificata di Protezione Minacce File e configurare la sospensione automatica delle attività in base a una pianificazione.

  g. Nella scheda **Avanzate** della sezione **Analizzatore euristico** configurare l'utilizzo dell'analizzatore euristico da parte di Protezione Minacce File.

  h. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Impostazioni: Protezione minacce file**.

- Nella sezione **Se viene rilevato un oggetto dannoso** selezionare l'azione che Protezione Minacce File deve eseguire al rilevamento di un oggetto infetto.

5. Salvare le modifiche in uno dei seguenti modi:

   - Fare clic sul pulsante **Applica** per rimanere nella finestra **Proprietà: Protezione minacce file** dopo il salvataggio delle modifiche.

   - Fare clic sul pulsante **OK** per chiudere la finestra **Proprietà: Protezione minacce file** dopo il salvataggio delle modifiche.

Gestire le impostazioni dell'attività Protezione Minacce Web

1. Aprire l'elenco di attività locali per un computer client.
2. Nell'elenco di attività locali selezionare l'attività Protezione Minacce Web e aprire le relative proprietà in uno dei seguenti modi:
   - Fare doppio clic sul nome dell'attività.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**.
   - Fare clic su **Proprietà**.
3. Selezionare la sezione **Protezione minacce Web**.
4. Se necessario, configurare le seguenti impostazioni:
   - Abilitare o disabilitare Protezione Minacce Web nel computer client.
   - Per selezionare uno dei livello di sicurezza preimpostati, utilizzare il dispositivo di scorrimento nella sezione **Livello di sicurezza**.
   - Per configurare manualmente le impostazioni di protezione fare clic su **Impostazioni** e, nella finestra **Impostazioni: Protezione minacce Web** visualizzata, eseguire le seguenti operazioni:
     a. Nella scheda **Generali**, nella sezione **Modalità di scansione**, abilitare o disabilitare il controllo degli indirizzi Web in base al database degli indirizzi Web dannosi.
     b. Nella scheda **Generali**, nella sezione **Impostazioni di Anti-Phishing**, abilitare o disabilitare il controllo degli indirizzi Web in base al database degli indirizzi Web di phishing.
     c. Nella scheda **Generali**, nella sezione **Impostazioni di Anti-Phishing**, abilitare o disabilitare l'utilizzo dell'analizzatore euristico per il rilevamento dei collegamenti di phishing.
     d. Nella scheda **Indirizzi Web attendibili** abilitare o disabilitare la scansione del traffico Web da indirizzi Web attendibili e creare o modificare un elenco di indirizzi Web attendibili.
     e. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Impostazioni: Protezione minacce Web**.
5. Nella sezione **Se viene rilevato un oggetto dannoso** selezionare l'azione che Protezione Minacce Web deve eseguire al rilevamento di un oggetto pericoloso nel traffico Web.
6. Salvare le modifiche in uno dei seguenti modi:
   - Fare clic sul pulsante **Applica** per rimanere nella finestra **Proprietà: Protezione minacce Web** dopo il salvataggio delle modifiche.
   - Fare clic sul pulsante **OK** per chiudere la finestra **Proprietà: Protezione minacce Web** dopo il salvataggio delle modifiche.

Gestire le impostazioni delle attività Scansione rapida

1. Aprire l'elenco di attività locali per un computer client.
2. Nell'elenco di attività locali selezionare l'attività Scansione rapida e aprire le relative proprietà in uno dei seguenti modi:
   - Fare doppio clic sul nome dell'attività.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**.
   - Fare clic su **Proprietà**.
3. Selezionare la sezione **Scansione**.
4. Se necessario, configurare le seguenti impostazioni:
   - Per selezionare uno dei livello di sicurezza preimpostati, utilizzare il dispositivo di scorrimento nella sezione **Livello di sicurezza**.
   - Per configurare manualmente le impostazioni di protezione fare clic su **Impostazioni** e, nella finestra **Impostazioni: Scansione** visualizzata, eseguire le seguenti operazioni:
     a. Nella scheda **Generali** della sezione **Tipi di file** selezionare i tipi di file che devono essere esaminati da Kaspersky Endpoint Security.
     b. Nella scheda **Generali** della sezione **Ottimizzazione** configurare le impostazioni delle prestazioni di scansione.
     c. Nella scheda **Generali** della sezione **File compositi** selezionare i file compositi che devono essere esaminati da Kaspersky Endpoint Security.
     d. Nella scheda **Avanzate** della sezione **Impostazioni avanzate** configurare l'utilizzo della tecnologia iSwift e il salvataggio delle informazioni sugli oggetti rilevati nelle statistiche dell'applicazione.
     e. Nella scheda **Avanzate** della sezione **Analizzatore euristico** configurare l'utilizzo dell'analizzatore euristico e selezionare il livello di protezione che deve essere applicato da quest'ultimo.
     f. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Impostazioni: Scansione**.
   - Nella sezione **Azione** selezionare l'azione che Kaspersky Endpoint Security deve eseguire al rilevamento di un oggetto infetto.
   - Per specificare un ambito della scansione, nella sezione **Ambito della scansione** fare clic su **Impostazioni** ed eseguire le seguenti operazioni nella finestra **Ambito della scansione**:
     - Se si desidera che Kaspersky Endpoint Security esamini gli oggetti nell'elenco predefinito, selezionare la casella accanto all'oggetto attinente.
     - Se si desidera che Kaspersky Endpoint Security esamini altri file o cartelle, fare clic su **Aggiungi** e specificare un file, una cartella o una maschera dei nomi di una cartella o di un file.
     - Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Ambito della scansione**.

5. Salvare le modifiche in uno dei seguenti modi:

   - Fare clic su **Applica** per rimanere nella finestra **Proprietà: Scansione rapida** dopo il salvataggio delle modifiche.

   - Fare clic su **OK** per chiudere la finestra **Proprietà: Scansione rapida** dopo il salvataggio delle modifiche.

Gestire le impostazioni delle attività Scansione completa

1. Aprire l'elenco di attività locali per un computer client.

2. Nell'elenco di attività locali selezionare l'attività Scansione completa e aprire le relative proprietà in uno dei seguenti modi:

   - Fare doppio clic sul nome dell'attività.

   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**.

   - Fare clic su **Proprietà**.

3. Selezionare la sezione **Scansione**.

4. Se necessario, configurare le seguenti impostazioni:

   - Per selezionare uno dei livello di sicurezza preimpostati, utilizzare il dispositivo di scorrimento nella sezione **Livello di sicurezza**.

   - Per configurare manualmente le impostazioni di protezione fare clic su **Impostazioni** e, nella finestra **Impostazioni: Scansione** visualizzata, eseguire le seguenti operazioni:

     a. Nella scheda **Generali** della sezione **Tipi di file** selezionare i tipi di file che devono essere esaminati da Kaspersky Endpoint Security.

     b. Nella scheda **Generali** della sezione **Ottimizzazione** configurare le impostazioni delle prestazioni di scansione.

     c. Nella scheda **Generali** della sezione **File compositi** selezionare i file compositi che devono essere esaminati da Kaspersky Endpoint Security.

     d. Nella scheda **Avanzate** della sezione **Impostazioni avanzate** configurare l'utilizzo della tecnologia iSwift e il salvataggio delle informazioni sugli oggetti rilevati nelle statistiche dell'applicazione.

     e. Nella scheda **Avanzate** della sezione **Analizzatore euristico** configurare l'utilizzo dell'analizzatore euristico e selezionare il livello di protezione che deve essere applicato da quest'ultimo.

     f. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Impostazioni: Scansione**.

   - Nella sezione **Azione** selezionare l'azione che Kaspersky Endpoint Security deve eseguire al rilevamento di un oggetto infetto.

- Per specificare un ambito della scansione, nella sezione **Ambito della scansione** fare clic su **Impostazioni** ed eseguire le seguenti operazioni nella finestra **Ambito della scansione**:

  - Se si desidera che Kaspersky Endpoint Security esamini gli oggetti nell'elenco predefinito, selezionare la casella accanto all'oggetto attinente.

  - Se si desidera che Kaspersky Endpoint Security esamini altri file o cartelle, fare clic su **Aggiungi** e specificare un file, una cartella o una maschera dei nomi di una cartella o di un file.

  - Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Ambito della scansione**.

5. Salvare le modifiche in uno dei seguenti modi:

   - Fare clic su **Applica** per rimanere nella finestra **Proprietà: Scansione completa** dopo il salvataggio delle modifiche.

   - Fare clic su **OK** per chiudere la finestra **Proprietà: Scansione completa** dopo il salvataggio delle modifiche.

Gestire le impostazioni delle attività Scansione personalizzata

1. Aprire l'elenco di attività locali per un computer client.

2. Nell'elenco di attività locali selezionare l'attività Scansione personalizzata e aprire le relative proprietà in uno dei seguenti modi:

   - Fare doppio clic sul nome dell'attività.

   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**.

   - Fare clic su **Proprietà**.

3. Selezionare la sezione **Scansione**.

4. Se necessario, configurare le seguenti impostazioni:

   - Per selezionare uno dei livello di sicurezza preimpostati, utilizzare il dispositivo di scorrimento nella sezione **Livello di sicurezza**.

   - Per configurare manualmente le impostazioni di protezione fare clic su **Impostazioni** e, nella finestra **Impostazioni: Scansione** visualizzata, eseguire le seguenti operazioni:

     a. Nella scheda **Generali** della sezione **Tipi di file** selezionare i tipi di file che devono essere esaminati da Kaspersky Endpoint Security.

     b. Nella scheda **Generali** della sezione **Ottimizzazione** configurare le impostazioni delle prestazioni di scansione.

     c. Nella scheda **Generali** della sezione **File compositi** selezionare i file compositi che devono essere esaminati da Kaspersky Endpoint Security.

     d. Nella scheda **Avanzate** della sezione **Impostazioni avanzate** configurare l'utilizzo della tecnologia iSwift e il salvataggio delle informazioni sugli oggetti rilevati nelle statistiche dell'applicazione.

e. Nella scheda **Avanzate** della sezione **Analizzatore euristico** configurare l'utilizzo dell'analizzatore euristico e selezionare il livello di protezione che deve essere applicato da quest'ultimo.

f. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Impostazioni: Scansione**.

- Nella sezione **Azione** selezionare l'azione che Kaspersky Endpoint Security deve eseguire al rilevamento di un oggetto infetto.
- Per specificare un ambito della scansione, nella sezione **Ambito della scansione** fare clic su **Impostazioni** ed eseguire le seguenti operazioni nella finestra **Ambito della scansione**:
  - Fare clic su **Aggiungi** e specificare un file, una cartella o una maschera per il nome di un file o di una cartella.
  - Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Ambito della scansione**.

5. Salvare le modifiche in uno dei seguenti modi:
   - Fare clic sul pulsante **Applica** per rimanere nella finestra **Proprietà: Scansione personalizzata** dopo il salvataggio delle modifiche.
   - Fare clic su **OK** per chiudere la finestra **Proprietà: Scansione personalizzata** dopo il salvataggio delle modifiche.

Gestire le impostazioni dell'attività Protezione Minacce di Rete

1. Aprire l'elenco di attività locali per un computer client.
2. Nell'elenco di attività locali selezionare l'attività Protezione Minacce di Rete e aprire le relative proprietà in uno dei seguenti modi:
   - Fare doppio clic sul nome dell'attività.
   - Fare clic con il pulsante destro del mouse per visualizzare il menu di scelta rapida dell'attività e selezionare **Proprietà**.
   - Fare clic su **Proprietà**.
3. Selezionare la sezione **Protezione minacce di rete**.
4. Se necessario, configurare le seguenti impostazioni:
   - Abilitare o disabilitare Protezione Minacce di Rete nel computer client.
   - Nella sezione **Impostazioni di Protezione minacce di rete** selezionare o deselezionare la casella di controllo **Blocca computer da cui ha origine l'attacco per <valore> min** e specificare il valore.
   - È inoltre possibile specificare gli indirizzi IP dei computer la cui attività di rete non verrà bloccata. A tale scopo, eseguire i seguenti passaggi:

     a. Fare clic su **Esclusioni**.

     Verrà visualizzata la finestra **Esclusioni**.

     b. Fare clic su **Aggiungi**.

     Verrà visualizzata la finestra **Indirizzo IP**.

c. Specificare l'Indirizzo IP del computer la cui attività di rete non verrà bloccata e fare clic su **OK**.

d. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Esclusioni**.

5. Salvare le modifiche in uno dei seguenti modi:

- Fare clic sul pulsante **Applica** per rimanere nella finestra **Proprietà: Protezione minacce di rete** dopo il salvataggio delle modifiche.
- Fare clic sul pulsante **OK** per chiudere la finestra **Proprietà: Protezione minacce di rete** dopo il salvataggio delle modifiche.

Creare e gestire i criteri

Questa sezione contiene informazioni su come creare e configurare criteri per Kaspersky Endpoint Security.

Un criterio determina le impostazioni di un'applicazione e gestisce la possibilità di configurare tale applicazione nei dispositivi all'interno di un gruppo di amministrazione. Per ogni applicazione è necessario creare un criterio individuale. È possibile creare un numero illimitato di vari criteri per le applicazioni installate nei dispositivi in ciascun gruppo di amministrazione, ma per ogni applicazione può essere applicato un solo criterio per volta all'interno di un gruppo di amministrazione.

Nota: durante la creazione e la configurazione di un criterio, è possibile consentire o vietare le modifiche per i gruppi di impostazioni nei criteri utilizzando i pulsanti e .

È possibile eseguire le seguenti azioni sui criteri personalizzati:

- Creare i criteri.
- Configurare i criteri.
- Copiare o spostare i criteri da un gruppo all'altro.
- Eliminare criteri.
- Modificare lo stato dei criteri.
- Esportare i criteri in un file.
- Importare i criteri da un file.

Per informazioni dettagliate sui criteri di Kaspersky Security Center, vedere la Guida di Kaspersky Security Center.

Creare un criterio

Questa sezione contiene istruzioni su come avviare la Creazione guidata nuovo criterio per creare un criterio.

Creare un criterio dalla cartella di un gruppo di amministrazione

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.
5. Nell'area di lavoro selezionare la scheda **Criteri** e fare clic su **Nuovo criterio**.
   Verrà avviata la Creazione guidata nuovo criterio.
6. Seguire i passaggi della Creazione guidata nuovo criterio per creare un criterio.

Creare un criterio dalla cartella Criteri

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Criteri**.
4. Nell'area di lavoro fare clic su **Nuovo criterio**.
   Verrà avviata la Creazione guidata nuovo criterio.
5. Seguire i passaggi della Creazione guidata nuovo criterio per creare un criterio.

Per procedere al passaggio successivo della procedura guidata, fare clic su **Avanti**. Per tornare al passaggio precedente della procedura guidata, fare clic su ←. Per uscire dalla procedura guidata in qualsiasi passaggio, fare clic su **Annulla**.

Nota: l'aspetto dei pulsanti può variare in base alla versione di Windows.

Passaggio 1. Selezionare un'applicazione

Nell'elenco delle applicazioni della finestra **Selezionare l'applicazione per cui creare un criterio di gruppo** selezionare **Kaspersky Endpoint Security for Mac (12.2.1)**.

Passaggio 2. Specificare il nome del criterio

1. Nel campo **Nome** della finestra **Immettere il nome di un criterio di gruppo** specificare il nome del criterio che si intende creare. Il nome non può contenere i seguenti simboli: " * < : > ? \ |.
2. Selezionare la casella di controllo **Utilizza le impostazioni del criterio per una versione precedente dell'applicazione** per importare le impostazioni di un criterio esistente di Kaspersky Endpoint Security in un nuovo criterio.

Passaggio 3. Specificare le impostazioni di protezione

Nella finestra **Protezione** configurare le seguenti impostazioni se necessario:

- Configurare le impostazioni di protezione per il sistema operativo nel computer client.
- Configurare Area attendibile.

  È possibile creare un elenco di oggetti che Kaspersky Endpoint Security non sottopone a scansione o monitoraggio.
- Configurare Applicazioni attendibili.

  È possibile creare un elenco di applicazioni la cui attività del file e della rete non verrà monitorata da Kaspersky Endpoint Security.
- Selezionare i tipi di oggetti da rilevare.
- Disabilitare o abilitare l'avvio delle attività pianificate quando il computer funziona con alimentazione a batteria.
- Limita l'uso della CPU per le scansioni.

Passaggio 4. Configurare le impostazioni di Protezione Minacce File

Nella finestra **Protezione minacce file** eseguire le seguenti operazioni se necessario:

- Attivare/disattivare Protezione Minacce File.

  Per impostazione predefinita, Protezione Minacce File è attivato.
- Selezionare un livello di sicurezza.

  Per impostazione predefinita è selezionato il livello di sicurezza consigliato da Kaspersky.
- Configurare le impostazioni di Protezione Minacce File.
- Selezionare l'azione da eseguire al rilevamento di un oggetto dannoso.

Passaggio 5. Configurare le impostazioni di Protezione Minacce Web

Nella finestra **Protezione minacce Web** eseguire le seguenti operazioni se necessario:

- Attivare/disattivare Protezione Minacce Web.

  Per impostazione predefinita, Protezione Minacce Web è attivato.
- Selezionare un livello di sicurezza.

  Per impostazione predefinita è selezionato il livello di sicurezza consigliato da Kaspersky.
- Configurare le impostazioni di Protezione Minacce Web.
- Selezionare l'azione da eseguire al rilevamento di un oggetto dannoso nel traffico Web.

Passaggio 6. Configurare le impostazioni di Protezione Minacce di Rete

Nella finestra **Protezione minacce di rete** eseguire le seguenti operazioni se necessario:

- Attivare/disattivare Protezione Minacce di Rete.

  Per impostazione predefinita, Protezione Minacce di Rete è abilitato.

- Configurare le impostazioni di Protezione Minacce di Rete.
- Creare o modificare un elenco di indirizzi IP di computer remoti le cui attività della rete non verranno mai bloccate da Kaspersky Endpoint Security.

Passaggio 7. Configurare le impostazioni di aggiornamento

Nella finestra **Aggiornamento** eseguire le seguenti operazioni se necessario:

- Attivare o disattivare l'aggiornamento dei moduli dell'applicazione.
- Specificare le sorgenti degli aggiornamenti.

Passaggio 8. Configurare le impostazioni KSN

Nella finestra **Kaspersky Security Network** eseguire le seguenti operazioni se necessario:

- Leggere il testo completo dell'Informativa di Kaspersky Security Network facendo clic su **Informativa KSN**.
- Visualizzare le informazioni sull'infrastruttura KSN rese disponibili da Kaspersky Security Center.
- Attivare o disattivare l'utilizzo di Kaspersky Security Network.
- Abilitare o disabilitare la modalità KSN estesa.
- Abilitare o disabilitare l'utilizzo di un proxy KSN.
- Abilitare o disabilitare l'utilizzo dei server Kaspersky quando il proxy KSN non è disponibile.

> **Nota:** l'utilizzo di Kaspersky Security Network e di un proxy KSN nei computer remoti è disponibile solo se Kaspersky Security Center Administration Server viene utilizzato come server proxy. Per informazioni dettagliate sulle proprietà di Administration Server, vedere la Guida di Kaspersky Security Center.

Quando l'infrastruttura di KSN globale viene utilizzata da Kaspersky Security Center e si sceglie di partecipare a Kaspersky Security Network nelle impostazioni dei criteri, le statistiche di Kaspersky Endpoint Security dei computer client a cui è applicato il criterio vengono automaticamente inviate a Kaspersky per incrementare la protezione di questi computer.

> **Nota:** Kaspersky non riceve, elabora o archivia dati personali senza il consenso esplicito dell'utente.

Dati forniti a Kaspersky durante l'utilizzo di Kaspersky Security Network nell'infrastruttura KSN globale

Se la casella di controllo **Accetto di utilizzare Kaspersky Security Network** è selezionata e la casella di controllo **Abilita modalità KSN estesa** è deselezionata, Kaspersky Endpoint Security fornisce a Kaspersky i seguenti dati:

- Informazioni sulla licenza utilizzata: tipo di licenza e relativo periodo di validità, numero di giorni restanti prima della scadenza della licenza, identificatore del partner dal quale la licenza è stata acquistata, identificatore del Centro regionale di attivazione, checksum del codice di attivazione, hash del corpo del ticket calcolato tramite l'algoritmo SHA1, data e ora di creazione del ticket di licenza, identificatore dei dati della licenza, identificatore del ticket della licenza, identificatore di sequenza del ticket della licenza, identificatore univoco del computer dell'utente, data di inizio validità del ticket della licenza, data di fine validità del ticket della licenza, stato corrente del ticket della licenza, versione intestazione ticket, versione della licenza, identificatore certificato di firma intestazione ticket, checksum del file chiave, numero di serie firmatario intestazione ticket, token di autenticazione.

- Versione completa del Software installato;
  tipo di software installato;
  ID aggiornamento Software; ID del servizio di reputazione; ID del tipo di protocollo; ID di un centro di attivazione regionale; versione dell'elenco delle decisioni del servizio Software revocato; ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record dei database anti-virus del Software attivati; ID univoco dell'istanza di installazione dell'applicazione nel computer; data di attivazione della licenza; data di scadenza della licenza; identificatore della licenza; stato della licenza utilizzata dal software; tipo di checksum per l'oggetto elaborato; nome del malware rilevato o del software legittimo che può essere utilizzato per danneggiare i dati o il dispositivo dell'utente; checksum dell'oggetto elaborato; checksum del codice di attivazione del Software; versione completa del software; ID dispositivo univoco; ID Software; checksum del file chiave del Software; ID del modello di informazioni utilizzato per fornire la licenza Software; identificatore del certificato utilizzato per accedere all'intestazione del ticket della licenza Software; data e ora di creazione del ticket di licenza Software; checksum del ticket di licenza Software; versione del ticket di licenza Software; versione del codice di attivazione del Software; formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; ID ticket licenza corrente; ID componente Software; risultato dell'azione del Software; codice errore; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); numero di porta; indirizzo Web dell'origine della richiesta del servizio Web (Referrer); chiave pubblica del certificato; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash.

Se le caselle di controllo **Accetto di utilizzare Kaspersky Security Network** e **Abilita modalità KSN estesa** sono selezionate, Kaspersky Endpoint Security fornisce a Kaspersky i seguenti dati:

- Informazioni sulla versione del sistema operativo (OS) e dei service pack installati sul computer, sulla versione e sui checksum (MD5, SHA2-256, SHA1) del file kernel del sistema operativo e sui parametri della modalità di esecuzione del sistema operativo; versione del sistema operativo, numero build del sistema operativo, numero di aggiornamento del sistema operativo, edizione del sistema operativo, informazioni estese sull'edizione del sistema operativo; versione Service Pack del sistema operativo; data e ora di avvio del sistema operativo; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di analisi comportamentale; numero di eventi azione del sistema operativo del tipo corrente ritardati; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di difesa proattiva; numero di eventi azione del sistema operativo elaborati; numero di eventi azione del sistema operativo sincroni elaborati; ritardo totale di tutti gli eventi azione del sistema operativo del tipo corrente; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di archiviazione degli eventi persistenti; ritardo totale di tutti gli eventi azione del sistema operativo; numero di eventi azione del sistema operativo sincroni in attesa; data e ora dell'evento ricevuto di un'azione nel sistema operativo.

- Informazioni sull'ultimo riavvio non riuscito del sistema operativo: numero di riavvii non riusciti.

- Informazioni sull'applicazione installata dal Titolare dei diritti e sullo stato della protezione anti-virus: ID installazione Software (PCID); versione del record del database del Software; identificativo univoco dell'istanza di installazione dell'applicazione sul computer, tipo di applicazione, ID del tipo di applicazione, versione completa dell'applicazione installata, identificativo della versione delle impostazioni dell'applicazione, identificativo del tipo di computer, identificativo univoco del computer su cui è installata l'applicazione, identificativo univoco dell'Utente nei servizi del Titolare dei diritti, lingua locale e stato operativo, versione dei componenti del Software installato e relativo stato operativo, versione del protocollo utilizzato per connettersi ai servizi del Titolare dei diritti. versione completa del Software installato; tipo di software installato; ID aggiornamento Software; ID del servizio di reputazione; ID del tipo di protocollo; ID di un centro di attivazione regionale; versione dell'elenco delle decisioni del servizio Software revocato; ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record dei database anti-virus del Software attivati; ID univoco dell'istanza di installazione dell'applicazione nel computer; data di attivazione della licenza; data di scadenza della licenza; identificatore della licenza; stato della licenza utilizzata dal software; tipo di checksum per l'oggetto elaborato; nome del malware rilevato o del software legittimo che può essere utilizzato per danneggiare i dati o il dispositivo dell'utente; checksum dell'oggetto elaborato; checksum del codice di attivazione del Software; versione completa del software; ID Software; checksum del file chiave del Software; ID del modello di informazioni utilizzato per fornire la licenza Software; identificatore del certificato utilizzato per accedere all'intestazione del ticket della licenza Software; data e ora di creazione del ticket di licenza Software; checksum del ticket di licenza Software; versione del ticket di licenza Software; versione del codice di attivazione del Software; formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; ID ticket licenza corrente; ID componente Software; risultato dell'azione del Software; codice errore; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); numero di porta; indirizzo Web dell'origine della richiesta del servizio Web (Referrer); numero di cicli di applicazione degli aggiornamenti per i database anti-virus; data e ora dell'ultimo aggiornamento e dell'applicazione dei database anti-virus; data e ora di rilascio dei database del Software; versione del componente del Software; ID aggiornamento Software; tipo di software installato; data e ora di avvio di Controllo sistema; data e ora di installazione del Software; probabilità di invio statistiche da parte di Controllo sistema; codice dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; tempo di elaborazione del database dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; tempo massimo consentito per l'elaborazione di un evento da parte di Controllo sistema; tempo di elaborazione dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; numero totale di eventi che hanno richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema.

- Informazioni su tutti gli oggetti elaborati e sulle operazioni: verdetto del Software sull'oggetto elaborato; codice directory; dimensioni dell'oggetto elaborato; checksum (SHA256) dell'oggetto elaborato; numero del software rilevato nel contesto Controllo sistema; data e ora di rilevamento del software da parte di Controllo sistema; caratteristiche di rilevamento; ID del record attivato nei database anti-virus del Software; motivo del rilevamento del software da parte di Controllo sistema; checksum (MD5) dell'oggetto elaborato; risultato del controllo dell'integrità del modulo; nome dell'oggetto elaborato; tipo di record dei database anti-virus del Software attivati; percorso dell'oggetto elaborato; nome dell'oggetto esaminato; data e ora della scansione; URL e indirizzi Referrer da cui è stato scaricato; dimensioni dei file esaminati e dei relativi percorsi; segno dell'archivio; data e ora di creazione del file; nome, dimensioni e checksum (MD5, SHA2-256) dello strumento di creazione dei pacchetti (se il file è stato compresso); l'entropia del file; tipo di file; codice del tipo di file; formato, ID e segno del file eseguibile; checksum dell'oggetto (MD5, SHA2-256); tipo e il valore del checksum supplementare dell'oggetto; dati relativi alla firma digitale dell'oggetto (certificato): dati sull'entità di pubblicazione del certificato, numero di avvii dell'oggetto dall'ultimo invio di dati statistici, ID dell'attività di scansione dell'applicazione, modalità di ricezione delle informazioni sulla reputazione dell'oggetto, valore del filtro di destinazione, parametri tecnici delle tecnologie di rilevamento applicabili; percorso dell'oggetto elaborato; codice directory.

- Per i file eseguibili: entropia delle sezioni dei file, flag di verifica della reputazione o flag di firma del file, nome, tipo, ID, checksum (MD5) e dimensione dell'applicazione caricata dall'oggetto in fase di convalida, percorso dell'applicazione e percorsi del template, attributo indicante la presenza nell'elenco di esecuzione automatica, data di inserimento, elenco di attributi, nome dello strumento di creazione dei pacchetti, informazioni sulla firma digitale dell'applicazione: certificato dell'autore, nome del file caricato nel formato MIME, data e ora di compilazione del file.

- Informazioni sulle applicazioni avviate e sui rispettivi moduli: checksum (MD5, SHA2-256) dei file in esecuzione, dimensioni, attributi, data di creazione, nome dello strumento di creazione dei pacchetti (se il file è stato inserito in un pacchetto), nomi dei file, informazioni sui processi in esecuzione nel sistema (ID processo (PID), nome processo, informazioni sull'account da cui è stato avviato il processo, l'applicazione e il comando che hanno avviato il processo, percorso completo dei file del processo e riga di comando iniziale, descrizione dell'applicazione alla quale appartiene il processo (nome dell'applicazione e informazioni sull'autore), certificati digitali utilizzati e informazioni necessarie per verificarne l'autenticità o informazioni sull'assenza della firma digitale di un file), nonché informazioni sui moduli caricati nei processi: nome, dimensione, tipo, data di creazione, attributi, checksum (MD5, SHA2-256, SHA1), percorsi, informazioni sull'intestazione dei file PE, nomi degli strumenti di creazione dei pacchetti (se il file è stato inserito in un pacchetto), informazioni sulla disponibilità e la validità di queste statistiche e ID della modalità utilizzata per generare le statistiche inviate.

- Se vengono identificate minacce o vulnerabilità, oltre alle informazioni sull'oggetto rilevato verranno fornite informazioni sull'identificatore, sulla versione e sul tipo di record nel database anti-virus, il nome della minaccia in base alla classificazione Kaspersky, la data e l'ora dell'ultimo aggiornamento del database anti-virus, il nome del file eseguibile, il checksum (MD5) del file dell'applicazione che ha richiesto l'URL in cui è stata rilevata la minaccia, l'indirizzo IP (IPv4 o IPv6) della minaccia rilevata, l'identificatore della vulnerabilità e il livello della minaccia, l'URL e il Referrer della pagina Web in cui è stata rilevata la vulnerabilità.

- Se viene rilevato un oggetto potenzialmente dannoso, le relative informazioni sui dati vengono trasmesse nella memoria dei processi.

- Informazioni sugli attacchi di rete: indirizzo IP del computer da cui proviene l'attacco e numero della porta nel computer dell'utente interessata dall'attacco di rete, ID del protocollo di attacco, nome e tipo di attacco.

- Informazioni sulle connessioni di rete: la versione e i checksum (MD5, SHA2-256, SHA1) del file da cui il processo è stato avviato che ha aperto la porta, il percorso del file del processo e la sua firma digitale, gli indirizzi IP locale e remoto, i numeri delle porte di connessione locali e remote, lo stato di connessione, il timestamp dell'apertura della porta.

- L'URL e l'indirizzo IP della pagina web su cui è stato rilevato il contenuto dannoso o sospetto, il nome, la dimensione e il checksum del file che ha richiesto l'URL, il codice identificativo, il peso e il grado della regola impiegata per raggiungere il verdetto, l'oggetto dell'attacco.

- Informazioni sugli aggiornamenti dell'applicazione installata e dei database anti-virus: stato di completamento dell'attività di aggiornamento, tipo di errore che potrebbe essersi verificato durante il processo di aggiornamento, numero di aggiornamenti non riusciti e identificatore del componente dell'applicazione che esegue gli aggiornamenti.

- Informazioni sull'utilizzo di Kaspersky Security Network (KSN): identificatore KSN, identificatore dell'applicazione, versione completa dell'applicazione, indirizzo IP depersonalizzato del dispositivo dell'Utente, indicatori della qualità di adempimento delle richieste KSN, indicatori della qualità di elaborazione dei pacchetti KSN, indicatori del numero di richieste KSN e informazioni sui tipi di richieste KSN, data e ora di inizio e fine dell'invio delle statistiche; Informazioni sugli aggiornamenti della configurazione KSN: identificatore della configurazione attiva, identificatore della configurazione ricevuta, codice di errore dell'aggiornamento della configurazione.

- Informazioni sugli eventi del registro di sistema: ora dell'evento, nome del registro in cui è stato rilevato l'evento, tipo e categoria dell'evento, nome dell'origine dell'evento e descrizione dell'evento.

- Informazioni per determinare la reputazione dei file e gli indirizzi URL: l'indirizzo URL a cui si chiede la reputazione e il Referrer, il tipo di protocollo della connessione, l'ID interno del tipo di applicazione, il numero della porta in uso, l'ID Utente, il checksum del file analizzato (MD5), il tipo di minaccia rilevata e le informazioni sul registro utilizzato per rilevare una minaccia (l'identificatore del registro per il database anti-virus, il tipo e la marca temporale); chiave pubblica del certificato; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash.

- Dati sulla distribuzione territoriale dell'applicazione: data di installazione e attivazione dell'applicazione, ID del partner che fornisce la licenza per l'attivazione dell'applicazione, ID dell'applicazione, ID localizzazione lingua applicazione, numero di serie della licenza di attivazione dell'applicazione, indicazione di partecipazione a KSN.

- Informazioni sulla licenza utilizzata: tipo di licenza e relativo periodo di validità, numero di giorni restanti prima della scadenza della licenza, identificatore del partner dal quale la licenza è stata acquistata, identificatore del Centro regionale di attivazione, checksum del codice di attivazione, hash del corpo del ticket calcolato tramite l'algoritmo SHA1, data e ora di creazione del ticket di licenza, identificatore dei dati della licenza, identificatore del ticket della licenza, identificatore di sequenza del ticket della licenza, identificatore univoco del computer dell'utente, data di inizio validità del ticket della licenza, data di fine validità del ticket della licenza, stato corrente del ticket della licenza, versione intestazione ticket, versione della licenza, identificatore certificato di firma intestazione ticket, checksum del file chiave, numero di serie firmatario intestazione ticket, token di autenticazione.

- - Informazioni sull'hardware installato nel computer; tipo, nome, nome del modello, versione firmware, parametri dei dispositivi integrati e collegati.

- Informazioni su dispositivo: ID dispositivo.

- Informazioni sul funzionamento del componente Controllo Web: versione del componente, motivo della categorizzazione, informazioni aggiuntive sul motivo della categorizzazione, URL categorizzato, indirizzo IP host dell'oggetto bloccato/categorizzato.

Quando l'infrastruttura di KSN Privato viene utilizzata da Kaspersky Security Center e si sceglie di partecipare a Kaspersky Security Network nelle impostazioni dei criteri, Kaspersky Endpoint Security non invia le statistiche dai computer client a cui è applicato il criterio a Kaspersky.

Dopo l'eliminazione o l'inattività di un criterio, le impostazioni KSN in un computer client tornano allo stato iniziale.

Passaggio 9. Configurare le impostazioni di interazione con l'utente

Nella finestra **Interazione utente** configurare le impostazioni di Kaspersky Endpoint Security per l'interazione con l'utente del computer client, se necessario.

Passaggio 10. Configurare le impostazioni della connessione di rete

Nella finestra **Rete** eseguire le seguenti operazioni se necessario:

- Configurare la connessione a un server proxy.

- Abilitare o disabilitare la scansione del traffico HTTPS in entrata e in uscita.

- Selezionare l'archivio certificati per il controllo del traffico HTTPS criptato nel browser Mozilla Firefox.

- Gestire l'elenco dei certificati radice attendibili.

- Configurare le porte monitorate.

  È possibile creare un elenco di porte monitorate da Kaspersky Endpoint Security.

Passaggio 11. Configurare le impostazioni relative a Rapporti e backup

Nella finestra **Rapporti e backup** eseguire le seguenti operazioni se necessario:

- Configurare le impostazioni per la generazione e l'archiviazione dei rapporti.

- Configurare le impostazioni per l'archiviazione degli oggetti in Backup.

Passaggio 12. Configurare il criptaggio disco FileVault

Nella finestra **Criptaggio disco FileVault** eseguire le seguenti operazioni se necessario:

- Abilitare o disabilitare la gestione del criptaggio disco FileVault per il disco di avvio dell'utente.

  Per impostazione predefinita, la gestione del criptaggio disco FileVault è disabilitata.

- Selezionare l'opzione **Cripta disco** se si desidera criptare il disco di avvio dell'utente quando il criterio viene applicato a un computer client.

Se la casella di controllo **Abilita gestione criptaggio disco FileVault** è deselezionata, gli utenti con i diritti di amministratore possono criptare e decriptare i propri dischi di avvio Mac dalle impostazioni di sistema.

Se la casella di controllo **Abilita gestione criptaggio disco FileVault** e l'opzione **Cripta disco** sono selezionate, gli utenti con diritti di amministrazione non possono decriptare il disco di avvio del proprio Mac dalle impostazioni di sistema.

Se la casella di controllo **Abilita gestione criptaggio disco FileVault** e l'opzione **Decripta disco** sono selezionate, gli utenti con diritti di amministratore non possono criptare il disco di avvio del proprio Mac dalle impostazioni di sistema.

Passaggio 13. Configurare Controllo Web

Nella finestra **Controllo Web** eseguire le seguenti operazioni se necessario:

- Attivare/disattivare Controllo Web.

> **Nota:** se si abilita Controllo Web per bloccare l'accesso alle risorse Web pericolose, Kaspersky Endpoint Security visualizza la notifica **Controllo Web abilitato** in Centro protezione nel computer remoto. Kaspersky Endpoint Security visualizza le notifiche quando l'utente accede alle risorse Web bloccate da Controllo Web nel computer remoto se la casella **Controlla connessioni protette (HTTPS)** è selezionata nella finestra **Rete** della Creazione guidata nuovo criterio.

- Aggiungere una nuova regola per Controllo Web facendo clic su **Aggiungi**.

  È possibile immettere il nome di una regola, scegliere se la regola è attiva, specificare un'area della regola creando un elenco di indirizzi Web specifici o selezionando le categorie di siti Web e selezionare un'azione che deve essere eseguita da Kaspersky Endpoint Security quando un utente accede a un sito Web incluso in questa regola.

- Modificare, eliminare o organizzare le regole create nell'elenco.

L'ordinamento delle regole determina la priorità della relativa applicazione da parte di Kaspersky Endpoint Security.

Passaggio 14. Configurare Managed Detection and Response

Nella finestra **Managed Detection and Response** eseguire le seguenti operazioni se necessario:

- Abilitare o disabilitare il componente Managed Detection and Response.

  Per impostazione predefinita, Managed Detection and Response è disabilitato.

- Importare o eliminare un file di configurazione utilizzato per attivare il componente Managed Detection and Response nei dispositivi gestiti.

Se la casella di controllo **Abilita Managed Detection and Response** è selezionata e il file di configurazione MDR viene importato, il componente Managed Detection and Response è attivo e interagisce con il servizio Kaspersky Managed Detection and Response. Questo servizio rileva ed elimina costantemente le minacce per la protezione rivolte all'organizzazione.

Passaggio 15. Configurare Endpoint Detection and Response Expert (on-premise)

Nella finestra **Endpoint Detection and Response Expert (on-premise)** eseguire le seguenti operazioni se necessario:

- Abilitare o disabilitare il componente Endpoint Detection and Response (on-premise).

  Per impostazione predefinita, il componente Endpoint Detection and Response Expert (on-premise) è disabilitato.

- Configurare le impostazioni di connessione al server e aggiungere un certificato TLS.

- Aggiungere un server.

Se la casella di controllo **Abilitare Endpoint Detection and Response Expert (7.1 o versioni precedenti)** è selezionata e vengono aggiunti un certificato TLS e un server, il componente Endpoint Detection and Response Expert (on-premise) è attivo e interagisce con la soluzione Kaspersky Anti Targeted Attack Platform. Questa soluzione rileva prontamente le minacce avanzate, come attacchi mirati, minacce persistenti avanzate, attacchi zero-day e altro.

Passaggio 16. Configurare la Scansione dischi esterni

Nella finestra **Scansione dischi esterni**, configurare le seguenti impostazioni:

- L'azione eseguita da Kaspersky Endpoint Security quando è connesso un disco esterno.

- L'azione eseguita da Kaspersky Endpoint Security in caso di rilevamento di un oggetto dannoso.

Passaggio 17. Configurare Rilevamento del Comportamento

Nella finestra **Rilevamento del comportamento** eseguire le seguenti operazioni se necessario:

- Abilitare o disabilitare Rilevamento del Comportamento.

  Per impostazione predefinita, Rilevamento del Comportamento è abilitato.

- Selezionare l'azione da eseguire quando viene rilevata un'attività malware.

- Abilitare o disabilitare la protezione delle cartelle condivise dal criptaggio esterno.

  - Selezionare l'azione da eseguire quando viene rilevata un'attività malware.

Passaggio 18. Configurare Protezione minacce di posta

Nella finestra **Protezione minacce di posta** eseguire le seguenti operazioni se necessario:

- Abilitare o disabilitare Protezione minacce di posta.

  Per impostazione predefinita, Protezione Minacce di Rete è abilitato.

- Selezionare l'azione da eseguire al rilevamento di un oggetto dannoso.

- Configurare le impostazioni di Protezione minacce di posta.

Passaggio 19. Configurare Prevenzione Exploit

Nella finestra **Prevenzione Exploit** eseguire le seguenti operazioni se necessario:

- Abilitare o disabilitare Prevenzione Exploit.
  Per impostazione predefinita, Prevenzione Exploit è abilitato.
- Selezionare l'azione da eseguire al rilevamento di un exploit.

Passaggio 20. Configurare Motore di Remediation

Nella finestra **Motore di Remediation** eseguire le seguenti operazioni se necessario:

- Abilitare o disabilitare Motore di Remediation.
  Per impostazione predefinita, Motore di Remediation è abilitato.

Passaggio 21. Configurare Controllo dispositivi

Nella finestra **Controllo dispositivi** eseguire le seguenti operazioni se necessario:

- Abilitare o disabilitare Controllo dispositivi.
  Per impostazione predefinita, Controllo dispositivi è abilitato.
- Configurare le impostazioni di Controllo dispositivi.

Passaggio 22. Configura Firewall

Nella finestra **Firewall** eseguire le seguenti operazioni se necessario:

- Abilitare o disabilitare Firewall.
  Per impostazione predefinita, Firewall è abilitato.
- Configurare le impostazioni Firewall.

Passaggio 23. Definire il gruppo di amministrazione a cui verrà applicato il criterio

Nella finestra **Gruppo di destinazione** fare clic su **Sfoglia** per selezionare un gruppo di amministrazione a cui si desidera applicare il criterio.

Passaggio 24. Selezionare lo stato del criterio e completare la creazione di un criterio

Nella finestra **Creare un criterio di gruppo per l'applicazione** eseguire le seguenti operazioni:

1. Selezionare lo stato che verrà assegnato al criterio:
   - *Criterio attivo*: il criterio viene applicato al gruppo di amministrazione selezionato.
   - *Criterio inattivo*: il criterio non viene applicato.
   - *Criterio fuori sede*: il criterio viene applicato al gruppo di amministrazione selezionato quando i computer vengono disconnessi dalla rete aziendale.

   Nota: è possibile creare più criteri per un'applicazione in un gruppo di amministrazione, ma solo uno di questi può essere attivo.

Per informazioni dettagliate sugli stati dei criteri, vedere la Guida di Kaspersky Security Center.

2. Selezionare la casella di controllo **Apri le proprietà del criterio subito dopo la creazione** se si desidera rivedere le impostazioni dei criteri dopo la relativa creazione.

3. Fare clic su **Fine** per chiudere la Creazione guidata nuovo criterio.

   Il criterio creato viene visualizzato nella scheda **Criteri** nell'area di lavoro del gruppo di amministrazione di riferimento. Il criterio viene applicato ai computer client dopo la prima sincronizzazione con Administration Server.

È possibile modificare le impostazioni del criterio creato. È inoltre possibile proibire o consentire le modifiche per ogni gruppo di impostazioni da un computer client utilizzando i pulsanti e per ogni gruppo di impostazioni. Il pulsante accanto a un gruppo di impostazioni indica che all'utente di un computer client non è consentito modificare queste impostazioni nel computer dell'utente. Il pulsante accanto a un gruppo di impostazioni indica che all'utente di un computer client è consentito modificare queste impostazioni nel computer dell'utente.

Visualizzare l'elenco dei criteri

È possibile creare un numero illimitato di vari criteri per le applicazioni installate nei computer in ciascun gruppo di amministrazione, ma per ogni applicazione può essere applicato un solo criterio per volta all'interno di un gruppo di amministrazione.

Visualizzare l'elenco dei criteri di un gruppo di amministrazione

1. Avviare Kaspersky Security Center Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nella struttura della console fare clic su **Dispositivi gestiti**.

4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.

5. Nell'area di lavoro selezionare la scheda **Criteri**.

   Viene visualizzato l'elenco dei criteri.

Configurare le impostazioni dei criteri

È possibile apportare modifiche al criterio creato in Kaspersky Security Center e bloccare qualsiasi modifica relativa alle impostazioni nei criteri dei sottogruppi e nelle impostazioni delle attività.

Le impostazioni dei criteri di Kaspersky Endpoint Security includono le impostazioni dell'applicazione e le impostazioni delle attività.

Configurare le impostazioni dei criteri

1. Avviare Kaspersky Security Center Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nella struttura della console fare clic su **Dispositivi gestiti**.

4. Nell'area di lavoro selezionare la scheda **Criteri**.

5. Fare clic con il pulsante destro del mouse sul criterio che si desidera configurare e scegliere **Proprietà**.

6. Nella finestra **Proprietà: <Nome criterio>** configurare le impostazioni del criterio:

- Nella sezione **Protezione minacce essenziale**

  Configurare le seguenti impostazioni di Protezione Minacce File

  - Attivare/disattivare Protezione Minacce File.
  - Selezionare uno dei livelli di protezione preimpostati o configurare le impostazioni di protezione manualmente.
  - Selezionare l'azione da eseguire al rilevamento di un oggetto dannoso.

  Configurare le seguenti impostazioni di Protezione Minacce Web

  - Attivare/disattivare Protezione Minacce Web.
  - Selezionare uno dei livelli di protezione preimpostati o configurare le impostazioni di protezione manualmente.
  - Abilitare o disabilitare il controllo degli indirizzi Web in base al database degli indirizzi Web dannosi.
  - Configurare le impostazioni di Anti-Phishing.
  - Aggiungere gli indirizzi attendibili il cui traffico non verrà esaminato da Protezione Minacce Web.
  - Selezionare l'azione da eseguire al rilevamento di un oggetto dannoso nel traffico Web.

  Configurare le seguenti impostazioni di Protezione minacce di posta

  - Abilitare o disabilitare Protezione minacce di posta.
  - Selezionare l'azione da eseguire al rilevamento di un oggetto dannoso.
  - Configurare le impostazioni di Protezione minacce di posta.

  Configurare le seguenti impostazioni di Protezione Minacce di Rete

  - Attivare/disattivare Protezione Minacce di Rete.
  - Configurare le impostazioni di Protezione Minacce di Rete.
  - Specificare gli indirizzi IP dei computer la cui attività di rete non verrà bloccata.

  Configurare le seguenti impostazioni Firewall

  - Abilitare o disabilitare Firewall.
  - Configurare le impostazioni Firewall.

- Nella sezione **Protezione minacce avanzata**

Configurare le seguenti impostazioni KSN

- Leggere il testo completo dell'Informativa di Kaspersky Security Network facendo clic su **Informativa KSN**.
- Attivare o disattivare l'utilizzo di Kaspersky Security Network.
- Abilitare o disabilitare la modalità KSN estesa.
- Attivare/disattivare la modalità cloud.
- Abilitare o disabilitare l'utilizzo di un proxy KSN.
- Abilitare o disabilitare l'utilizzo dei server Kaspersky quando il proxy KSN non è disponibile.

Nota: l'utilizzo di Kaspersky Security Network e di un proxy KSN nei computer remoti è disponibile solo se Kaspersky Security Center Administration Server viene utilizzato come server proxy. Per informazioni dettagliate sulle proprietà di Administration Server, vedere la Guida di Kaspersky Security Center.

Configurare le seguenti impostazioni di Rilevamento del Comportamento

- Abilitare o disabilitare Rilevamento del Comportamento.

  Per impostazione predefinita, Rilevamento del Comportamento è abilitato.
- Selezionare l'azione da eseguire quando viene rilevata un'attività malware.

Configurare le seguenti impostazioni di Prevenzione Exploit

- Abilitare o disabilitare Prevenzione Exploit.
- Selezionare l'azione da eseguire al rilevamento di un exploit.

Configurare le seguenti impostazioni di Motore di Remediation

Abilitare o disabilitare Motore di Remediation.

- Nella sezione **Controlli di sicurezza**

  Configurare le seguenti impostazioni di Controllo dispositivi

  - Abilitare o disabilitare Controllo dispositivi.
  - Configurare le impostazioni di Controllo dispositivi.

  Configurare le seguenti impostazioni di Controllo Web

  - Attivare/disattivare Controllo Web.
  - Aggiungere una nuova regola per Controllo Web facendo clic su **Aggiungi**.
  - Modificare, eliminare o organizzare le regole create nell'elenco.
- Nella sezione **Criptaggio dei dati**

Configurare le seguenti impostazioni di criptaggio disco FileVault

- Abilitare o disabilitare la gestione del criptaggio disco FileVault per i computer client.
- Criptare o decriptare il disco di avvio nei computer client.

  Se la casella di controllo **Abilita gestione criptaggio disco FileVault** è deselezionata, gli utenti con i diritti di amministratore possono criptare e decriptare i propri dischi di avvio Mac dalle impostazioni di sistema.

  Se la casella di controllo **Abilita gestione criptaggio disco FileVault** e l'opzione **Cripta disco** sono selezionate, gli utenti con diritti di amministrazione non possono decriptare il disco di avvio del proprio Mac dalle impostazioni di sistema.

  Se la casella di controllo **Abilita gestione criptaggio disco FileVault** e l'opzione **Decripta disco** sono selezionate, gli utenti con diritti di amministratore non possono criptare il disco di avvio del proprio Mac dalle impostazioni di sistema.

- Nella sezione **Detection and Response**

  Configurare le seguenti impostazioni di Managed Detection and Response

  - Abilitare o disabilitare il componente Managed Detection and Response.
  - Importare o eliminare un file di configurazione utilizzato per attivare il componente Managed Detection and Response nei dispositivi gestiti.

  Configurare le seguenti impostazioni di Endpoint Detection and Response (KATA)

  - Abilitare o disabilitare il componente Endpoint Detection and Response (KATA).
  - Configurare le impostazioni di connessione al server e aggiungere un certificato TLS.
  - Aggiungere un server KATA.

- Nella sezione **Attività locali**

  Configurare le seguenti impostazioni di Scansione dischi esterni

  - L'azione eseguita da Kaspersky Endpoint Security quando è connesso un disco esterno.
  - L'azione eseguita da Kaspersky Endpoint Security in caso di rilevamento di un oggetto dannoso.

- Nella sezione **Aggiornamento**

  Configurare le seguenti impostazioni di aggiornamento

  - Attivare o disattivare l'aggiornamento dei moduli dell'applicazione.
  - Specificare le sorgenti degli aggiornamenti.

- Nella sezione **Impostazioni avanzate**

  Configurare le seguenti impostazioni di protezione

  - Abilitare o disabilitare la protezione in tempo reale del computer client.
  - Abilitare o disabilitare l'avvio di Kaspersky Endpoint Security all'avvio del computer client.
  - Configurare Area attendibile.
  - Configurare Applicazioni attendibili.

- Selezionare i tipi di oggetti da rilevare.
- Disabilitare o abilitare l'avvio delle attività pianificate quando il computer funziona con alimentazione a batteria.

Configurare le seguenti impostazioni di rete

- Abilitare o disabilitare l'utilizzo di un server proxy.
- Specificare l'indirizzo del server proxy.
- Abilitare o disabilitare l'utilizzo di un server proxy per gli indirizzi locali.
- Specificare il nome utente e la password per l'autenticazione del server proxy.
- Abilitare o disabilitare la scansione del traffico HTTPS in entrata e in uscita.
- Selezionare l'archivio certificati per il controllo del traffico HTTPS criptato nel browser Mozilla Firefox.
- Configurare le porte monitorate.

Configurare le seguenti impostazioni relative a Rapporti e backup

- Abilitare o disabilitare il salvataggio degli eventi non critici nel rapporto.
- Abilitare o disabilitare il salvataggio solo degli eventi recenti.
- Abilitare o disabilitare la rimozione degli eventi dopo il periodo specificato.
- Specificare il periodo per l'archiviazione degli eventi.
- Abilitare o disabilitare la rimozione degli oggetti da Backup dopo il periodo specificato.
- Specificare il periodo per l'archiviazione degli oggetti in Backup.

Configurare le seguenti impostazioni di interazione utente

- Abilitare o disabilitare le notifiche degli eventi.
- Selezionare il modo in cui Kaspersky Endpoint Security invierà una notifica all'utente relativa agli eventi.
- Abilitare o disabilitare la visualizzazione dell'icona di Kaspersky Endpoint Security nella barra dei menu.
- Stabilire se un utente può aprire la finestra principale di Kaspersky Endpoint Security e utilizzare l'interfaccia dell'applicazione in un computer client.
- Abilitare o disabilitare la disponibilità dell'elemento **Esci** nel menu di scelta rapida dell'icona di Kaspersky Endpoint Security nel computer client.
- Selezionare la lingua utilizzata per visualizzare gli eventi di Kaspersky Security Center.
- Configurare le impostazioni di Kaspersky Endpoint Security disponibili per gli utenti del computer client.
- Configurare Protezione tramite password per limitare le azioni indesiderate nei dispositivi degli utenti.

7. Fare clic su **OK** per salvare le modifiche e chiudere la finestra delle proprietà dei criteri.

Modificare lo stato del criterio

Lo stato del criterio definisce il funzionamento di un criterio. Il criterio può avere lo stato attivo, fuori sede o inattivo. È possibile modificare lo stato del criterio nelle impostazioni del criterio.

Modificare lo stato del criterio

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.
5. Nell'area di lavoro selezionare la scheda **Criteri**.
6. Fare clic con il pulsante destro del mouse sul criterio per cui si desidera modificare lo stato e scegliere **Proprietà** nel menu di scelta rapida.
7. Nella finestra **Proprietà: <Nome criterio>** selezionare la sezione **Generale**.
8. Nella sezione **Stato del criterio** selezionare uno dei seguenti stati per il criterio:
   - **Criterio attivo**. Il criterio viene sempre applicato al gruppo di amministrazione selezionato.
   - **Criterio fuori sede**. Il criterio viene applicato al gruppo di amministrazione selezionato quando i computer client vengono disconnessi dalla rete aziendale.
   - **Criterio inattivo**. Il criterio non viene applicato al gruppo di amministrazione selezionato.
9. Fare clic su **OK** per salvare le modifiche e chiudere la finestra **Proprietà: <Nome criterio>**.

Esportare un criterio in un file KLP

È possibile esportare un criterio personalizzato in un file per utilizzare questo criterio in un altro Administration Server.

Esportare un criterio in un file KLP

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.
5. Nell'area di lavoro selezionare la scheda **Criteri**.

6. Fare clic con il pulsante destro del mouse sul criterio per visualizzare il relativo menu di scelta rapida e scegliere **Esporta**.

   Verrà visualizzata la finestra **Salva con nome**.

7. Selezionare la cartella in cui si desidera salvare il file KLP per il criterio.

8. Specificare il nome del file.

9. Fare clic su **Salva** per salvare il file nella cartella selezionata.

Importare un criterio da un file KLP

È possibile importare un criterio esistente con impostazioni predefinite da un file.

Importare un criterio da un file KLP

1. Avviare Kaspersky Security Center Administration Console.

2. Ingrandire il nodo **Administration Server <nome server>**.

3. Nella struttura della console fare clic su **Dispositivi gestiti**.

4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.

5. Nell'area di lavoro selezionare la scheda **Criteri**.

6. Aprire la finestra di selezione in uno dei seguenti modi:

   - Facendo clic sul pulsante **Importa criteri da file**;

   - Facendo clic con il pulsante destro del mouse su un'area vuota nell'area di lavoro per aprire il menu di scelta rapida e selezionando l'elemento **Importa**.

7. Selezionare un file KLP con un criterio e fare clic su **Apri**.

Il criterio importato viene aggiunto all'elenco dei criteri nell'area di lavoro.

Creare e gestire i profili criterio

Un profilo criterio è un set denominato di impostazioni variabili per un criterio, attivato in un computer client quando vengono soddisfatte condizioni specifiche. L'attivazione di un profilo modifica le impostazioni del criterio attive nel dispositivo all'attivazione del profilo criterio.

Creare un profilo criterio

1. Nell'albero della console selezionare il gruppo di amministrazione per cui si desidera creare un profilo criterio.

2. Nell'area di lavoro selezionare la scheda **Criteri**.

3. Eseguire una delle seguenti operazioni per aprire le proprietà del criterio per cui si desidera creare un profilo:

   - Fare doppio clic sul nome del criterio.
   - Fare clic con il pulsante destro del mouse sul nome del criterio per visualizzare il menu di scelta rapida e scegliere **Proprietà**.
   - Fare clic sul collegamento **Configura criterio**.

4. Nella finestra **Proprietà: <Nome criterio>** selezionare la sezione **Profili criterio**.

5. Nell'area di lavoro fare clic su **Aggiungi**.

6. Nella finestra **Assegnazione dei profili criterio** leggere le informazioni sui criteri e fare clic sul pulsante **Avanti**.

   Se non si desidera visualizzare questa finestra quando si creano nuovi profili criterio, selezionare la casella di controllo **Non visualizzare più questa finestra** prima di fare clic su **Avanti**.

7. Nella finestra **Nome profilo criterio** procedere come segue per configurare il profilo criterio:

   - Immettere il nome del nuovo profilo criterio.

     > **Nota:** il nome di un profilo non può includere più di 100 caratteri.

   - Nella sezione **Stato profilo criterio** selezionare se il profilo criterio è abilitato o disabilitato.
   - Nell'elenco a discesa nella sezione **Stato profilo criterio** selezionare se il profilo criterio può essere modificato.
   - Se si desidera configurare le regole di attivazione per il profilo criterio, selezionare la casella di controllo **Dopo aver chiuso la Creazione guidata nuovo profilo criterio, passa alla configurazione della regola di attivazione del profilo criterio**.

8. Fare clic su **Fine**.

9. Se è stata selezionata la casella di controllo **Dopo aver chiuso la Creazione guidata nuovo profilo criterio, passa alla configurazione della regola di attivazione del profilo criterio**, procedere con i passaggi della Creazione guidata nuova regola di attivazione di un profilo criterio.

Il profilo criterio creato viene visualizzato nella sezione **Profili criterio** della finestra **Proprietà: <Nome criterio>**.

Creare una regola di attivazione profilo criterio

1. Nell'albero della console selezionare il gruppo di amministrazione in cui si desidera creare una regola di attivazione profilo criterio.

2. Nell'area di lavoro selezionare la scheda **Criteri**.

3. Per aprire le proprietà del criterio, eseguire una delle seguenti operazioni:

   - Fare doppio clic sul nome del criterio.
   - Fare clic con il pulsante destro del mouse sul nome del criterio per visualizzare il menu di scelta rapida e scegliere **Proprietà**.
   - Fare clic sul collegamento **Configura criterio**.

4. Nella finestra **Proprietà: <Nome criterio>** selezionare la sezione **Profili criterio**.

5. Nell'area di lavoro selezionare il profilo criterio per cui si desidera creare una regola di attivazione, quindi fare clic su **Proprietà**.

   Verrà visualizzata la finestra **Proprietà: <Nome profilo criterio>**.

6. Selezionare la sezione **Regole di attivazione**.

7. Nell'area di lavoro fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova regola di attivazione di un profilo criterio.

Seguire i passaggi della Creazione guidata nuova regola di attivazione di un profilo criterio.

Modificare un profilo criterio

1. Nell'albero della console selezionare il gruppo di amministrazione per cui si desidera modificare un profilo criterio.

2. Nell'area di lavoro selezionare la scheda **Criteri**.

3. Eseguire una delle seguenti operazioni per aprire le proprietà del criterio per cui si desidera modificare un profilo:

   - Fare doppio clic sul nome del criterio.
   - Fare clic con il pulsante destro del mouse sul nome del criterio per visualizzare il menu di scelta rapida e scegliere **Proprietà**.
   - Fare clic sul collegamento **Configura criterio**.

4. Nella finestra **Proprietà: <Nome criterio>** selezionare la sezione **Profili criterio**.

5. Nell'area di lavoro selezionare il profilo criterio che si desidera modificare e fare clic su **Proprietà**.

   Verrà visualizzata la finestra **Proprietà: <Nome profilo criterio>**.

6. Configurare il profilo se necessario:

   - Nella sezione **Generale** rinominare il profilo o abilitare/disabilitare il profilo selezionando/deselezionando la casella di controllo **Abilita profilo**.
   - Nella sezione **Regole di attivazione** creare, modificare o eliminare le regole di attivazione.
   - Nella sezione **Dispositivi** selezionare i dispositivi a cui viene applicato il profilo criterio.
   - Modificare le impostazioni del criterio nelle sezioni attinenti.

7. Fare clic su **OK**.

Se il profilo criterio è attivo, le impostazioni modificate saranno applicate dopo la sincronizzazione del computer client con Administration Server. Se il profilo criterio è inattivo, queste saranno applicate dopo l'attivazione della regola.

Modificare la priorità di un profilo criterio

1. Nell'albero della console selezionare il gruppo di amministrazione per cui si desidera modificare la priorità di un profilo criterio.
2. Nell'area di lavoro selezionare la scheda **Criteri**.
3. Eseguire una delle seguenti operazioni per aprire le proprietà del criterio per cui si desidera modificare la priorità di un profilo criterio:
   - Fare doppio clic sul nome del criterio.
   - Fare clic con il pulsante destro del mouse sul nome del criterio per visualizzare il menu di scelta rapida e scegliere **Proprietà**.
   - Fare clic sul collegamento **Configura criterio**.
4. Nella finestra **Proprietà: <Nome criterio>** selezionare la sezione **Profili criterio**.
5. Nell'area di lavoro selezionare il profilo criterio per cui si desidera modificare la priorità.
6. Aumentare o ridurre la priorità del profilo selezionato facendo clic sui pulsanti  .

Eliminare un profilo criterio

1. Nell'albero della console selezionare il gruppo di amministrazione per cui si desidera eliminare un profilo criterio.
2. Nell'area di lavoro selezionare la scheda **Criteri**.
3. Eseguire una delle seguenti operazioni per aprire le proprietà del criterio per cui si desidera eliminare un profilo:
   - Fare doppio clic sul nome del criterio.
   - Fare clic con il pulsante destro del mouse sul nome del criterio per visualizzare il menu di scelta rapida e scegliere **Proprietà**.
   - Fare clic sul collegamento **Configura criterio**.
4. Nella finestra **Proprietà: <Nome criterio>** selezionare la sezione **Profili criterio**.
5. Nell'area di lavoro selezionare il profilo che si desidera eliminare e fare clic su **Elimina**.

Per informazioni dettagliate sui profili criterio, vedere la Guida di Kaspersky Security Center.

Generare un rapporto sugli oggetti rilevati

Generare un rapporto sugli oggetti rilevati

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console fare clic su **Dispositivi gestiti**.
4. Selezionare il gruppo di amministrazione che contiene il computer client richiesto.
5. Selezionare la scheda **Dispositivi**.
6. Selezionare il computer dall'elenco dei computer client.
7. Fare clic con il pulsante destro del mouse sul computer selezionato per aprire il menu di scelta rapida, quindi scegliere **Tutte le attività** > **Visualizza rapporto sulle minacce**.

Il rapporto generato viene visualizzato in una finestra del browser.

Le informazioni sulle altre modalità di generazione di un rapporto sugli oggetti rilevati dall'applicazione nel computer client sono disponibili nella Guida di Kaspersky Security Center.

Ottenere una chiave di ripristino per un'unità criptata

Se un utente di un computer client dimentica o smarrisce le credenziali e non può accedere a un'unità criptata, è possibile ottenere una chiave di ripristino.

Ottenere una chiave di ripristino

1. Avviare Kaspersky Security Center Administration Console.
2. Ingrandire il nodo **Administration Server <nome server>**.
3. Nella struttura della console selezionare la cartella **Avanzate**, quindi la sottocartella **Criptaggio e protezione dei dati** e la sottocartella **Unità criptate**.
4. Nell'area di lavoro fare clic con il pulsante destro del mouse sul dispositivo con il disco criptato per visualizzare il menu di scelta rapida e selezionare **Ottieni chiave di ripristino per macOS**.

   Verrà visualizzata una finestra con la chiave di ripristino.
5. Salvare la chiave di ripristino nel modo più idoneo.

È possibile utilizzare questa chiave di ripristino in un computer client per accedere all'unità criptata.

Amministrazione remota dell'applicazione tramite Kaspersky Security Center Web Console e Cloud Console

Kaspersky Security Center Web Console (Web Console) è un'applicazione Web che consente di eseguire in modo centralizzato le principali attività di gestione e manutenzione della sicurezza di rete di un'organizzazione. Web Console è un componente di Kaspersky Security Center che offre un'interfaccia utente per la gestione di Kaspersky Endpoint Security in una finestra del browser. Per informazioni dettagliate su Kaspersky Security Center Web Console, vedere la Guida di Kaspersky Security Center.

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

È inoltre possibile gestire Kaspersky Endpoint Security tramite l'interfaccia utente grafica dell'applicazione, Kaspersky Security Center Administration Console e la riga di comando.

Installare il plug-in Web di Kaspersky Endpoint Security

Il plug-in Web di Kaspersky Endpoint Security consente l'interazione tra Kaspersky Endpoint Security e Kaspersky Security Center. Il plug-in Web deve essere installato in un dispositivo in cui è installato Kaspersky Security Center Web Console. La funzionalità del plug-in Web è disponibile per tutti gli amministratori che hanno accesso a Kaspersky Security Center Web Console in un browser.

È possibile installare il plug-in Web come segue:

- Utilizzo dell'Avvio rapido guidato di Kaspersky Security Center Web Console.

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

- Manualmente, utilizzando un pacchetto di distribuzione per Web Console da un'origine esterna.

  Per installare il plug-in Web, aggiungere l'archivio ZIP del pacchetto di distribuzione per il plug-in Web di Kaspersky Endpoint Security nell'interfaccia di Web Console: **Impostazioni** → **Plug-in Web**. Il pacchetto di distribuzione del plug-in Web può essere scaricato dal sito Web di Kaspersky.

Per installare manualmente il plug-in Web di Kaspersky Endpoint Security:

1. Nella finestra principale di Kaspersky Security Center Web Console selezionare **Impostazioni** → **Plug-in Web**.

   Viene aperto un elenco dei plug-in Web installati.

2. Avviare l'installazione del plug-in Web di Kaspersky Endpoint Security in uno dei seguenti modi:

   - Installazione dall'elenco dei plug-in Web di Kaspersky:

     a. Fare clic su **Aggiungi**.

        Verrà visualizzato un elenco di tutti i plug-in Web di Kaspersky disponibili. L'elenco viene aggiornato automaticamente dopo il rilascio di nuove versioni dei plug-in Web.

     b. Individuare il plug-in Web di Kaspersky Endpoint Security for Mac 12.2.1 nell'elenco e fare clic sul relativo nome.

     c. Nella finestra con la descrizione del plug-in Web, fare clic sul pulsante **Installa plug-in**.

     d. Attendere il completamento dell'installazione e fare clic su **OK** nella finestra delle informazioni.

   - Installazione del plug-in Web da una fonte esterna (gli archivi necessari per l'installazione dei plug-in Web sono inclusi nel kit di distribuzione):

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

     b. Nella finestra visualizzata specificare il percorso dell'archivio ZIP con il kit di distribuzione per il plug-in Web e il percorso del file della firma in formato TXT. Questo file si trova nell'archivio con il plug-in Web.

     c. Fare clic su **Aggiungi**.

     d. Attendere il completamento dell'installazione e fare clic su **OK** nella finestra delle informazioni.

Il nuovo plug-in viene visualizzato nell'elenco dei plug-in Web installati (**Impostazioni** → **Plug-in Web**).

Nota: se si seleziona una lingua non inclusa nel pacchetto di distribuzione di Kaspersky Endpoint Security nelle proprietà di Kaspersky Security Center Administration Server, il Contratto di licenza e l'intera interfaccia di Kaspersky Security Center Web Console verranno visualizzati in inglese.

Creare un criterio

Questa sezione contiene informazioni su come creare e configurare criteri per Kaspersky Endpoint Security utilizzando Kaspersky Security Center Web Console e Cloud Console.

Un criterio determina le impostazioni di un'applicazione e gestisce la possibilità di configurare tale applicazione nei dispositivi all'interno di un gruppo di amministrazione. Per ogni applicazione è necessario creare un criterio individuale. È possibile creare un numero illimitato di vari criteri per le applicazioni installate nei dispositivi in ciascun gruppo di amministrazione, ma per ogni applicazione può essere applicato un solo criterio per volta all'interno di un gruppo di amministrazione.

Nota: durante la creazione e la configurazione di un criterio, è possibile consentire o vietare le modifiche per i gruppi di impostazioni nei criteri utilizzando l'interruttore **Applica**.

Creare un criterio

1. Nella sezione **Dispositivi** a sinistra selezionare la sezione **Criteri e profili**.
2. Fare clic su **Aggiungi**.
3. Selezionare l'applicazione per cui creare un criterio e fare clic su **Avanti**.

   Verrà visualizzata la finestra **Nuovo criterio**.
4. Nella scheda **Generale** specificare il nome del criterio e configurare lo stato del criterio e le opzioni di ereditarietà delle impostazioni del criterio.
5. Nella scheda **Impostazioni applicazione** configurare le impostazioni dell'applicazione che verranno applicate a Kaspersky Endpoint Security nel computer client quando viene applicato il criterio.
6. Fare clic su **Salva**.

È possibile eseguire le seguenti azioni sui criteri personalizzati:

- Creare i criteri.
- Configurare i criteri.
- Copiare o spostare i criteri da un gruppo all'altro.
- Eliminare criteri.
- Modificare lo stato dei criteri.

Per informazioni dettagliate sui criteri di Kaspersky Security Center Web Console, vedere la Guida di Kaspersky Security Center.

Per informazioni dettagliate sui criteri di Kaspersky Security Center Cloud Console, vedere la Guida di Kaspersky Security Center Cloud Console.

Nota: dopo aver creato un profilo criterio per un criterio di Kaspersky Endpoint Security utilizzando Kaspersky Security Center Web Console e Cloud Console, è necessario verificare che le impostazioni siano applicate correttamente nei computer client.

Protezione minacce host

Configurare il componente Protezione minacce file

È possibile configurare il componente Protezione minacce file in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Protezione minacce host** > **Protezione minacce file**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione minacce file**.
  6. Configurare il componente Protezione minacce file.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Protezione minacce essenziale** → **Protezione minacce file**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione minacce file**.
  6. Configurare il componente Protezione minacce file.
  7. Salvare le modifiche.

Impostazioni di Protezione minacce file

Impostazioni	Descrizione
Esclusioni dalla scansione	Un'*esclusione dalla scansione* è un set di condizioni che devono essere soddisfatte perché Kaspersky Endpoint Security non esegua la scansione di un determinato oggetto alla ricerca di virus e altre minacce. Le esclusioni dalla scansione consentono di utilizzare senza rischi il software legittimo che utenti malintenzionati possono sfruttare per danneggiare il computer o i dati dell'utente. Benché non presentino funzioni pericolose, le applicazioni di questo tipo possono essere sfruttate dagli utenti malintenzionati. Per ulteriori dettagli sulle applicazioni legittime utilizzabile da utenti malintenzionati per compromettere il computer o i dati personali, consultare il sito Web dell'Enciclopedia IT di Kaspersky.
Azione se viene rilevata una minaccia	**Disinfetta (se non è possibile, elimina)** Se questa opzione è selezionata, l'applicazione tenta automaticamente di disinfettare il file infetto rilevato. Se la disinfezione non riesce, il file viene eliminato. **Richiedi intervento utente**. Kaspersky Endpoint Security visualizza una finestra di notifica con informazioni sull'oggetto dannoso che ha infettato il file e richiede all'utente di scegliere l'azione che deve essere eseguita da Kaspersky Endpoint Security. Le azioni disponibili possono variare in base allo stato dell'oggetto.

Impostazioni	Descrizione
Ambito della protezione	Contiene gli oggetti che sono esaminati dal componente Protezione minacce file. Un oggetto da esaminare può essere un disco rigido, un'unità rimovibile, un'unità di rete, una cartella, un file o più file definiti da una maschera. Per impostazione predefinita, il componente Protezione minacce file esamina i file avviati in tutti i dischi rigidi, le unità rimovibili o le unità di rete. L'ambito di protezione per questi oggetti non può essere modificato o eliminato. È possibile escludere solo un oggetto (ad esempio unità rimovibili) dalle scansioni.
Ottimizzazione della scansione	In **Ottimizzazione della scansione**, è possibile configurare Kaspersky Endpoint Security per prestazioni migliori durante la scansione dei file. • **Esamina solo i file nuovi e modificati** Esamina solo i nuovi file e i file che sono stati modificati dopo l'ultima scansione. Questo consente di ridurre la durata di una scansione. Questa modalità si applica sia ai file semplici che compositi. • **Ignora la scansione del volume di sistema di sola lettura**. Se questa casella di controllo è selezionata, l'applicazione non esegue la scansione del volume di sistema di sola lettura. Questo riduce notevolmente la durata scansione.
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. • **Esamina gli archivi**. Scansione di file ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE e altri archivi. L'applicazione esegue la scansione degli archivi non solo in base all'estensione, ma anche in base al formato. Durante il controllo degli archivi, l'applicazione esegue una decompressione ricorsiva. In questo modo, è possibile rilevare le minacce all'interno di archivi multilivello (archivio all'interno di un archivio). • **Esamina pacchetti di distribuzione e archivi autoestraenti**. Scansione dei pacchetti di installazione delle applicazioni di terze parti e degli archivi autoestraenti. Gli archivi autoestraenti sono dotati di un modulo di estrazione eseguibile. Per eseguire la scansione degli archivi autoestraenti, la casella di controllo **Esamina gli archivi** deve essere selezionata. • **Esamina file nei formati Microsoft Office e oggetti OLE incorporati**. File di Microsoft Office (ad esempio DOC, DOCX, XLS, PPT) e oggetti OLE incorporati nei file (ad esempio tabelle Excel, macro, allegati e-mail).
Consenti la decompressione in background di archivi di dimensioni superiori a (MB)	Se la casella di controllo è selezionata, l'applicazione consente di accedere ai file compositi di dimensioni superiori al valore specificato prima della scansione dei file. In questo caso, Kaspersky Endpoint Security decomprime ed esamina i file compositi in background. L'applicazione consente di accedere ai file compositi di dimensioni inferiori a questo valore solo dopo la decompressione e la scansione dei file. Se la casella di controllo non è selezionata, l'applicazione consente di accedere ai file compositi solo dopo la decompressione e la scansione di file di qualsiasi dimensione.
Non esaminare archivi superiori a (MB)	Se la casella di controllo è selezionata, l'applicazione non esegue la scansione dei file compositi se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, l'applicazione esamina i file compositi di qualsiasi dimensione. L'applicazione esamina i file di grandi dimensioni estratti dagli archivi indipendentemente dal fatto che la casella di controllo sia selezionata o meno.

Configurare la Scansione unità rimovibili

È possibile configurare il componente Scansione unità rimovibili in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Protezione minacce host → Scansione unità rimovibili**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Scansione delle unità rimovibili**.

6. Configurare il componente Scansione unità rimovibili.
7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Attività locali** > **Scansione dischi esterni**.
5. Configurare il componente Scansione unità rimovibili.
6. Salvare le modifiche.

Configurare Rilevamento del Comportamento

È possibile configurare il componente Rilevamento del Comportamento in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare alla sezione **Protezione minacce host** → **Analisi del comportamento** → **Rilevamento del Comportamento**.
5. Abilitare o disabilitare il componente utilizzando l'interruttore **Rilevamento del Comportamento**.
6. Configurare il componente Rilevamento del Comportamento.
7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Accedere a **Protezione minacce avanzata** → **Rilevamento del comportamento**.
5. Abilitare o disabilitare il componente utilizzando l'interruttore **Rilevamento del Comportamento**.

6. Configurare il componente Rilevamento del Comportamento.
7. Salvare le modifiche.

Impostazioni di Rilevamento del Comportamento

Impostazioni	Descrizione
Applicazioni attendibili	L'*elenco delle applicazioni attendibili* è un elenco di applicazioni per cui Kaspersky Endpoint Security non monitora le attività sui file e di rete (incluse le attività dannose) e l'accesso al Registro di sistema. Per impostazione predefinita, Kaspersky Endpoint Security monitora gli oggetti aperti, eseguiti o salvati da qualsiasi processo di applicazione e controlla l'attività di tutte le applicazioni e il traffico di rete che generano. Dopo aver aggiunto un'applicazione all'elenco delle applicazioni attendibili, Kaspersky Endpoint Security interrompe il monitoraggio delle attività dell'applicazione.
Esclusioni dalla scansione	Un'*esclusione dalla scansione* è un set di condizioni che devono essere soddisfatte perché Kaspersky Endpoint Security non esegua la scansione di un determinato oggetto alla ricerca di virus e altre minacce. Le esclusioni dalla scansione consentono di utilizzare senza rischi il software legittimo che utenti malintenzionati possono sfruttare per danneggiare il computer o i dati dell'utente. Benché non presentino funzioni pericolose, le applicazioni di questo tipo possono essere sfruttate dagli utenti malintenzionati. Per ulteriori dettagli sulle applicazioni legittime utilizzabile da utenti malintenzionati per compromettere il computer o i dati personali, consultare il sito Web dell'Enciclopedia IT di Kaspersky .
Azione se viene rilevata una minaccia	**Richiedi azione**. Se viene rilevata un'attività dannosa, Kaspersky Endpoint Security richiede all'utente di selezionare l'azione da eseguire quando viene rilevata un'attività dannosa. Le azioni disponibili possono variare in base allo stato dell'oggetto. **Blocca**. Se vengono rilevate attività dannose, Kaspersky Endpoint Security blocca l'applicazione che esegue le attività dannose e registra le informazioni sulle attività dannose rilevate. **Elimina**. Se questa opzione è selezionata, durante il rilevamento di attività dannose Kaspersky Endpoint Security elimina il file eseguibile dell'applicazione dannosa e crea una copia di backup del file in Backup.

Configurare Anti-Cryptor

È possibile configurare il componente Anti-Cryptor in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**
  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare alla sezione **Protezione minacce host → Analisi del comportamento → Anti-Cryptor**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Anti-Cryptor**.
  6. Configurare il componente Anti-Cryptor.
  7. Salvare le modifiche.
- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**
  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere a **Protezione minacce avanzata → Rilevamento del comportamento**.

5. Utilizzare l'interruttore **Proteggi le cartelle condivise dal criptaggio esterno** per abilitare o disabilitare il componente.
6. Configurare il componente Anti-Cryptor.
7. Salvare le modifiche.

Impostazioni di Anti-Cryptor

Parametro	Descrizione
Azione se viene rilevata una minaccia	**Informa**. Se questa opzione è selezionata, quando viene rilevato un tentativo di modifica dei file nelle cartelle condivise, Kaspersky Endpoint Security aggiunge informazioni sul tentativo all'elenco delle minacce attive, aggiunge una voce al rapporto. **Blocca la connessione per (min)**. Quando rileva un tentativo di modifica dei file nelle cartelle condivise, Kaspersky Endpoint Security blocca il traffico di rete proveniente da un dispositivo che svolge attività dannosa. L'applicazione crea un evento *Criptaggio rilevato* che contiene informazioni sul dispositivo compromesso.

Configurazione del componente Prevenzione exploit

È possibile configurare il componente Prevenzione Exploit in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**
  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare alla sezione **Protezione minacce host → Analisi del comportamento → Prevenzione Exploit**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Prevenzione Exploit**.
  6. Configurare il componente Prevenzione Exploit.
  7. Salvare le modifiche.
- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**
  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere a **Protezione minacce avanzata → Prevenzione Exploit**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Prevenzione Exploit**.
  6. Configurare il componente Prevenzione Exploit.
  7. Salvare le modifiche.

Impostazioni	Descrizione
Azione se viene rilevata una minaccia	**Informa**. Se questa opzione è selezionata, quando Kaspersky Endpoint Security rileva un exploit registra una voce contenente informazioni sull'exploit e aggiunge le informazioni sull'exploit all'elenco delle minacce attive. **Blocca**. Se questo elemento è selezionato durante il rilevamento di un exploit, Kaspersky Endpoint Security blocca le operazioni di questo exploit e crea una voce di registro con le informazioni sull'exploit.

Configurazione del componente Motore di Remediation

È possibile configurare il componente Motore di Remediation in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare alla sezione **Protezione minacce host → Analisi del comportamento → Motore di Remediation**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Motore di Remediation**.
  6. Configurare il componente Motore di Remediation.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere a **Protezione minacce avanzata → Motore di Remediation**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Motore di Remediation**.
  6. Configurare il componente Motore di Remediation.
  7. Salvare le modifiche.

Protezione Web e comunicazione

Configurare Protezione minacce di posta

È possibile configurare il componente Protezione minacce di posta in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Comunicazione e protezione Web → Protezione minacce di posta**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione minacce di posta**.
  6. Configurare il componente Protezione minacce di posta.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Protezione minacce essenziale → Protezione minacce Web**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione minacce di posta**.
  6. Configurare il componente Protezione minacce di posta.
  7. Salvare le modifiche.

Impostazioni di Protezione minacce di posta

Impostazioni	Descrizione
Azione se viene rilevata una minaccia	**Disinfetta (se non è possibile, elimina)** Quando un oggetto infetto viene rilevato in un messaggio in entrata o in uscita, l'applicazione tenta di disinfettare l'oggetto rilevato. L'utente sarà in grado di accedere al messaggio con un allegato sicuro. Se l'oggetto non può essere disinfettato, l'applicazione elimina l'oggetto infetto. L'applicazione aggiunge informazioni sull'azione eseguita all'oggetto del messaggio, ad esempio *[Il messaggio è stato elaborato] <oggetto del messaggio>*. **Blocca**. Se un oggetto infetto viene rilevato in un messaggio in entrata, l'applicazione aggiunge un avviso all'oggetto del messaggio. L'utente sarà in grado di accedere al messaggio con l'allegato originale. Se un oggetto infetto viene rilevato in un messaggio in uscita, l'applicazione blocca la trasmissione del messaggio e il client di posta mostra un errore.
Non esaminare archivi superiori a (MB)	Se la casella di controllo è selezionata, il componente Protezione minacce di posta esclude dalla scansione gli archivi allegati ai messaggi e-mail se la loro dimensione supera il valore specificato. Se la casella di controllo è deselezionata, il componente Protezione minacce di posta esamina gli archivi allegati ai messaggi e-mail di qualsiasi dimensione.
Ignora file scansionato per più di (sec)	Se la casella di controllo è selezionata, il tempo allocato per la scansione degli archivi allegati ai messaggi e-mail è limitato al periodo specificato.

Configurazione del componente Protezione minacce Web

È possibile configurare il componente Protezione Minacce di Rete in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare alla sezione **Comunicazione e protezione Web** → **Protezione minacce Web**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione minacce Web**.
  6. Configurare il componente Protezione minacce Web
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Protezione minacce essenziale** → **Protezione minacce Web**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione minacce Web**.
  6. Configurare il componente Protezione minacce Web
  7. Salvare le modifiche.

Impostazioni di Protezione minacce Web

Impostazioni	Descrizione
Indirizzi Web attendibili	Elenco di indirizzi Web considerati attendibili da Protezione minacce Web. Il componente non esegue la scansione del traffico in entrata e in uscita da questi indirizzi alla ricerca di minacce. L'elenco di indirizzi attendibili può essere utilizzato, ad esempio, nei casi in cui il componente Protezione minacce Web interferisca con il download di un file da un sito Web conosciuto.
Esclusioni dalla scansione	Un'*esclusione dalla scansione* è un set di condizioni che devono essere soddisfatte perché Kaspersky Endpoint Security non esegua la scansione di un determinato oggetto alla ricerca di virus e altre minacce. Le esclusioni dalla scansione consentono di utilizzare senza rischi il software legittimo che utenti malintenzionati possono sfruttare per danneggiare il computer o i dati dell'utente. Benché non presentino funzioni pericolose, le applicazioni di questo tipo possono essere sfruttate dagli utenti malintenzionati. Per ulteriori dettagli sulle applicazioni legittime utilizzabile da utenti malintenzionati per compromettere il computer o i dati personali, consultare il sito Web dell'Enciclopedia IT di Kaspersky.
Azione se viene rilevata una minaccia	**Blocca**. Se questa opzione è selezionata e viene rilevato un oggetto infetto nel traffico Web, il componente Protezione minacce Web blocca l'accesso all'oggetto e visualizza un messaggio nel browser. **Richiedi azione**. Kaspersky Endpoint Security visualizza una notifica con informazioni sul tipo di malware che ha infettato l'oggetto del traffico Web e richiede all'utente di scegliere l'azione che deve essere eseguita da Kaspersky Endpoint Security su tale oggetto. Le azioni disponibili possono variare in base allo stato dell'oggetto.

Configurare Protezione Minacce di Rete

È possibile configurare il componente Protezione Minacce di Rete in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Comunicazione e protezione Web** > **Protezione minacce di rete**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione Minacce di Rete**.
  6. Configurare il componente Protezione Minacce di Rete.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Protezione minacce essenziale → Protezione minacce di rete**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione Minacce di Rete**.
  6. Configurare il componente Protezione Minacce di Rete.
  7. Salvare le modifiche.

Impostazioni di Protezione minacce di Rete

Impostazioni	Descrizione
Indirizzi IP attendibili	Elenco di indirizzi IP dei dispositivi attendibili. Il componente Protezione minacce di rete non blocca le attività di rete da questi indirizzi.
Azione se viene rilevata una minaccia	**Blocca**. Quando viene rilevata una minaccia, Protezione minacce di rete blocca l'attacco. **Blocca attacco e dispositivo che ha sferrato l'attacco per (min)**. Se l'opzione è abilitata, il componente Protezione minacce di rete aggiunge il computer che ha originato l'attacco all'elenco di computer bloccati. In altre parole, il componente Protezione minacce di rete blocca la connessione di rete con il computer che ha originato l'attacco dopo il primo tentativo di un attacco di rete per il periodo di tempo specificato. Questo blocco protegge automaticamente il computer dell'utente da ulteriori possibili attacchi di rete dallo stesso indirizzo. Il tempo minimo che un computer che ha originato l'attacco deve trascorrere nell'elenco dei blocchi è di un minuto. Il tempo massimo è 999 minuti.

Configura il componente Firewall

È possibile configurare il componente Firewall in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Comunicazione e protezione Web → Firewall**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Firewall**.
  6. Configurare il componente Firewall.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare alla sezione **Protezione minacce essenziale** > **Firewall**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Firewall**.
  6. Configurare il componente Firewall.
  7. Salvare le modifiche.

Impostazioni firewall

Impostazioni	Descrizione
Regole per i pacchetti di rete	Tabella con un elenco delle regole per i pacchetti di rete. Le regole per i pacchetti di rete vengono utilizzate per applicare restrizioni ai pacchetti di rete, indipendentemente dall'applicazione. Le regole di questo tipo limitano il traffico di rete in entrata e in uscita tramite specifiche porte del protocollo dati selezionato. Nella tabella sono elencate le regole per i pacchetti di rete preconfigurate, consigliate da Kaspersky per una protezione ottimale del traffico di rete dei computer con sistema operativo macOS. Firewall imposta la priorità di esecuzione per ogni regola per i pacchetti di rete. Firewall elabora le regole per i pacchetti di rete nell'ordine in cui compaiono nell'elenco delle regole per i pacchetti di rete, dalla prima all'ultima. Firewall individua la regola per i pacchetti di rete più adatta alla connessione di rete e la applica, consentendo o bloccando l'attività di rete. Firewall ignora quindi tutte le successive regole per i pacchetti di rete per la connessione di rete specifica. Le regole per i pacchetti di rete hanno una priorità superiore rispetto alle regole di rete per le applicazioni.

Impostazioni	Descrizione
Reti disponibili	Questa tabella contiene informazioni sulle connessioni di rete rilevate da Firewall sul computer. Sono disponibili i seguenti tipi di connessione di rete: • La rete non è protetta da applicazioni anti-malware, firewall o filtri (ad esempio Wi-Fi in un bar). Quando l'utente utilizza un computer connesso a tale rete, Firewall blocca l'accesso ai file e alle stampanti del computer. Gli utenti esterni non sono inoltre in grado di accedere ai dati tramite le cartelle condivise e l'accesso remoto al desktop del computer. Firewall filtra l'attività di rete di ogni applicazione in base alle regole di rete impostate per l'applicazione. • Rete per gli utenti con accesso limitato a file e stampanti nel computer (ad esempio una LAN aziendale o una rete domestica). • Rete sicura in cui il computer non è esposto ad attacchi o tentativi di accesso non autorizzati ai dati. Firewall consente qualsiasi attività di rete all'interno di reti con questo stato.

Controlli di sicurezza

Configurazione del componente Controllo dispositivi

È possibile configurare il componente Controllo dispositivi in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere a **Controlli di sicurezza** → **Controllo dispositivi**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Controllo dispositivi**.
  6. Configurare Controllo dispositivi.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere a **Controlli di sicurezza** → **Controllo dispositivi**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Controllo dispositivi**.
  6. Configurare Controllo dispositivi.
  7. Salvare le modifiche.

Impostazioni di Controllo dispositivi

Impostazioni	Descrizione
Dispositivi attendibili	Elenco di dispositivi attendibili e di utenti ai quali è stato concesso l'accesso a questi dispositivi.
Dispositivi e reti Wi-Fi	Un elenco di tutti i tipi di dispositivi disponibili in base alla classificazione del componente Controllo dispositivi, con i relativi stati di accesso.

Configurazione del componente Controllo Web

È possibile configurare il componente Controllo Web in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere a **Controlli di sicurezza** → **Controllo Web**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Controllo Web**
  6. Configurare il componente Controllo Web.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere a **Controlli di sicurezza** → **Controllo Web**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Controllo Web**
  6. Configurare il componente Controllo Web.
  7. Salvare le modifiche.

Impostazioni	Descrizione
Elenco di regole	Elenco contenente le regole di accesso alle risorse Web. Ogni regola ha una priorità. Più in alto si trova una regola nell'elenco, maggiore è la sua priorità. Se un sito Web è stato aggiunto a più regole, Controllo Web regola l'accesso al sito Web in base alla regola con la massima priorità.
Azione predefinita	La regola di accesso per le risorse Web a cui non si applica nessun'altra regola. Sono disponibili le seguenti opzioni: • **Consenti tutto tranne l'elenco di regole**. • **Blocca tutto tranne l'elenco di regole**.

Criptaggio dei dati

È possibile configurare il componente Criptaggio dei dati in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare alla sezione **Criptaggio dei dati**
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Criptaggio dei dati**.
  6. Configurare il componente Criptaggio dei dati.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare alla sezione **Criptaggio dei dati**
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Criptaggio del disco FileVault**.
  6. Configurare il componente Criptaggio dei dati.
  7. Salvare le modifiche.

Impostazioni	Descrizione
Azione sui dispositivi	**Cripta tutti i dischi rigidi**. Se questa opzione è selezionata, l'applicazione cripta tutti i dischi rigidi quando viene applicato il criterio. **Decripta tutti i dischi rigidi**. Se questa opzione è selezionata, l'applicazione decripta tutti i dischi rigidi criptati precedentemente quando viene applicato il criterio.

Impostazioni generali

Impostazioni di rilevamento

È possibile configurare le impostazioni di rilevamento in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Vai a **Impostazioni generali** → **Impostazioni di rilevamento**.
  5. Configurare le Impostazioni di rilevamento
  6. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Impostazioni aggiuntive** → **Protezione**.
  5. Configurare le Impostazioni di rilevamento
  6. Salvare le modifiche.

Impostazioni di rilevamento

Impostazioni	Descrizione
Rilevamento di altri tipi di oggetti	Indipendentemente dalle impostazioni configurate dell'applicazione, Kaspersky Endpoint Security rileva e blocca sempre virus, worm, Trojan e strumenti pericolosi. Dal momento che possono danneggiare in modo significativo il computer. È inoltre possibile abilitare il rilevamento dei seguenti tipi di oggetti: • **Software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali**. Benché non presentino funzioni pericolose, le applicazioni di questo tipo possono essere sfruttate dagli utenti malintenzionati. Per ulteriori dettagli sulle applicazioni legittime utilizzabile da utenti malintenzionati per compromettere il computer o i dati personali, consultare il sito Web dell'Enciclopedia IT di Kaspersky.

Kaspersky Security Network

È possibile configurare le impostazioni di Kaspersky Security Network in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Impostazioni generali** → **Kaspersky Security Network**.
  5. Utilizzare l'interruttore **Kaspersky Security Network (KSN)** per abilitare o disabilitare il componente.
  6. Configurare il componente Kaspersky Security Network.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Protezione minacce avanzata** → **Kaspersky Security Network**.
  5. Utilizzare l'interruttore **Kaspersky Security Network** per abilitare o disabilitare il componente.
  6. Configurare il componente Kaspersky Security Network.
  7. Salvare le modifiche.

Impostazioni di rilevamento

Impostazioni	Descrizione
Usa modalità KSN estesa	*Modalità KSN estesa* è una modalità in cui Kaspersky Endpoint Security invia dati aggiuntivi a Kaspersky. Kaspersky Endpoint Security utilizza KSN per rilevare le minacce indipendentemente dalla posizione di attivazione/disattivazione.
Usa modalità cloud	La *Modalità cloud* fa riferimento alla modalità operativa dell'applicazione in cui Kaspersky Endpoint Security utilizza una versione leggera dei database anti-virus. Kaspersky Security Network supporta il funzionamento dell'applicazione con l'utilizzato dei database anti-virus leggeri. La versione leggera dei database anti-virus consente di utilizzare circa la metà della RAM del computer che altrimenti verrebbe utilizzata con i database standard. Se non si partecipa a Kaspersky Security Network o se la modalità cloud è disabilitata, Kaspersky Endpoint Security scarica la versione completa dei database anti-virus dai server di Kaspersky. Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza la versione leggera dei database anti-virus, riducendo così il carico sulle risorse del sistema operativo. Kaspersky Endpoint Security scarica la versione leggera dei database anti-virus durante il successivo aggiornamento dopo la selezione della casella di controllo. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security utilizza la versione completa dei database anti-virus. Kaspersky Endpoint Security scarica la versione completa dei database anti-virus durante il successivo aggiornamento dopo la deselezione della casella di controllo.
Usa Administration Server come server proxy KSN	Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza il servizio proxy KSN. È possibile configurare le impostazioni del servizio proxy KSN nelle proprietà di Administration Server.
Usa i server di Kaspersky Security Network se il server proxy KSN non è disponibile	Se la casella di controllo è selezionata, Kaspersky Endpoint Security usa i server KSN quando il servizio KSN Proxy non è disponibile. I server KSN possono essere gestiti sia da Kaspersky che da terzi (quando si utilizza Kaspersky Private Security Network).

Interazione utente

È possibile configurare le impostazioni dell'interfaccia dell'applicazione, nonché le impostazioni per l'interazione dell'applicazione con l'utente in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Vai a **Impostazioni generali → Interazione utente**.
  5. Configurare le impostazioni di interazione con l'utente.
  6. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Impostazioni aggiuntive → Interazione utente**.
  5. Configurare le impostazioni di interazione con l'utente.
  6. Salvare le modifiche.

Impostazioni di interazione con l'utente

Impostazioni	Descrizione
Avvia Kaspersky Endpoint Security all'avvio del computer (consigliato)	Se questa opzione è selezionata, Kaspersky Endpoint Security viene avviato dopo il caricamento del sistema operativo, proteggendo il computer durante l'intera sessione. Se questa funzionalità è disabilitata, Kaspersky Endpoint Security non viene avviato dopo l'avvio del sistema operativo, finché non viene avviato dall'utente. La protezione del computer è disabilitata e i dati dell'utente potrebbero essere esposti a minacce.
Mostra l'icona dell'applicazione	Questa casella di controllo consente di abilitare o disabilitare la visualizzazione dell'icona dell'applicazione nella barra dei menu di un computer remoto. Se questa casella di controllo è selezionata, l'icona dell'applicazione viene visualizzata nella barra dei menu. Se questa casella di controllo è deselezionata, l'icona dell'applicazione viene nascosta dalla barra dei menu. Questa casella di controllo è selezionata per impostazione predefinita.
Gestisci aggiornamenti in locale	Se questa casella di controllo è selezionata, la gestione locale degli aggiornamenti di Kaspersky Endpoint Security in un computer remoto è abilitata. Se questa casella di controllo è deselezionata, gli aggiornamenti di Kaspersky Endpoint Security in un computer remoto possono essere gestiti solo tramite il plug-in di amministrazione di Kaspersky Endpoint Security in Kaspersky Security Center.
Gestisci chiavi in locale	Se la casella di controllo è selezionata, la gestione locale delle chiavi di Kaspersky Endpoint Security in un computer remoto è abilitata. Se la casella di controllo è deselezionata, le chiavi di Kaspersky Endpoint Security in un computer remoto possono essere gestite solo tramite il plug-in di amministrazione di Kaspersky Endpoint Security in Kaspersky Security Center.
Chiudi l'applicazione	Se questa casella di controllo è selezionata, il comando **Esci** è presente nel menu di scelta rapida dell'icona dell'applicazione. L'utente di un computer remoto può chiudere Kaspersky Endpoint Security nel computer remoto. Se questa casella di controllo è deselezionata, il comando **Esci** non è presente nel menu di scelta rapida dell'icona dell'applicazione. L'utente di un computer remoto non può chiudere Kaspersky Endpoint Security nel computer remoto.

Auto-difesa

È possibile configurare le impostazioni di Auto-difesa in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.

3. Selezionare la scheda **Impostazioni applicazione**.
4. Vai a **Impostazioni generali → Auto-difesa**.
5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione tramite password**.
6. Configurare Auto-difesa.
7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni aggiuntive → Interazione utente**.
5. Abilitare o disabilitare il componente utilizzando l'interruttore **Protezione tramite password**.
6. Configurare Protezione tramite password.
7. Salvare le modifiche.

Impostazioni di Auto-difesa

Impostazioni	Descrizione
Protezione tramite password	Se l'interruttore è abilitato, Kaspersky Endpoint Security richiede all'utente una password quando tenta di eseguire un'operazione nell'ambito di Protezione tramite password. L'ambito di Protezione tramite password include le operazioni vietate (ad esempio la disabilitazione dei componenti della protezione) e gli account utente a cui si applica l'ambito di Protezione tramite password. Dopo l'abilitazione di Protezione tramite password, Kaspersky Endpoint Security richiede all'utente di impostare una password per l'account KLAdmin.

Prestazioni

È possibile configurare le impostazioni delle prestazioni in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali → Prestazioni**.

5. Configurare le impostazioni delle prestazioni.
6. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Impostazioni aggiuntive** → **Protezione**.
  5. Configurare le impostazioni delle prestazioni.
  6. Salvare le modifiche.

Impostazioni delle prestazioni

Impostazioni	Descrizione
Rimanda o ignora attività pianificate durante l'alimentazione a batteria	Se questa funzionalità è abilitata, Kaspersky Endpoint Security passa alla modalità di risparmio energetico. Kaspersky Endpoint Security *annulla* le attività pianificate. È possibile avviare manualmente le attività di scansione e aggiornamento, se necessario.
Limita l'utilizzo della CPU per le attività di scansione	Per ottimizzare le prestazioni di Kaspersky Endpoint Security, è possibile limitare l'utilizzo della CPU tramite l'attività di scansione malware. Se questa funzionalità è abilitata, il carico medio su tutti i core della CPU dall'attività di scansione malware si avvicina al valore specificato.

Rapporti e archivi

È possibile configurare le impostazioni di Rapporti e archivi in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Impostazioni generali** → **Rapporti e archivi**.
  5. Configurare le impostazioni relative a Rapporti e archivi.
  6. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Vai a **Impostazioni aggiuntive → Rapporti e backup**.
  5. Configurare le impostazioni relative a Rapporti e archivi.
  6. Salvare le modifiche.

Impostazioni di Rapporti e archivi.

Impostazioni	Descrizione
Elimina i rapporti dopo (giorni)	Se la casella di controllo è selezionata, il periodo di archiviazione massimo dei rapporti si limita all'intervallo di tempo definito. Al termine di tale periodo di tempo, Kaspersky Endpoint Security elimina automaticamente le voci meno recenti dal file del rapporto.
Mantieni solo eventi recenti	Se questa casella di controllo è selezionata, ogni volta che l'attività viene avviata, Kaspersky Endpoint Security elimina le informazioni sugli eventi non critici che si sono verificati dall'avvio precedente dell'attività, ma mantiene note importanti nel rapporto (ad esempio, informazioni sugli oggetti dannosi rilevati).
Registra eventi non critici	Se questa casella di controllo è selezionata, Kaspersky Endpoint Security registra gli eventi non critici (ad esempio, eventi informativi) nei rapporti. Gli eventi non critici non influiscono sulla protezione.
Elimina oggetti dopo (giorni)	Se la casella di controllo è selezionata, il periodo di archiviazione massimo del file si limita all'intervallo di tempo definito. Al termine del periodo massimo di archiviazione, Kaspersky Endpoint Security elimina i file meno recenti da Backup.

Impostazioni di Rete

È possibile configurare le impostazioni di rete in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Vai a **Impostazioni generali → Impostazioni di rete**.
  5. Configurare le impostazioni di rete.
  6. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.

3. Selezionare la scheda **Impostazioni applicazione**.
4. Vai a **Impostazioni aggiuntive → Rete**.
5. Configurare le impostazioni di rete.
6. Salvare le modifiche.

Impostazioni di Rete

Impostazioni	Descrizione
Certificati radice attendibili	Elenco dei certificati radice attendibili. Kaspersky Endpoint Security consente di installare i certificati radice attendibili nei computer degli utenti se, ad esempio, è necessario distribuire un nuovo centro di certificazione. L'applicazione consente di aggiungere un certificato a uno speciale archivio certificati di Kaspersky Endpoint Security. In questo caso, il certificato viene considerato attendibile solo per l'applicazione Kaspersky Endpoint Security. In altre parole, l'utente può accedere a un sito Web con il nuovo certificato nel browser. Se un'altra applicazione tenta di accedere al sito Web, è possibile che si verifichi un errore di connessione a causa di un problema di certificato.
Server proxy	Impostazioni del server proxy utilizzato per l'accesso a Internet degli utenti dei computer client. Kaspersky Endpoint Security utilizza queste impostazioni per determinati componenti della protezione, oltre che per l'aggiornamento dei database e dei moduli dell'applicazione.
Usa l'autenticazione per il server proxy	Se questa casella di controllo è selezionata, l'applicazione utilizza l'autenticazione con un nome utente e una password durante la connessione al server proxy.
Ignora un server proxy per gli indirizzi locali	Se la casella di controllo è selezionata, Kaspersky Endpoint Security non utilizza un server proxy durante un aggiornamento da una cartella condivisa.
Scansione delle connessioni criptate	Questa funzionalità consente ai componenti Protezione minacce Web, Protezione minacce di posta e Controllo Web di monitorare e gestire le connessioni criptate (HTTPS).

Impostazioni di telemetria

È possibile configurare le impostazioni di telemetria in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**
  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Impostazioni generali → Impostazioni di telemetria**.
  5. Configurare le impostazioni di telemetria.
  6. Salvare le modifiche.
- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**
  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse → Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.

4. Passare a **Impostazioni aggiuntive** → **Area attendibile** → **Impostazioni di telemetria**.

5. Configurare le impostazioni di telemetria.

6. Salvare le modifiche.

Impostazioni di telemetria

Impostazioni	Descrizione
Telemetria EDR Expert (on-premise)	**Importa** ed **Esporta**. È possibile esportare le impostazioni di telemetria EDR Expert (on-premise) in un file JSON. Quindi è possibile modificare il file, ad esempio per aggiungere un numero elevato di ID di eventi. È inoltre possibile utilizzare la funzione di esportazione/importazione per eseguire il backup delle impostazioni degli eventi inviati o per eseguire la migrazione dell'elenco in un altro criterio.
Esclusioni generali	Per ottimizzare i dati trasmessi, è possibile configurare regole di esclusione per determinati tipi di evento. Kaspersky Endpoint Security non raccoglie la telemetria che rientra in tale regola. Ciò consente di ridurre il traffico ed evitare di elaborare gli eventi provenienti da oggetti e processi attendibili.

Impostazioni degli eventi

Durante il funzionamento dell'applicazione, possono verificarsi vari *eventi*. Questi eventi possono essere puramente informative o contenere informazioni critiche. L'applicazione può ad esempio utilizzare un evento per inviare una notifica in merito all'aggiornamento del database riuscito o segnalare l'errore di un componente che deve essere corretto.

Gli eventi di Kaspersky Endpoint Security possono rientrare nelle seguenti classi di gravità:

- *Eventi critici* - eventi che rappresentano una minaccia per la protezione del computer (rilevamento di oggetti dannosi, vulnerabilità, problemi relativi a Kaspersky Endpoint Security). Gli eventi critici richiedono attenzione immediata da parte dell'utente. È consigliabile non disabilitare le notifiche sugli eventi critici.

- *Errori funzionali* sono eventi che si verificano in caso di malfunzionamento di Kaspersky Endpoint Security (errore di elaborazione, errore nelle impostazioni delle attività). Tali eventi non minacciano direttamente la sicurezza del computer, ma richiedono l'intervento dell'utente per assicurarsi che Kaspersky Endpoint Security funzioni correttamente e protegga i dispositivi.

- *Avvisi* - eventi che non richiedono attenzione immediata da parte dell'utente, ma possono rappresentare una minaccia futura per la protezione del computer.

- *Messaggi informativi* - gli eventi segnalati a scopo informativo.

Indipendentemente dal fatto che le notifiche siano abilitate o disabilitate, Kaspersky Endpoint Security registra le informazioni su tutti gli eventi dell'applicazione nei rapporti dell'applicazione.

Impostazioni di aggiornamento

È possibile configurare le impostazioni di aggiornamento in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

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

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

     Viene visualizzata la finestra delle proprietà dei criteri.

3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare a **Impostazioni generali** → **Aggiornamento**.
5. Configurare le impostazioni di aggiornamento.
6. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Passare alla sezione **Aggiornamento**.
5. Configurare le impostazioni di aggiornamento.
6. Salvare le modifiche.

Impostazioni di aggiornamento

Impostazioni	Descrizione
Sorgenti degli aggiornamenti	Una *sorgente degli aggiornamenti* è una risorsa che contiene gli aggiornamenti per i database e i moduli dell'applicazione di Kaspersky Endpoint Security. Le sorgenti degli aggiornamenti includono il server Kaspersky Security Center, i server degli aggiornamenti Kaspersky e cartelle di rete o locali. Se i server degli aggiornamenti di Kaspersky non sono disponibili, Kaspersky Endpoint Security può utilizzare domini alternativi per ricevere gli aggiornamenti dei database e dei moduli dell'applicazione. Per i dettagli, consultare la Knowledge Base dell'Assistenza tecnica. L'elenco predefinito di sorgenti degli aggiornamenti include Kaspersky Security Center e i server degli aggiornamenti Kaspersky. È possibile aggiungere all'elenco altre sorgenti degli aggiornamenti. È possibile specificare server HTTP/FTP e cartelle condivise come sorgenti degli aggiornamenti. Kaspersky Endpoint Security non supporta gli aggiornamenti dai server HTTPS, a meno che non si tratti dei server degli aggiornamenti Kaspersky. Se sono state selezionate più risorse come sorgenti degli aggiornamenti, Kaspersky Endpoint Security tenta di connettersi a esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco e recupera gli aggiornamenti dalla prima disponibile. Per impostazione predefinita, Kaspersky Endpoint Security utilizza il server Kaspersky Security Center come prima sorgente di aggiornamenti. Questo aiuta a conservare il traffico durante l'aggiornamento. Se un criterio non viene applicato al computer, i server Kaspersky vengono selezionati come prima sorgente degli aggiornamenti nelle impostazioni dell'attività locale di aggiornamento perché l'applicazione potrebbe non avere accesso al server Kaspersky Security Center.

Agenti integrati

Configurare Managed Detection and Response

È possibile configurare il componente Managed Detection and Response in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere alla sezione **Configurazione agenti integrati** → **Managed Detection and Response**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Managed Detection and Response**.
  6. Configurare il componente Managed Detection and Response
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Passare a **Detection and Response** > **Managed Detection and Response**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Managed Detection and Response**.
  6. Configurare il componente Managed Detection and Response
  7. Salvare le modifiche.

Impostazioni del componente Managed Detection and Response

Impostazioni	Descrizione
File di configurazione MDR	Il file BLOB contiene l'ID client e le informazioni sulla licenza per Kaspersky Managed Detection and Response. Il file BLOB si trova nell'archivio ZIP del file di configurazione MDR. È possibile ottenere l'archivio ZIP in Kaspersky Managed Detection and Response Console. Per informazioni dettagliate su un file BLOB, consultare la Guida di Kaspersky Managed Detection and Response.

Configurare Endpoint Detection and Response

È possibile configurare il componente Endpoint Detection and Response in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere alla sezione **Configurazione agenti integrati** → **Endpoint Detection and Response**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Managed Detection and Response**.
  6. Configurare il componente Endpoint Detection and Response.
  7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.
     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Selezionare **Detection and Response** > **Endpoint Detection and Response**.
  5. Abilitare o disabilitare il componente utilizzando l'interruttore **Endpoint Detection and Response**.
  6. Configurare il componente Endpoint Detection and Response.
  7. Salvare le modifiche.

Impostazioni di Endpoint Detection and Response

Impostazioni	Descrizione
Isolamento di rete	Isolamento automatico del computer dalla rete in risposta alle minacce rilevate. Quando l'isolamento di rete è attivato, l'applicazione interrompe tutte le connessioni attive e blocca tutte le nuove connessioni TCP/IP nel computer. L'applicazione lascia attive solo le seguenti connessioni: • Connessioni elencate in Esclusioni dall'isolamento di rete. • Connessioni avviate dai servizi di Kaspersky Endpoint Security. • Connessioni avviate da Kaspersky Security Center Network Agent.
Sblocca automaticamente un dispositivo isolato tra (ore)	L'isolamento di rete può essere disattivato automaticamente dopo un periodo di tempo specificato o manualmente.

Impostazioni	Descrizione
Esclusioni dall'isolamento di rete	Elenco di regole per le esclusioni dall'isolamento di rete. Le connessioni di rete che corrispondono alle regole non vengono bloccate nei computer quando Isolamento di rete è attivato. Per configurare le esclusioni dall'isolamento di rete, è possibile utilizzare un elenco di *profili di rete standard*. Per impostazione predefinita, le esclusioni includono i profili di rete che contengono regole che garantiscono il funzionamento costante dei dispositivi con il server DNS/DHCP e i ruoli client DNS/DHCP. È inoltre possibile modificare le impostazioni dei profili di rete standard o definire manualmente le esclusioni. Le esclusioni specificate nelle proprietà dei criteri vengono applicate solo se Isolamento di rete viene attivato automaticamente in risposta a una minaccia rilevata. Le esclusioni specificate nelle proprietà del computer vengono applicate solo se Isolamento di rete è attivato manualmente nelle proprietà del computer in Kaspersky Security Center Console o nei dettagli degli avvisi.
Prevenzione dell'esecuzione	Controlla l'esecuzione dei file eseguibili e degli script, nonché l'apertura di file in formato Office. Ad esempio, è possibile impedire l'esecuzione di applicazioni considerate non sicure sul computer selezionato. Prevenzione dell'esecuzione supporta una serie di estensioni di file Office e una serie di interpreti di script. Per utilizzare il componente Prevenzione dell'esecuzione, è necessario aggiungere regole di prevenzione dell'esecuzione.
Azione in caso di esecuzione o apertura di un oggetto vietato	**Blocca e aggiungi al registro eventi**. In questa modalità, l'applicazione blocca l'esecuzione di oggetti o l'apertura di documenti che soddisfano i criteri della regola di prevenzione. L'applicazione pubblica anche un evento sui tentativi di esecuzione di oggetti o apertura di documenti nel registro eventi del sistema e Kaspersky Security Center. **Aggiungi al registro eventi**. In questa modalità, Kaspersky Endpoint Security pubblica un evento sui tentativi di esecuzione di oggetti eseguibili o apertura di documenti che corrispondono ai criteri della regola di prevenzione nel registro eventi del sistema e in Kaspersky Security Center, ma non blocca il tentativo di esecuzione o apertura dell'oggetto o del documento. Questa modalità è selezionata per impostazione predefinita.
Regole di prevenzione dell'esecuzione	*Regola di prevenzione dell'esecuzione* è un insieme di criteri che l'applicazione prende in considerazione quando reagisce all'esecuzione di un oggetto, ad esempio quando blocca l'esecuzione di un oggetto. L'applicazione identifica i file in base ai loro percorsi o checksum calcolati utilizzando gli algoritmi di hash MD5 e SHA256.
Sandbox cloud	*Cloud Sandbox* è una tecnologia che consente di rilevare le minacce avanzate in un computer. Kaspersky Endpoint Security inoltra automaticamente i file rilevati a sandbox cloud per l'analisi. Sandbox cloud esegue questi file in un ambiente isolato per identificare le attività dannose e decidere in merito alla reputazione. I dati su questi file vengono quindi inviati a Kaspersky Security Network. Pertanto, se Cloud Sandbox ha rilevato un file dannoso, Kaspersky Endpoint Security eseguirà l'azione appropriata per eliminare questa minaccia in tutti i computer in cui viene rilevato questo file. Una connessione KSN è necessaria per ottenere informazioni sugli oggetti da analizzare.

Configurare Endpoint Detection and Response Expert (on-premise)

È possibile configurare il componente Endpoint Detection and Response Expert (on-premise) in uno dei seguenti modi:

- **Ufilizzando Unified Protection and Management Plug-in**

  1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
  2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

     Viene visualizzata la finestra delle proprietà dei criteri.
  3. Selezionare la scheda **Impostazioni applicazione**.
  4. Accedere alla sezione **Configurazione agenti integrati** → **Endpoint Detection and Response Expert (on-premise)**.

5. Abilitare o disabilitare il componente utilizzando l'interruttore **Expert Managed Detection and Response (on-premise)**.
6. Configurare il componente Endpoint Detection and Response (on-premise)
7. Salvare le modifiche.

- **Utilizzo del plug-in Web di Kaspersky Endpoint Security**

1. Nella finestra principale di Web Console, selezionare **Gestione delle risorse** → **Criteri**.
2. Fare clic sul nome del criterio di Kaspersky Endpoint Security.

   Viene visualizzata la finestra delle proprietà dei criteri.
3. Selezionare la scheda **Impostazioni applicazione**.
4. Selezionare Detection and Response > **Endpoint Detection and Response Expert (on-premise)**.
5. Abilitare o disabilitare il componente utilizzando l'interruttore **Expert Managed Detection and Response (on-premise)**.
6. Configurare il componente Endpoint Detection and Response (on-premise)
7. Salvare le modifiche.

Impostazioni del componente Endpoint Detection and Response Expert (on-premise)

Impostazioni	Descrizione
Soluzione Endpoint Detection and Response Expert	Soluzioni Endpoint Detection and Response Expert con cui Kaspersky Endpoint Security può integrarsi. • **Endpoint Detection and Response Expert (versione 7.1 o precedente)** • **Endpoint Detection and Response Expert (versione 8.0 o successiva)**
Impostazioni di connessione	Gestire le seguenti impostazioni di connessione al server di raccolta di telemetria o KATA: • **Timeout connessione server**. Timeout massimo di risposta del server di Central Node. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server Central Node. • **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server di Central Node. È possibile ottenere un certificato TLS nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nella guida di Kaspersky Anti Targeted Attack Platform). • **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server Central Node. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server Central Node, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un contenitore crittografico è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni di Central Node, è necessario abilitare anche l'autenticazione bidirezionale nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password. Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore criptato con una password vuota.
Invia richiesta di sincronizzazione al server ogni (min) *(Disponibile solo per Endpoint Detection and Response Expert 7.1 o versione successiva).*	Frequenza delle richieste di sincronizzazione inviate al server. Durante la sincronizzazione, Kaspersky Endpoint Security invia informazioni sulle attività e le impostazioni dell'applicazione modificate.

Impostazioni	Descrizione
Connessione ai server KATA / Connessione ai server di raccolta della telemetria	Immettere l'indirizzo IP e la porta di connessione al server Kaspersky Anti Targeted Attack Platform o al server di raccolta della telemetria. È possibile aggiungere diversi indirizzi del Central Node (per KATA) o del server di raccolta della telemetria. Kaspersky Endpoint Security tenta di connettersi al server al primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi al secondo indirizzo IP nell'elenco e così via. Le soluzioni EDR (KATA) ed EDR Expert (on-premises) hanno architetture diverse. Per l'elaborazione della telemetria, EDR Expert (on-premises) utilizza un server di raccolta della telemetria, EDR (KATA) utilizza un server Central Node. Se quindi si integra l'applicazione con EDR Expert (on-premises), è necessario aggiungere un server di raccolta della telemetria.
Invia telemetria a KATA / Invia telemetria ai server di raccolta della telemetria	Questa funzione consente di impedire completamente l'invio della telemetria al server KATA o al server di raccolta della telemetria, a seconda della soluzione selezionata. Ad esempio, se si utilizza Kaspersky Anti Targeted Attack Platform insieme a un'altra soluzione che usa anch'essa la telemetria, è possibile disattivare l'invio della telemetria per KATA (EDR). Ciò consente di ottimizzare il carico del server per queste soluzioni. Se è stata distribuita la soluzione Managed Detection and Response e KATA (EDR), è possibile utilizzare la telemetria MDR e creare attività Risposta alle minacce in KATA (EDR).
Ritardo di trasmissione eventi massimo (sec)	L'applicazione si sincronizza con il server per inviare eventi dopo la scadenza dell'intervallo di sincronizzazione.
Abilita limitazione delle richieste	Questa funzionalità consente di ottimizzare il carico sul server. Se la casella di controllo è selezionata, l'applicazione limita gli eventi trasmessi. Se il numero di eventi supera i limiti configurati, Kaspersky Endpoint Security interrompe l'invio degli eventi. **Numero massimo di eventi all'ora**. L'applicazione analizza il flusso di dati di telemetria e limita l'invio degli eventi se il flusso di eventi supera il limite di eventi all'ora configurato. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora. Se l'applicazione è installata in un server, il flusso di dati di telemetria è maggiore. Per i server, è consigliabile aumentare il valore a 60.000 eventi all'ora. **Percentuale di eccedenza limite eventi**. L'applicazione ordina gli eventi in base al tipo (ad esempio, eventi di "Modifiche nel Registro di sistema") e limita la trasmissione degli eventi se il rapporto tra eventi dello stesso tipo e il numero totale di eventi supera il limite percentuale configurato. Kaspersky Endpoint Security riprende l'invio degli eventi quando il rapporto tra altri eventi e il numero totale di eventi diventa di nuovo sufficientemente elevato.
Connessione ai server di risposta *(disponibile solo per Endpoint Detection and Response Expert 8.0 o versione successiva)*	Impostazioni di connessione alle impostazioni dei server di risposta. Immettere l'indirizzo IP del server di risposta (IPv4 o IPv6) e la porta per connettersi al server. È possibile aggiungere più indirizzi server di risposta. Kaspersky Endpoint Security tenta di connettersi al server al primo indirizzo IP. Se non è possibile stabilire una connessione, Kaspersky Endpoint Security tenta di connettersi al secondo indirizzo IP nell'elenco e così via.
Impostazioni di connessione *(disponibile solo per Endpoint Detection and Response Expert 8.0 o versione successiva)*	Configurare quanto segue per la connessione ai server di risposta: • **Timeout connessione server**. Timeout massimo di risposta del server di risposta. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server di risposta. • **Certificato server**. Certificato TLS per stabilire una connessione attendibile con il server di risposta. • **Usa autenticazione a due vie**. Autenticazione bidirezionale quando si stabilisce una connessione sicura tra Kaspersky Endpoint Security e il server di risposta. Per utilizzare l'autenticazione bidirezionale, è necessario abilitare l'autenticazione bidirezionale nelle impostazioni del server di risposta, quindi recuperare un contenitore crittografico e impostare una password per proteggerlo. Un *contenitore crittografico* è un archivio PFX con un certificato e una chiave privata. È possibile ottenere un contenitore crittografico nella console di Kaspersky Anti Targeted Attack Platform (vedere le istruzioni nel file Guida di Kaspersky Anti Targeted Attack Platform). Dopo aver configurato le impostazioni del server di risposta, è necessario abilitare anche l'autenticazione a due vie nelle impostazioni di Kaspersky Endpoint Security e caricare un contenitore crittografico protetto da password. Il contenitore crittografico deve essere protetto tramite password. Non è possibile aggiungere un contenitore criptato con una password vuota.

Creare un'attività

Questa sezione descrive come utilizzare Kaspersky Security Center Web Console e Cloud Console per creare e configurare le attività che Kaspersky Endpoint Security esegue in un computer client o in un gruppo di computer gestiti da Kaspersky Security Center.

Un'attività è un set di azioni configurabili che Kaspersky Endpoint Security esegue in un computer client.

In Kaspersky Security Center Web Console e Cloud Console è possibile creare le seguenti attività:

- Scansione
- Aggiornamento
- Rollback
- Aggiungi chiave

Creare un'attività

1. Nella sezione **Dispositivi** a sinistra selezionare la sezione **Attività**.
2. Fare clic su **Aggiungi**.
   Verrà avviata l'Aggiunta guidata attività.
3. Nell'elenco a discesa **Applicazione** selezionare **Kaspersky Endpoint Security for Mac 12.2.1**.
4. Nell'elenco a discesa **Tipo di attività** selezionare l'attività che si desidera creare.
5. Se necessario, modificare il nome dell'attività nel campo **Nome attività**.
6. Selezionare i dispositivi a cui assegnare l'attività.
7. Configurare le impostazioni per il tipo di attività selezionato.
8. Completare l'Aggiunta guidata attività facendo clic su **Fine**.

> **Nota:** se si seleziona la casella di controllo **Apri i dettagli dell'attività al termine della creazione** nella finestra **Completare la creazione dell'attività**, è possibile procedere con la modifica delle impostazioni predefinite dell'attività. Se non si seleziona questa casella di controllo, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite dell'attività in un secondo momento.

È possibile eseguire le seguenti azioni sulle attività:

- Avviare e interrompere le attività.
- Configurare le impostazioni delle attività.
- Monitorare lo stato di avanzamento di un'attività.
- Copiare e spostare le attività da un gruppo all'altro.
- Eliminare le attività.

Per informazioni dettagliate sulle attività di Kaspersky Security Center Web Console, vedere la Guida di Kaspersky Security Center.

Per informazioni dettagliate sulle attività di Kaspersky Security Center Cloud Console, vedere la Guida di Kaspersky Security Center Cloud Console.

Configurare le impostazioni dell'attività Scansione

Nella scheda **Impostazioni applicazione** è possibile configurare le impostazioni dell'attività **Scansione** per Kaspersky Endpoint Security nei computer remoti.

Aprire le impostazioni dell'attività Scansione

1. Accedere a **Dispositivi** > **Attività**.
2. Fare doppio clic su un'attività con il tipo di attività **Scansione**.
3. Selezionare la scheda **Impostazioni applicazione**.

Eseguire le seguenti operazioni, se necessario:

- Definire un ambito di scansione.
- Specificare l'azione eseguita da Kaspersky Endpoint Security in caso di rilevamento di un oggetto infetto.
- Selezionare i tipi di file che Kaspersky Endpoint Security esaminerà durante l'esecuzione dell'attività Scansione.
- Configurare le impostazioni delle prestazioni di scansione.
- Selezionare i file compositi che Kaspersky Endpoint Security analizzerà.

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Configurare le impostazioni dell'attività Aggiungi chiave

Nella scheda **Impostazioni applicazione** è possibile configurare le impostazioni dell'attività **Aggiungi chiave** per Kaspersky Endpoint Security nei computer remoti.

Aprire le impostazioni dell'attività Aggiungi chiave

1. Accedere a **Dispositivi** > **Attività**.
2. Fare doppio clic su un'attività con il tipo di attività **Aggiungi chiave**.
3. Selezionare la scheda **Impostazioni applicazione**.

Eseguire le seguenti operazioni, se necessario:

- Rendere la chiave di licenza corrente una chiave di riserva.
- Selezionare un'altra chiave per l'attivazione di Kaspersky Endpoint Security nel computer di un utente.
- Aggiungere una nuova chiave di licenza all'archivio di Kaspersky Security Center.

Configurare l'attività Aggiornamento

Nella scheda **Impostazioni applicazione** è possibile configurare le impostazioni dell'attività **Aggiornamento** per Kaspersky Endpoint Security nei computer remoti.

Aprire le impostazioni dell'attività Aggiornamento

1. Accedere a **Dispositivi** > **Attività**.
2. Fare doppio clic su un'attività con il tipo di attività **Aggiornamento**.
3. Selezionare la scheda **Impostazioni applicazione**.

La principale sorgente degli aggiornamenti per Kaspersky Endpoint Security sono i server degli aggiornamenti dedicati di Kaspersky. Kaspersky Endpoint Security può inoltre utilizzare i punti di distribuzione, le cartelle locali o altri server Web come *sorgente degli aggiornamenti*.

Se si gestisce Kaspersky Endpoint Security tramite Kaspersky Security Center Web Console, l'elenco delle sorgenti degli aggiornamenti include i server degli aggiornamenti Kaspersky e i server di Kaspersky Security Center per impostazione predefinita. Kaspersky Endpoint Security scarica gli aggiornamenti prima dai server di Kaspersky Security Center, poi dai server degli aggiornamenti Kaspersky.

Se si gestisce Kaspersky Endpoint Security tramite Kaspersky Security Center Cloud Console, l'elenco delle sorgenti degli aggiornamenti include i server degli aggiornamenti Kaspersky e i punti di distribuzione per impostazione predefinita. Kaspersky Endpoint Security scarica gli aggiornamenti prima dai punti di distribuzione, poi dai server degli aggiornamenti Kaspersky. Per informazioni dettagliate sui punti di distribuzione, vedere la Guida di Kaspersky Security Center.

Eseguire le seguenti operazioni, se necessario:

- Attivare o disattivare l'aggiornamento dei moduli dell'applicazione.
- Aggiungere o eliminare le sorgenti degli aggiornamenti che verranno utilizzate per aggiornare Kaspersky Endpoint Security.

Ottenere una chiave di ripristino per un'unità criptata

Se un utente di un computer client dimentica o smarrisce le credenziali e non può accedere a un'unità criptata, è possibile ottenere una chiave di ripristino.

Ottenere una chiave di ripristino

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **Impostazioni** → **Opzioni di interfaccia**.
2. Abilitare l'interruttore **Mostra Criptaggio e protezione dei dati** per abilitare la gestione del criptaggio dei dati e fare clic su **Salva**.

3. Passare a **Operazioni** → **Criptaggio e protezione dei dati** → **Unità criptate**.

   Viene visualizzato l'elenco dei dispositivi criptati.

4. Selezionare la casella di controllo accanto al dispositivo con l'unità criptata.

5. Fare clic su **Concedi l'accesso al dispositivo in modalità offline**.

6. Nella finestra di dialogo **Concedi l'accesso al dispositivo in modalità offline**, selezionare il plug-in Web per Kaspersky Endpoint Security e fare clic su **OK**.

7. Fare clic su **Ottieni chiave di ripristino**.

   Nella finestra di dialogo corrente viene visualizzata una chiave di ripristino.

8. Salvare la chiave di ripristino nel modo più idoneo.

È possibile utilizzare questa chiave di ripristino in un computer client per accedere all'unità criptata.

Gestire l'applicazione dalla riga di comando

L'applicazione Kaspersky Endpoint Security può essere gestita dalla riga di comando.

Nota: al termine dell'installazione degli aggiornamenti dei moduli di Kaspersky Endpoint Security, la versione del client dell'applicazione nella riga di comando potrebbe essere diversa dalla versione installata dell'applicazione.

Sintassi della riga di comando:

```
kav <comando> <parametri>
```

Ogni comando dispone di una gamma specifica di parametri supportati.

Visualizzare la guida della riga di comando

Il seguente comando consente di visualizzare le informazioni relative alla sintassi della riga di comando dell'applicazione:

```
kav -? | help
```

Eseguire una scansione anti-malware

Sintassi del comando:

```
kav scan <ambito della scansione> <azione> <tipi di file> <esclusioni> <parametri rapporti> <parametri avanzati>
```

Nota: per eseguire una scansione anti-malware, è inoltre possibile utilizzare le attività create nell'applicazione avviando quella desiderata dalla riga di comando. L'attività viene avviata con i parametri specificati nell'interfaccia di Kaspersky Endpoint Security.

Descrizioni dei parametri

`<ambito della scansione>` – questo parametro specifica un elenco di oggetti da esaminare per rilevare eventuale codice dannoso. È possibile includere diversi parametri separandoli con uno spazio.

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Sono disponibili i seguenti valori:

- `<file>` - elenco di percorsi dei file e/o delle cartelle da esaminare. È possibile specificare i percorsi assoluti o relativi dei file. Gli elementi dell'elenco devono essere separati da uno spazio.

  Nota: se il nome di un oggetto o il relativo percorso include uno spazio o caratteri speciali (come `$`, `&`, o `@`), il nome deve essere racchiuso tra virgolette singole (`' '`) oppure ciascuno dei caratteri speciali deve essere preceduto da una barra rovesciata (`\`). Se viene fatto riferimento a una cartella specifica, verranno esaminati tutti i file e le cartelle in essa contenuti.

- `-all` – Scansione completa del computer.
- `-remdrives` – Tutte le unità rimovibili.
- `-fixdrives` – Tutte le unità interne.
- `-netdrives` – Tutte le unità di rete.
- `-@:<elencofile.lst>` – Percorso del file contenente un elenco di oggetti e cartelle all'interno dell'ambito di scansione. Il file deve essere in formato testo e ogni oggetto della scansione deve essere elencato in una riga separata. È possibile immettere solo un percorso assoluto del file.

`<azione>` – Questo parametro determina l'azione da eseguire sugli oggetti dannosi rilevati durante la scansione. Se il parametro non è definito, l'azione predefinita è quella che corrisponde al valore `-i8`.

Sono disponibili i seguenti valori:

- `-i0` – Nessuna azione sull'oggetto, esclusivamente il salvataggio delle informazioni sull'oggetto in un rapporto.
- `-i1` – Gli oggetti infetti vengono disinfettati e, se la disinfezione è impossibile, vengono ignorati.
- `-i2`– Gli oggetti infetti vengono disinfettati e se la disinfezione è impossibile, vengono eliminati; non vengono eliminati i contenitori, tranne quelli con intestazioni eseguibili (archivi SFX).
- `-i3` – Gli oggetti infetti vengono disinfettati e se la disinfezione è impossibile, vengono eliminati; vengono eliminati completamente i contenitori se è impossibile eliminare i file infetti al loro interno.
- `-i4` – Gli oggetti infetti vengono eliminati; vengono eliminati completamente i contenitori se è impossibile eliminare i file infetti contenuti.
- `-i8` – Viene richiesto l'intervento dell'utente se viene rilevato un oggetto infetto (utilizzato per impostazione predefinita).
- `-i9` – Viene richiesto l'intervento dell'utente al termine della scansione.

`<tipi di file>` – Questo parametro definisce i tipi di file che sono sottoposti a scansione anti-malware. Per impostazione predefinita, se questo parametro non è definito vengono esaminati solo i file potenzialmente infettabili (in base ai contenuti dei file).

Sono disponibili i seguenti valori:

- `-fe` – Vengono esaminati solo i file potenzialmente infettabili (in base all'estensione dei file).
- `-fi` – Vengono esaminati solo i file potenzialmente infettabili (in base ai contenuti dei file). Questo parametro viene utilizzato per impostazione predefinita.
- `-fa` – Esamina tutti i file.

`<esclusioni>` – Questo parametro definisce gli oggetti da escludere dalla scansione. È possibile includere diversi parametri separandoli con uno spazio.

Sono disponibili i seguenti valori:

- `-e:a` – Non esaminare gli archivi.
- `-e:b` – Non esaminare i database e-mail.
- `-e:m` – Non esaminare i messaggi di posta in formato testo.
- `-e:<maschera>` – Non esaminare gli oggetti in base alla maschera.
- `-e:<secondi>` – Ignora gli oggetti la cui scansione richiede un intervallo di tempo superiore alla durata specificata (in secondi).
- `-es:<formato>` – Ignora gli oggetti la cui scansione supera il valore specificato (in megabyte).

`<parametri rapporti>` – Questi parametri determinano il formato del rapporto sui risultati della scansione. È possibile specificare un percorso assoluto o relativo del file del rapporto. Se il parametro non è definito, vengono visualizzati i risultati del rollback e tutti gli eventi.

Sono disponibili i seguenti valori:

- `-r:<file rapporto>` – Registra solo gli eventi importanti nel file di rapporto specificato.
- `-ra:<file rapporto>` – Registra tutti gli eventi nel file di rapporto specificato.

`<parametri avanzati>` – Parametri che definiscono l'utilizzo delle tecnologie di scansione anti-malware e i file di configurazione:

- `-iSwift=<on|off>` – Consente di abilitare o disabilitare l'utilizzo di iSwift.
- `-c:<file di configurazione>` – Definisce il percorso del file di configurazione che contiene le impostazioni dell'applicazione per le attività di scansione anti-malware. È possibile indicare un percorso assoluto o relativo del file. Se questo parametro non è specificato, i valori impostati nell'interfaccia dell'applicazione sono usati insieme ai valori già specificati nella riga di comando.

Esempio:
Avviare la scansione delle cartelle ~/Documenti, /Applicazioni e il file test.exe:

```
kav scan ~/Documents /Applications 'my test.exe'
```

Scansione degli oggetti elencati nel file objects2scan.txt. Utilizzo del file di configurazione scan_settings.txt. Al termine della scansione, creare un rapporto per registrare tutti gli eventi:

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

File di configurazione di esempio:

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

Aggiornare l'applicazione

Sintassi del comando:

```
kav update <sorgente aggiornamenti> <parametri rapporti> <parametri avanzati>
```

Descrizioni dei parametri

`<sorgente aggiornamenti>` – Un server HTTP o una cartella di rete o locale da cui vengono scaricati gli aggiornamenti. Se non viene selezionato alcun percorso, sarà utilizzata la sorgente degli aggiornamenti definita nelle impostazioni di aggiornamento dell'applicazione.

`<parametri rapporti>` – Questi parametri determinano il formato del rapporto sui risultati della scansione. È possibile specificare un percorso assoluto o relativo del file del rapporto. Se il parametro non è definito, vengono visualizzati i risultati del rollback e tutti gli eventi.

Sono disponibili i seguenti valori:

- `-r: <file rapporto>` – Registra solo gli eventi importanti nel file di rapporto specificato.
- `-ra: <file rapporto>` – Registra tutti gli eventi nel file di rapporto specificato.

`<parametri avanzati>` – Un parametro che definisce l'utilizzo di un file di configurazione.

`-c: <file di configurazione>` – Definisce il percorso di un file di configurazione che contiene le impostazioni dell'applicazione per l'aggiornamento dell'applicazione. È possibile indicare un percorso assoluto o relativo del file. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia dell'applicazione.

Esempio:
Aggiornamento dei database dell'applicazione dalla sorgente predefinita, registrazione di tutti gli eventi nel rapporto:

```
kav update -ra:avbases_upd.txt
```

Aggiornamento dei moduli di Kaspersky Endpoint Security mediante i parametri del file di configurazione updateapp.ini:

```
kav update -app=on -c:updateapp.ini
```

Eseguire il rollback dell'ultimo aggiornamento

Sintassi del comando:

```
kav rollback <parametri rapporti>
```

Importante: sono necessari i diritti di amministratore per l'esecuzione di questo comando.

Descrizioni dei parametri

`<parametri rapporti>` – Questo parametro definisce il formato del rapporto contenente i risultati del rollback dell'aggiornamento. È possibile specificare un percorso assoluto o relativo del file del rapporto. Se il parametro non è definito, vengono visualizzati i risultati del rollback e tutti gli eventi.

Sono disponibili i seguenti valori:

- `-r: <file rapporto>` – Registra solo gli eventi importanti nel file di rapporto specificato.
- `-ra: <file rapporto>` – Registra tutti gli eventi nel file di rapporto specificato.

Esempio:
```
kav rollback -ra:rollback.txt
```

Avviare/interrompere un'attività o un componente

La sintassi del comando di avvio:

```
kav start <nome componente o attività> <parametri rapporto>
```

La sintassi del comando di interruzione:

```
kav stop <nome componente o attività>
```

Importante: sono necessari i diritti di amministratore per l'esecuzione del comando di arresto.

Descrizioni dei parametri

`<nome componente o attività>` – Specificare uno dei seguenti valori:

- `fm` o `file_monitoring` – Protezione Minacce File
- `wm` o `web_monitoring` – Protezione Minacce Web
- `mail_monitoring` – Protezione Minacce di Posta
- `ids` – Protezione Minacce di Rete
- `firewall` – Firewall
- `behaviordetection` – Rilevamento del comportamento
- `exploitprevention` – Prevenzione Exploit
- `remediationengine` – Motore di Remediation

- `devicecontrol` – Controllo dispositivi
- `webcontrol` – Controllo Web
- `full` o `scan_my_computer` – Attività Scansione completa
- `scan_objects` – Attività Scansione personalizzata
- `quick` o `scan_critical_areas` – Attività Scansione rapida
- `externalstoragesscanner` – Attività Scansione disco rimovibile
- `updater` – Attività di aggiornamento
- `rollback` – Attività di rollback
- `diskencryption` – Criptaggio disco FileVault
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response Expert (on premises)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

`<parametri rapporti>` – Questi parametri determinano il formato del rapporto sui risultati dell'attività o del componente. È possibile specificare un percorso assoluto o relativo del file del rapporto. Se questo parametro non è definito, Kaspersky Endpoint Security consente di visualizzare i risultati secondo i parametri configurati nell'interfaccia utente.

Nota: `<parametri rapporto>` è disponibile solo per `scan_objects`, `updater` e valori di `rollback`.

Sono disponibili i seguenti valori:

- `-r: <file rapporto>` – Registra solo gli eventi importanti nel file di rapporto specificato.
- `-ra: <file rapporto>` – Registra tutti gli eventi nel file di rapporto specificato.

Nota: i componenti e le attività avviati dal prompt dei comandi vengono eseguiti con i parametri configurati nell'interfaccia utente.

Esempio:
Per abilitare il componente Protezione Minacce File, immettere il seguente comando nella riga di comando:

```
kav start fm
```

Per interrompere l'attività Scansione completa dalla riga di comando, immettere il seguente comando:

```
kav stop scan_my_computer
```

Visualizzare lo stato e le statistiche di un componente o un'attività

Sintassi del comando status:

```
kav status <nome componente o attività>
```

Sintassi del comando statistics:

```
kav statistics <nome componente o attività>
```

Descrizioni dei parametri

`<nome componente o attività>` – Specificare uno dei seguenti valori:

- `fm` o `file_monitoring` – Protezione Minacce File
- `wm` o `web_monitoring` – Protezione Minacce Web
- `mail_monitoring` – Protezione Minacce di Posta
- `ids` – Protezione Minacce di Rete
- `firewall` – Firewall
- `behaviordetection` – Rilevamento del comportamento
- `exploitprevention` – Prevenzione Exploit
- `remediationengine` – Motore di Remediation
- `devicecontrol` – Controllo dispositivi
- `webcontrol` – Controllo Web
- `full` o `scan_my_computer` – Attività Scansione completa
- `scan_objects` – Attività Scansione personalizzata
- `quick` o `scan_critical_areas` – Attività Scansione rapida
- `externalstoragesscanner` – Attività Scansione disco rimovibile
- `updater` – Attività di aggiornamento
- `rollback` – Attività di rollback
- `diskencryption` – Criptaggio disco FileVault

- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response Expert (on premises)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

Nota: se il comando status è eseguito senza specificare alcun valore per il parametro `<nome componente o attività>`, sarà visualizzato lo stato di tutte le attività e i componenti dell'applicazione. Per il comando statistics, è necessario specificare un valore per il parametro `<nome componente o attività>`.

Esportare le impostazioni di protezione

Sintassi del comando:

```
kav export <nome componente o attività> <file di esportazione>
```

Descrizioni dei parametri

`<nome componente o attività>` – Specificare uno dei seguenti valori:

- `fm` o `file_monitoring` – Protezione Minacce File
- `wm` o `web_monitoring` – Protezione Minacce Web
- `mail_monitoring` – Protezione Minacce di Posta
- `ids` – Protezione Minacce di Rete
- `firewall` – Firewall
- `behaviordetection` – Rilevamento del comportamento
- `exploitprevention` – Prevenzione Exploit
- `remediationengine` – Motore di Remediation
- `devicecontrol` – Controllo dispositivi
- `webcontrol` – Controllo Web
- `full` o `scan_my_computer` – Attività Scansione completa
- `scan_objects` – Attività Scansione personalizzata
- `quick` o `scan_critical_areas` – Attività Scansione rapida

- `externalstoragesscanner` – Attività Scansione disco rimovibile
- `updater` – Attività di aggiornamento
- `rollback` – Attività di rollback
- `diskencryption` – Criptaggio disco FileVault
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response Expert (on premises)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

`<file di esportazione>` – Percorso del file in cui sono esportate le impostazioni dell'applicazione. È possibile indicare un percorso assoluto o relativo del file.

Esempio:
```
kav export fm fm_settings.txt
```

Attivare l'applicazione

È possibile attivare Kaspersky Endpoint Security applicando un file chiave.

Sintassi del comando:

```
kav license /add <file chiave o codice di attivazione della chiave>
```

Descrizioni dei parametri

`<file chiave>` – File chiave dell'applicazione con estensione key.

`<codice di attivazione della chiave>` – Codice di attivazione in formato XXXX-XXXX-XXXX-XXXX.

Esempio:
```
kav license /add ./1AA111A1.key
kav license /add A11A1-11111-1A1AA-1A11A
```

Installazione dell'estensione di sistema

Sintassi del comando:

```
kav activatesystemextension /sysext
```

Nota: per completare l'installazione dell'estensione è necessario concedere a Kaspersky Endpoint Security le autorizzazioni nelle impostazioni **Privacy e sicurezza**.

Configurare le connessioni di rete

È possibile configurare le connessioni di rete per i componenti Protezione Minacce Web e Protezione Minacce di Rete.

Sintassi del comando:

```
kav activatesystemextension /webav
```

Nota: per completare la configurazione è necessario concedere a Kaspersky Endpoint Security le autorizzazioni per il filtro dei contenuti di rete.

Rimuovere le chiavi di licenza

È possibile rimuovere tutte le chiavi di licenza attualmente aggiunte all'applicazione.

Sintassi del comando:

```
kav license /del
```

Importante: sono necessari i diritti di amministratore per l'esecuzione di questo comando.

Codici restituiti della riga di comando

I codici generali possono essere restituiti da qualsiasi comando dalla riga di comando. I codici restituiti comprendono i codici generali nonché quelli relativi a un'attività specifica.

Sintassi del comando per la ricezione del codice restituito:

```
echo $?
```

Codici restituiti generali:

- `0` – Operazione completata con successo
- `1` – Valore non valido per il parametro

- `2` – Errore sconosciuto
- `3` – Errore di completamento dell'attività
- `4` – Attività annullata

Codici restituiti dall'attività di scansione anti-malware:

- `101` – Tutti gli oggetti dannosi sono stati elaborati
- `102` – Rilevati oggetti dannosi

Chiudere l'applicazione

Sintassi del comando:

```
kav exit
```

Importante: sono necessari i diritti di amministratore per l'esecuzione di questo comando.

Disinstallare l'applicazione

Per disinstallare Kaspersky Endpoint Security dalla riga di comando utilizzare la sequenza di comandi seguente:

```
sudo /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/UninstallScript
sudo /Library/Application\ Support/Kaspersky\ Lab/KAV/Binaries/UninstallScript
sudo rm -rf /Library/Application\ Support/Kaspersky\ Lab/ /Applications/Kaspersky
```

Importante: per disinstallare l'applicazione sono necessari i privilegi amministratore.

Comandi di gestione Detection and Response

È possibile utilizzare la riga di comando per gestire la funzionalità integrata della soluzione Detection and Response. È possibile gestire le soluzioni Detection and Response se la gestione tramite la console di Kaspersky Security Center non è possibile.

Gestire Prevenzione dell'esecuzione

È possibile visualizzare le impostazioni di Prevenzione dell'esecuzione del computer client e disabilitare la prevenzione dell'esecuzione nel computer client.

Sintassi del comando:

```
kav prevention </disable | /show>
```

Descrizioni dei comandi

`/disable` - Il comando per disattivare la prevenzione dell'esecuzione nel computer client.

`/show` - Il comando per visualizzare le impostazioni di Prevenzione dell'esecuzione, inclusa la modalità e l'elenco delle regole di prevenzione dell'esecuzione.

Gestire Isolamento di rete

È possibile visualizzare le impostazioni dell'Isolamento di rete dell'host e disabilitare l'Isolamento di rete nell'host.

Sintassi del comando:

```
kav isolation </off | /status>
```

Descrizioni dei comandi

`/off` - Il comando per disattivare l'Isolamento di rete.

Importante: sono necessari i diritti di amministratore per l'esecuzione di questo comando.

`/status` - Il comando per visualizzare lo stato dell'Isolamento di rete e le esclusioni.

Nota: questi comandi devono essere eseguiti contemporaneamente.

Contattare l'Assistenza tecnica

In questa sezione vengono descritte le modalità per ottenere assistenza tecnica e le condizioni con cui viene resa disponibile.

Come ottenere assistenza tecnica

Se non è possibile trovare una soluzione per il proprio problema nella documentazione di Kaspersky Endpoint Security o in una delle fonti di informazioni su Kaspersky Endpoint Security, contattare l'Assistenza tecnica di Kaspersky. Gli specialisti dell'Assistenza tecnica risponderanno a tutte le domande relative all'installazione e all'utilizzo di Kaspersky Endpoint Security.

Nota: Kaspersky garantisce il supporto di Kaspersky Endpoint Security durante il ciclo di vita (vedere la pagina del ciclo di vita del supporto dell'applicazione). Prima di contattare l'Assistenza tecnica, consultare le regole dell'assistenza.

È possibile contattare l'Assistenza tecnica in uno dei seguenti modi:

- Visitando il sito Web dell'Assistenza tecnica
- Inviando una richiesta all'Assistenza tecnica dal portale Kaspersky CompanyAccount

Assistenza tecnica tramite il 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 e specialisti di Kaspersky tramite le richieste online. È possibile utilizzare Kaspersky CompanyAccount per tenere traccia dello stato delle richieste online e archiviare la relativa cronologia.

In Kaspersky CompanyAccount è possibile registrare tutti i dipendenti dell'organizzazione con un unico account. Un unico account consente di gestire in modo centralizzato le richieste elettroniche da parte dei dipendenti registrati a Kaspersky, nonché di gestire i privilegi di tali 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.

Acquisire informazioni per l'Assistenza tecnica

Per un supporto e una risoluzione dei problemi dell'applicazione più efficaci, gli esperti dell'Assistenza tecnica possono richiedere all'utente di modificare temporaneamente le impostazioni dell'applicazione per il debug durante la diagnostica. A tale scopo può essere necessario eseguire le seguenti operazioni:

- Attivazione della funzionalità per l'estrazione di informazioni di diagnostica estese.
- Ottimizzazione delle impostazioni dei singoli componenti dell'applicazione, non disponibili tramite elementi di interfaccia utente standard.
- Modifica delle impostazioni di trasmissione delle informazioni diagnostiche estratte.

Gli specialisti dell'Assistenza tecnica forniranno all'utente tutte le informazioni necessarie per eseguire le operazioni elencate e indicare l'ambito dei dati da acquisire per il debug. Dopo l'estrazione delle informazioni di diagnostica estese, queste vengono salvate nel computer dell'utente. I dati non vengono inviati automaticamente a Kaspersky.

Utilizzare un file di traccia

Quando si segnala un problema agli specialisti del servizio di Assistenza tecnica di Kaspersky, questi potrebbero richiedere di generare un rapporto con informazioni sull'esecuzione di Kaspersky Endpoint Security e di inviarlo all'Assistenza tecnica di Kaspersky. All'utente potrebbe essere richiesto inoltre di creare un *file di traccia*. Il file di traccia consente di analizzare nel dettaglio l'esecuzione dei comandi dell'applicazione e di stabilire quando si verificano gli errori.

Creare un file di traccia

Il tracciamento è un modo efficace di registrare le informazioni sulle attività dell'applicazione. Gli esperti dell'Assistenza tecnica usano i file di traccia per la risoluzione dei problemi.

Creare un file di traccia

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Interfaccia**, nella sezione **Tracce**, selezionare la casella di controllo **Abilita tracce**.

Importante: è consigliabile abilitare la traccia solo se richiesto da un esperto dell'Assistenza tecnica di Kaspersky.

I file di traccia possono richiedere molto spazio su disco. Quando i file di traccia non sono più necessari, disabilitare la traccia.

Disabilitare la traccia

1. Nella barra dei menu fare clic sull'icona dell'applicazione e scegliere **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni dell'applicazione.

2. Nella scheda **Interfaccia**, nella sezione **Tracce**, deselezionare la casella di controllo **Abilita tracce**.

Kaspersky Endpoint Security salva le seguenti informazioni in un file di traccia:

- Informazioni sul dispositivo e sul sistema operativo (ID univoco dispositivo, tipo di dispositivo, indirizzi MAC dei dispositivi di rete, tipo di sistema operativo, versione del sistema operativo).
- Informazioni sul funzionamento dell'applicazione e dei relativi moduli.
- Informazioni sull'abbonamento (tipo di abbonamento, area geografica).
- Informazioni sulle impostazioni locali della lingua, ID applicazione, personalizzazione applicazione, versione applicazione, ID installazione univoco dell'applicazione, ID univoco computer.
- Informazioni sullo stato della protezione anti-malware del computer, nonché su tutti gli oggetti rilevati ed elaborati (nome dell'oggetto rilevato, data e ora del rilevamento, indirizzo Web da cui è stato eseguito il download, nomi e dimensioni dei file infetti e relativi percorsi, indirizzo IP del computer che ha originato l'attacco e numero della porta del computer interessata dall'attacco di rete, elenco delle attività malware e indirizzi Web indesiderati) e le relative decisioni e azioni intraprese dall'applicazione e dall'utente.
- Informazioni sulle applicazioni scaricate dall'utente (indirizzo Web, attributi, dimensioni dei file e informazioni sul processo che ha scaricato il file).
- Informazioni sulle applicazioni avviate e sui moduli delle applicazioni (dimensioni, attributi, data di creazione, dettagli dell'intestazione PE, area geografica, nome, percorso e programmi di compressione).
- Informazioni sugli errori dell'interfaccia e sull'utilizzo dell'interfaccia dell'applicazione Kaspersky installata.
- Informazioni sulle connessioni di rete: l'indirizzo IP del computer remoto e del computer dell'utente, i numeri delle porte utilizzate per stabilire la connessione e il protocollo di rete della connessione.
- Informazioni sui pacchetti di rete ricevuti e inviati dal computer tramite le reti IT e di telecomunicazione.
- Informazioni sui messaggi e-mail e i messaggi istantanei inviati e ricevuti.
- Informazioni sugli indirizzi Web visitati: l'orario in cui è stata stabilita la connessione utilizzando un protocollo aperto, dati sul nome utente e la password per il sito Web e contenuto dei cookie.
- Certificato pubblico del server.

I file di traccia contengono solo le informazioni necessarie per risolvere gli errori dell'applicazione. Kaspersky utilizza i file di traccia per analizzare gli incidenti associati agli errori durante l'esecuzione dell'applicazione Kaspersky Endpoint Security.

Per impostazione predefinita, la creazione dei file di traccia è disabilitata. È possibile abilitare la generazione dei file di traccia nelle impostazioni dell'applicazione.

I file di traccia possono essere inviati solo manualmente a Kaspersky. L'applicazione non invia automaticamente i file di traccia a Kaspersky.

È possibile scegliere la modalità di invio dei file di traccia a Kaspersky.

Prima di inviare i file di traccia a Kaspersky, rivedere i dati che contengono.

Importante: i file di traccia possono contenere informazioni personali o sensibili. Inviando i file di traccia a Kaspersky, l'utente accetta di fornire a Kaspersky tutti i dati contenuti nei file di traccia inviati e accetta il metodo utilizzato per l'invio.

Fonti di informazioni sull'applicazione

Questa sezione descrive le fonti di informazioni sull'applicazione.

È possibile scegliere la fonte di informazioni più adatta a seconda dell'importanza e dell'urgenza del problema.

Pagina di Kaspersky Endpoint Security nel sito Web di Kaspersky

Nella pagina di Kaspersky Endpoint Security sul sito Web di Kaspersky è possibile visualizzare informazioni generali sull'applicazione e 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 nel sito Web dell'Assistenza tecnica di Kaspersky.

Nella pagina di Kaspersky Endpoint Security nella Knowledge Base è possibile leggere articoli che forniscono informazioni utili, raccomandazioni e risposte alle domande più frequenti relative all'acquisto, l'installazione e l'utilizzo dell'applicazione.

Gli articoli della Knowledge Base possono fornire risposte a domande relative sia a Kaspersky Endpoint Security che ad altre applicazioni Kaspersky. Gli articoli della Knowledge Base possono inoltre contenere notizie dell'Assistenza tecnica di Kaspersky.

Accedere alla Knowledge Base dal menu a discesa Guida

1. Selezionare **Guida** → **Assistenza**.
2. Fare clic su **Assistenza tecnica**.

Discutere delle applicazioni Kaspersky nel forum

Se la domanda non richiede una risposta immediata, è possibile sottoporla agli specialisti di Kaspersky e ad altri utenti nel Forum.

Nel Forum è possibile visualizzare gli argomenti di discussione, pubblicare i propri commenti e creare nuovi argomenti di discussione.

Accedere al forum dal menu a discesa Guida

1. Selezionare **Guida** → **Assistenza**.
2. Fare clic su **Community**.

Appendici

Questa sezione contiene informazioni complementari al testo della documentazione.

Problemi noti e limitazioni

Kaspersky Endpoint Security presenta le seguenti limitazioni e i seguenti problemi noti:

- Se nel computer è installata un'applicazione che raccoglie informazioni e le invia per l'elaborazione, l'applicazione Kaspersky Endpoint Security può classificare questa applicazione come malware. Per evitare questo, è possibile escludere l'applicazione dalla scansione configurando l'applicazione Kaspersky Endpoint Security come descritto nel presente documento.
- Le impostazioni funzionali dell'applicazione possono essere modificate modificando i file di configurazione.
- In Kaspersky Security Center le attività locali possono essere elencate due volte nelle proprietà dei dispositivi gestiti.
- La modifica della sorgente degli aggiornamenti per un'attività di aggiornamento locale disabilita l'esecuzione automatica dell'attività di aggiornamento.
- Se si avvia un'attività di riavvio del computer tramite Administration Console con un messaggio per l'utente contenente un punto e virgola (;), l'attività viene visualizzata come completata ma all'utente non viene richiesto di riavviare il Mac.
- Per escludere il traffico di rete di Safari dalla scansione da parte di Kaspersky Endpoint Security, è necessario aggiungere i seguenti percorsi all'elenco delle esclusioni:
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.a`
  - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit`
- Per escludere il traffico di rete di Google Chrome dalla scansione da parte di Kaspersky Endpoint Security, è necessario aggiungere il seguente percorso all'elenco delle esclusioni:
  - `/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/<VersionNumber>/Helpers/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper`
- Dopo aver creato un profilo criterio per un criterio di Kaspersky Endpoint Security utilizzando Kaspersky Security Center Web Console e Cloud Console, è necessario verificare che le impostazioni siano applicate correttamente nei computer client.
- Quando si abilita il criptaggio del disco FileVault nelle impostazioni dei criteri, gli utenti con diritti di amministratore possono decriptare il disco di avvio del Mac da Impostazioni di Sistema (Preferenze di Sistema).

- Le modifiche apportate alle opzioni del server proxy verranno applicate solo dopo il riavvio di Kaspersky Endpoint Security.
- Safari potrebbe non connettersi a un sito Web con un certificato non attendibile. È possibile aggiungere un sito Web di questo tipo alle esclusioni o utilizzare un altro browser.
- Dopo la disinstallazione di Kaspersky Endpoint Security 11.2 o versione successiva in remoto tramite Kaspersky Security Center, una delle estensioni di sistema dell'applicazione potrebbe rimanere nella memoria del computer. In rari casi può verificarsi un problema con l'autorizzazione accesso completo al disco durante l'installazione di Kaspersky Endpoint Security. In questo caso è consigliabile disinstallare l'applicazione in locale e reinstallarla.
- Le applicazioni che richiedono Rosetta potrebbero non essere installate se Kaspersky Endpoint Security è in esecuzione. Per risolvere il problema, chiudere Kaspersky Endpoint Security e provare a reinstallare l'applicazione.
- I dettagli degli avvisi per le minacce rilevate all'interno degli oggetti composti contengono solo informazioni sull'oggetto stesso rilevato senza un grafico della catena di sviluppo della minaccia.
- Durante il salvataggio di una password per Protezione tramite password, potrebbe verificarsi un errore. In questo caso, si consiglia di disinstallare e reinstallare l'applicazione.
- Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.
- Non è possibile eseguire la scansione di un oggetto inserito in Quarantena a causa dell'attività Sposta file in Quarantena.
- In Kaspersky Security Center il nome del dispositivo viene visualizzato correttamente solo se il nome NetBIOS, il nome del computer e il nome host coincidono.

Problemi risolti

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

Elenco dei problemi risolti nella versione 12.2.1

ID problema	Descrizione del problema
10054891	Non è possibile aggiungere un'applicazione all'area attendibile nel criterio di Kaspersky Endpoint Security for Mac in Web Console.

Elenco di oggetti esaminati in base all'estensione

Se durante la creazione di un'attività di scansione in Kaspersky Security Center nelle impostazioni di scansione è stata selezionata l'opzione **Esamina applicazioni e documenti in base all'estensione**, Kaspersky Endpoint Security esegue scansioni anti-malware sugli oggetti senza estensione e sugli oggetti con le seguenti estensioni:

Formati generali:

- txt
- csv
- htm
- html

File multimediali (audio/video):

- flv
- f4v
- avi
- 3gp
- 3g2
- 3gp2
- 3p2
- divx
- mp4
- mkv
- mov
- qt
- asf
- wmv
- rm
- rmvb
- vob
- dat
- mpg

- mpeg
- bik
- fcs
- mp3
- mpeg3
- flac
- ape
- ogg
- aac
- m4a
- wma
- ac3
- wav
- mka
- rm
- ra
- ravb
- mid
- midi
- cda

File di immagine:

- jpg
- jpe
- jpeg
- jff
- gif

- png
- bmp
- tif
- tiff
- emf
- wmf
- eps
- psd
- cdr
- swf

File eseguibili e di sistema:

- exe
- dll
- scr
- ocx
- com
- sys
- class
- o
- so
- elf
- prx
- vb
- vbs
- js
- bat

- cmd
- msi
- deb
- rpm
- sh
- pl
- dylib

Documenti e modelli:

- doc
- dot
- docx
- dotx
- docm
- dotm
- xsl
- xls
- xlsx
- xltx
- xlsm
- xltm
- xlam
- xlsb
- ppt
- pot
- pps
- pptx

- potx
- pptm
- potm
- ppsx
- ppsm
- rtf
- pdf
- msg
- eml
- vsd
- vss
- vst
- vdx
- vsx
- vtx
- xps
- oxps
- one
- onepkg
- xsn
- odt
- ods
- odp
- sxw
- pub
- mdb
- accdb
- accde

- accdr
- accdc
- chm
- mht

Archivi:

- zip
- 7z*
- 7-z
- rar
- iso
- cab
- jar
- bz
- bz2
- tbz
- tbz2
- gz
- tgz
- arj
- dmg
- smi
- img
- xar

Nota: il formato effettivo di un file potrebbe non corrispondere alla relativa estensione del nome file.

Maschere nei percorsi di file e cartelle

Una maschera per il nome del file o una maschera per il nome della cartella rappresenta il nome e l'estensione di un file o il nome di una cartella utilizzando simboli comuni.

È possibile utilizzare questi simboli quando si specifica l'ambito della protezione, l'ambito della scansione e l'area attendibile.

- Il simbolo tilde `~` sostituisce `/Users/<nome utente>` nel percorso di un file o una cartella. Ad esempio, il percorso `~/Desktop` indica che l'ambito di protezione include le cartelle `Desktop` di tutti gli utenti nei computer che si desidera proteggere.

- Il simbolo asterisco `*` sostituisce qualsiasi set di caratteri nel nome di un file o di una cartella, ad eccezione dei caratteri `\` e `/` (che delimitano i nomi dei file e delle cartelle nei percorsi dei file e delle cartelle). Ad esempio, la maschera `/*/*.db*` includerà tutti i percorsi dei file con un'estensione che inizia con `db` presenti nelle cartelle sul disco interno, ma non nelle sottocartelle.

- Due simboli asterisco consecutivi `**` sostituiscono qualsiasi set di caratteri (incluso un set vuoto) nel nome di un file o di una cartella, inclusi i caratteri `\` e `/` (che delimitano i nomi dei file e delle cartelle nei percorsi dei file e delle cartelle). Ad esempio, la maschera `/Folder/**/*.txt` includerà tutti i percorsi dei file con l'estensione `TXT` presenti nella cartella denominata `Folder` e nelle sottocartelle. La maschera deve includere almeno un livello di nidificazione. La maschera `/**/*.txt` non è una maschera valida.

- Il punto interrogativo `?` sostituisce qualsiasi carattere singolo nel nome di un file o di una cartella, ad eccezione dei caratteri `\` e `/` (che delimitano i nomi dei file e delle cartelle nei percorsi dei file e delle cartelle). Ad esempio, la maschera `/Folder/???.txt` includerà i percorsi di tutti i file presenti nella cartella denominata `Folder` con l'estensione TXT e un nome composto da tre caratteri.

Requisiti del file IOC

Quando si creano attività di scansione IOC, considerare i seguenti requisiti e limitazioni del file IOC:

- L'applicazione supporta i file IOC con le estensioni IOC, XML e JSON nelle versioni OpenIOC standard aperte 1.0 e 1.1 o STIX versioni 2.0 e 2.1 per la descrizione degli indicatori di compromissione.

- Se durante la creazione di un'attività di scansione IOC nella riga di comando si caricano file IOC, alcuni dei quali non sono supportati, quando l'attività viene eseguita, l'applicazione utilizza solo i file IOC supportati. Se, durante la creazione di un'attività di scansione IOC nella riga di comando, tutti i file IOC caricati risultano non supportati, l'attività può ancora essere eseguita, ma non rileverà alcun indicatore di compromissione. Non è possibile caricare file IOC non supportati utilizzando Web Console o Cloud Console.

- Gli errori semantici e i termini e i tag IOC non supportati nei file IOC non determinano l'esito negativo dell'esecuzione dell'attività. In tali sezioni dei file IOC, l'applicazione non rileva alcuna corrispondenza.

- Gli identificatori di tutti i file IOC utilizzati in una singola attività di scansione IOC devono essere univoci. Se sono presenti file IOC con lo stesso identificatore, ciò potrebbe influire sui risultati dell'esecuzione dell'attività.

- Un singolo file IOC non deve superare le dimensioni di 2 MB. Se si utilizzano file di dimensioni maggiori le attività di scansione IOC termineranno con un errore. La dimensione totale di tutti i file aggiunti alla raccolta IOC non deve superare i 10 MB. Se la dimensione totale di tutti i file supera i 10 MB, è necessario dividere la raccolta IOC e creare diverse attività di Scansione IOC.

- Si consiglia di creare un file IOC per minaccia. Ciò semplifica l'analisi dei risultati dell'attività di Scansione IOC.

Le caratteristiche e le limitazioni del supporto dell'applicazione per i file IOC vengono mostrate nella tabella seguente.

Funzionalità e limitazioni del supporto per i documenti IOC.

Condizioni supportate	OpenIOC 1.0:
	
	`is`
	`isnot` (come eccezione rispetto al set)
	`contiene`
	`containsnot` (come eccezione rispetto al set)
	OpenIOC 1.1:
	
	`is`
	`contiene`
	`starts-with`
	`ends-with`
	`corrispondenze`
	`greater-than`
	`less-than`
	STIX 2.0 e 2.1:
	
	`=`
	`!=`
	`>`
	`<`
	`=>`
	`<=`
	`in`
	`like`
	`corrispondenze`

Attributi della condizione supportati	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Operatori supportati	`AND` `OR`
Tipi di dati supportati	`"date"`: data (condizioni applicabili: `is`, `greater-than`, `less-than`) `"int"`: numero intero (condizioni applicabili: `is`, `greater-than`, `less-than`) `"string"`: stringa (condizioni applicabili: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: durata in secondi (condizioni applicabili: `is`, `greater-than`, `less-than`)

Caratteristiche dell'interpretazione del tipo di dati	I tipi di dati `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` vengono interpretati come stringa.
	
	L'applicazione supporta l'interpretazione dell'impostazione `Content` per i tipi di dati `int` e `date` quando è impostata sotto forma di intervalli:
	
	OpenIOC 1.0:
	Utilizzando l'operatore `TO` nel campo `Contenuto`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Utilizzo delle condizioni `greater-than` e `less-than`
	Utilizzo dell'operatore `TO` nel campo `Contenuto`
	L'applicazione supporta l'interpretazione dei tipi di dati di `daty` e `duration` se gli indicatori sono impostati in formato `ISO 8601`, `Zulu Time Zone`, `UTC`.

Interpreti di script supportati per Prevenzione dell'esecuzione

Prevenzione dell'esecuzione supporta i seguenti interpreti di script:

- PkgUtil
- PkgInstaller
- /usr/bin/osascript
- /usr/bin/osacompile
- /usr/local/bin/python
- /usr/local/bin/python3
- /usr/bin/perl
- /usr/bin/ruby
- /bin/bash
- /bin/zsh
- /bin/sh
- /bin/dash
- /bin/csh
- /bin/ksh
- /bin/tcsh

Importante: se lo script specificato nella regola di prevenzione dell'esecuzione viene aperto dagli interpreti di script PkgUtil o PkgInstaller già avviati, l'esecuzione di questo script non verrà bloccata.

Come aggiungere il certificato Kaspersky Endpoint Security all'archivio dei certificati di Mozilla Firefox

Se il browser utilizza l'archivio certificati di Mozilla Firefox, è necessario esportare e aggiungere manualmente il certificato Kaspersky a questo archivio certificati. In caso contrario, il browser non sarà in grado di aprire le pagine HTTPS.

Esportare il certificato Kaspersky

1. Aprire **Launchpad** > **Altro** > **Accesso keychain** nel Mac.
2. Nel riquadro sinistro della finestra, fare clic su **Sistema** e aprire la scheda **Certificati**.
3. Nell'elenco dei certificati, individuare **Kaspersky Web Anti-Virus Certification Authority**.
4. Fare clic con il pulsante destro del mouse su questo certificato e selezionare **Esporta "Kaspersky Web Anti-Virus Certification Authority"**.
5. Selezionare una posizione in cui salvare il certificato e fare clic su **Salva**.

Il certificato Kaspersky viene salvato.

Aggiungere il certificato Kaspersky all'archivio certificati di Mozilla Firefox

1. Aprire Mozilla Firefox
2. Nell'angolo superiore destro, fare clic sul pulsante del menu e selezionare **Impostazioni**.
3. Nel riquadro sinistro della finestra selezionare **Privacy e sicurezza**.
4. Scorrere verso il basso fino alla sezione **Certificati**.
5. Fare clic su **Visualizza certificati**.
6. Nella finestra visualizzata fare clic su **Importa**.
7. Scegliere il file del certificato Kaspersky e fare clic su **Apri**.
8. Selezionare le caselle di controllo **Considera attendibile questa CA per identificare i siti Web** e **Considera attendibile questa CA per identificare gli utenti e-mail**. Fare clic su **OK**.

   Il certificato Kaspersky viene importato nell'archivio certificati di Mozilla Firefox. Viene visualizzato nell'elenco dei certificati nella finestra **Gestione certificati**.

Importante: ogni volta che l'applicazione Kaspersky Endpoint Security viene reinstallata, viene generato un nuovo certificato radice Kaspersky. Ciò significa che è necessario completare questa procedura dopo ogni reinstallazione dell'applicazione Kaspersky Endpoint Security.

Impostazioni di rete per l'interazione con servizi esterni

Kaspersky Endpoint Security utilizza le seguenti impostazioni di rete per interagire con i servizi esterni.

Impostazioni di Rete

Indirizzo	Descrizione
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocollo: `HTTPS` Porta: `443`	Attivazione dell'applicazione.

Indirizzo	Descrizione

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protocollo: `HTTPS`
Porta: `443`
	Aggiornamento di database e moduli software dell'applicazione.

`downloads.upd.kaspersky.com` Protocollo: `HTTPS` Porta: `443`	• Aggiornamento di database e moduli software dell'applicazione. • Verifica dell'accesso ai server Kaspersky. Se non è possibile accedere ai server che utilizzano il DNS di sistema, l'applicazione utilizza il DNS pubblico. Ciò è necessario per assicurarsi che i database antivirus siano aggiornati e che il livello di protezione del computer sia mantenuto. Kaspersky Endpoint Security utilizza il seguente elenco di server DNS pubblici nel seguente ordine: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168).

Indirizzo	Descrizione
	Importante: Le richieste emesse dall'applicazione possono contenere indirizzi di domini e l'indirizzo IP pubblico dell'utente, poiché l'applicazione stabilisce una connessione TCP/UDP con il server DNS. Queste informazioni sono necessarie, ad esempio, per convalidare il certificato di una risorsa Web quando si utilizza HTTPS. Se Kaspersky Endpoint Security utilizza un server DNS pubblico, l'elaborazione dei dati è regolata dall'informativa sulla privacy del servizio pertinente. **Come impedire a Kaspersky Endpoint Security di utilizzare un server DNS pubblico** 1. Chiudere l'applicazione Kaspersky Endpoint Security nel dispositivo dell'utente. 2. Aggiungere la variabile `ForceUseSystemDNS` e impostare il valore su `1` nel file di configurazione dell'applicazione Kaspersky Endpoint Security disponibile in `/Library/Application Support/ Kaspersky Lab/KAV/Binaries/config.xml`. 3. Avviare l'applicazione Kaspersky Endpoint Security. Di conseguenza, l'applicazione Kaspersky Endpoint Security utilizzerà solo il DNS di sistema.
`touch.kaspersky.com` Protocollo: `HTTP`	• Ricezione dell'ora attendibile per il controllo del periodo di validità del certificato (connessione TLS). • Avviso relativo al negato accesso a una risorsa Web nel browser quando Protezione minacce Web è in esecuzione.

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protocollo: `HTTP`
Porta: `80`
	Aggiornamento di database e moduli software dell'applicazione.

Indirizzo	Descrizione

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protocollo: `HTTPS`
Porta: `443`
	Utilizzo di Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protocollo: `KSN`
Porta: `443`, `1443`
	Utilizzo di Kaspersky Security Network.

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Protocollo: `HTTPS`
Porta: `443`
	Seguire i collegamenti presenti nell'interfaccia.

Impostazioni utilizzate per il criptaggio

Indirizzo	Descrizione

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocollo: `HTTP`
Porta: `80`
	PKI (Public Key Infrastructure).

Informazioni sul codice di terze parti

Le informazioni sul codice di terze parti sono contenute nel file legal_notices.txt ubicato nella cartella di installazione dell'applicazione.

Note relative ai marchi

I marchi registrati e i marchi di servizi sono di proprietà dei rispettivi titolari.

ActiveSync, Active Directory, Excel, IIS, Microsoft, Outlook, Windows, Windows Installer e WMI sono marchi di fabbrica del gruppo di aziende Microsoft.

Apple, Apple Remote Desktop, FileVault, iCloud, Keychain, Launchpad, Mac, macOS, Rosetta, Safari e Xcode sono marchi di Apple Inc.

Chrome, Gmail, Google e Google Chrome sono marchi di Google, LLC.

Composer e JAMF sono marchi registrati o di diritto comune di JAMF SOFTWARE, LLC negli Stati Uniti e in altri paesi.

Firefox, Mozilla e Thunderbird sono marchi di Mozilla Foundation negli Stati Uniti e in altri paesi.

Intel è un marchio di Intel Corporation o delle relative consociate.

JavaScript è un marchio registrato di Oracle e/o delle sue affiliate.

Linux è un marchio di Linus Torvalds registrato negli Stati Uniti e in altri paesi.

Parallels, il logo Parallels e Coherence sono marchi o marchi registrati di Parallels International GmbH.

VMware e VMware Fusion sono marchi o marchi registrati di VMware, Inc. negli Stati Uniti e in altri paesi.

Finestra Assistenza per gli utenti

Questa finestra fornisce le seguenti informazioni:

- Versione di Kaspersky Endpoint Security
- Data di rilascio dei database utilizzata attualmente da Kaspersky Endpoint Security
- Versione del sistema operativo installata nel computer

Assistenza tecnica

Questo pulsante apre la Knowledge Base dell'Assistenza tecnica di Kaspersky, dove è possibile trovare articoli su Kaspersky Endpoint Security pubblicati dagli specialisti dell'Assistenza tecnica.

Community

Questo pulsante consente di aprire la community dove è possibile discutere di Kaspersky Endpoint Security con gli esperti Kaspersky e altri utenti.

Chiudi

Questo pulsante chiude la finestra Assistenza.

Finestra Impostazioni certificato

Nella scheda **Generali** è possibile selezionare l'archivio del certificato per il controllo del traffico HTTPS criptato nel browser Mozilla Firefox:

- **Keychain delle radici di sistema (scelta consigliata)**
- **Archivio certificati dalle impostazioni del browser Mozilla Firefox**

  In questo caso, è necessario aggiungere manualmente il certificato Kaspersky Endpoint Security all'archivio certificati del browser Mozilla Firefox. Per ulteriori informazioni, fare riferimento alla sezione Come aggiungere il certificato Kaspersky Endpoint Security all'archivio dei certificati di Mozilla Firefox.

Nella scheda **Certificati attendibili** è possibile creare un elenco di certificati radice attendibili per connettersi ai server corrispondenti senza notifiche.

Per impostazione predefinita, l'elenco è vuoto.

+

Questo pulsante consente di aprire una finestra di dialogo per l'aggiunta dei certificati che verranno considerati attendibili.

–

Questo pulsante consente di eliminare il certificato selezionato dall'elenco dei certificati attendibili.

Nome certificato

Questa colonna mostra i nomi dei certificati radice attendibili.

Annulla

Questo pulsante consente di chiudere la finestra senza salvare le modifiche.

Salva

Questo pulsante consente di salvare l'elenco corrente di certificati radice attendibili e consente inoltre di chiudere la finestra.

Finestra Verificare il certificato

Mostra certificato

Questo pulsante consente di aprire una finestra di sistema con le informazioni relative al certificato.

Annulla

Questo pulsante consente di chiudere la finestra.

Aggiungi ad Attendibili

Questo pulsante consente di aggiungere il certificato all'elenco dei certificati attendibili. Di conseguenza, l'utente sarà in grado di connettersi al server corrispondente senza notifiche.

Connetti

Questo pulsante consente di connettere l'utente al server.

Nota: i pulsanti disponibili possono variare in base al tipo di certificato.

Finestra Selezionare il certificato

Elenco dei certificati disponibili

Selezionare la casella di controllo accanto a un certificato per utilizzarlo durante la connessione al server.

Mostra certificato

Questo pulsante consente di aprire una finestra di sistema con le informazioni relative al certificato.

Annulla

Questo pulsante consente di chiudere la finestra.

Continua

Questo pulsante consente di continuare la connessione al server utilizzando il certificato selezionato.

Finestra "Rilevato archivio protetto da password"

Se Kaspersky Endpoint Security deve esaminare un archivio protetto da password durante l'esecuzione di Protezione Minacce File o di un'attività di scansione, verrà visualizzata una finestra di notifica.

Archivio

Percorso dell'archivio.

Password

Campo di immissione della password.

Se si immette la password, Kaspersky Endpoint Security esamina l'archivio per verificare la presenza di malware e altre minacce per la protezione del computer.

Ignora archivi protetti

Facendo clic su questo pulsante, vengono ignorati l'oggetto e tutti gli oggetti dello stesso tipo.

Ignora

Facendo clic su questo pulsante, viene ignorato l'oggetto.

Finestra di dialogo Oggetto rilevato

Quando Kaspersky Endpoint Security rileva un virus o un'altra minaccia per la sicurezza del computer, sullo schermo verrà visualizzata una finestra di notifica.

Rilevato

Nome dell'oggetto in base alla classificazione di Virus Encyclopedia di Kaspersky.

Dettagli

Questo pulsante apre una pagina nella Virus Encyclopedia di Kaspersky con informazioni sull'oggetto rilevato.

Oggetto

Percorso della cartella contenente l'oggetto rilevato o l'indirizzo Web in cui è stato rilevato l'oggetto.

Applica a tutti

Questa casella di controllo consente di abilitare o disabilitare l'azione selezionata per tutti gli oggetti dello stesso tipo durante la sessione corrente di Protezione Minacce File, Protezione Minacce Web o un'attività di scansione anti-malware.

Questa casella è deselezionata per impostazione predefinita.

Per sessione corrente di Protezione Minacce File o Protezione Minacce Web si intende l'intervallo di tempo che intercorre tra l'avvio e l'arresto del componente o fino alla chiusura o al riavvio dell'applicazione. Per sessione corrente delle attività di scansione anti-malware si intende l'intervallo di tempo che intercorre tra l'avvio e il completamento di un'attività di scansione anti-malware.

I pulsanti con le azioni che è possibile eseguire sugli oggetti rilevati variano a seconda del tipo di oggetto rilevato.

È possibile selezionare una delle azioni seguenti:

- **Disinfetta**. L'oggetto viene disinfettato. Prima di eseguire la disinfezione, Kaspersky Endpoint Security crea una copia di backup del file nel caso sia necessario ripristinare il file originale.
- **Elimina**. L'oggetto viene eliminato. Prima di eseguire l'eliminazione, Kaspersky Endpoint Security crea una copia di backup del file nel caso sia necessario ripristinare il file originale.
- **Non bloccare**. Viene consentito l'accesso a un sito Web considerato un oggetto del traffico Web pericoloso.
- **Blocca**. Viene impedito l'accesso a un sito Web considerato un oggetto del traffico Web pericoloso.
- **Elimina archivio**. L'archivio contenente l'oggetto rilevato viene eliminato.
- **Ignora archivi protetti**. Vengono ignorati gli archivi protetti da password durante le scansioni malware.
- **Ignora**. Viene bloccato l'accesso all'oggetto, senza eseguire alcuna azione.

Finestra "Scansione"



Questo pulsante consente di tornare alla finestra precedente di Kaspersky Endpoint Security.



Questo pulsante consente di passare alla finestra successiva di Kaspersky Endpoint Security.



Questo pulsante consente di eliminare i record di tutte le attività di scansione malware nella finestra **Scansione**.

Pianifica scansione

Questo pulsante consente di aprire una finestra di dialogo in cui è possibile pianificare le attività Scansione completa o Scansione rapida.

Scansione rapida

Facendo clic sul pulsante di avvio () in questa sezione viene eseguita un'attività Scansione rapida.

Scansione completa

Facendo clic sul pulsante di avvio () in questa sezione viene eseguita un'attività Scansione completa.

Questo pulsante consente di interrompere l'attività di scansione anti-malware selezionata.

Questo pulsante è visualizzato se è in esecuzione un'attività di scansione anti-malware.

Impostazioni

Facendo clic su questo pulsante viene aperta la scheda **Scansione** in cui è possibile configurare le impostazioni delle attività di scansione.

Seleziona

Questo pulsante apre una finestra in cui è possibile scegliere un file o una cartella da esaminare.

Nella parte inferiore della sezione **File e cartelle** è possibile visualizzare i record di tutte le attività di scansione malware eseguite per i file o le cartelle selezionati.

Dettagli

Questo pulsante apre la finestra del rapporto sull'attività di scansione anti-malware.

Questo pulsante viene visualizzato quando si passa il cursore del mouse su un'attività di scansione.

Cancella la cronologia di scansione

Questo pulsante consente di eliminare tutti i record di tutte le attività di scansione malware.

Mostra tutto

Questo pulsante apre la finestra **Oggetti rilevati** in cui è possibile visualizzare tutti gli oggetti rilevati.

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Finestra Oggetti rilevati

La sezione **Oggetti rilevati** contiene gli oggetti dannosi rilevati dall'applicazione.

Disinfetta tutto

Questo pulsante avvia la disinfezione di tutti gli oggetti dannosi rilevati.

Ignora tutto

Questo pulsante consente di rimuovere tutti gli oggetti dannosi dall'elenco degli oggetti dannosi nella sezione **Oggetti rilevati**.

•••

Questo pulsante consente di aprire un menu pop-up in cui è possibile selezionare una delle seguenti azioni da eseguire con un oggetto dannoso:

- **Disinfetta**. L'oggetto viene disinfettato. Prima della disinfezione l'applicazione Kaspersky Endpoint Security crea una copia di backup del file in modo da poterlo ripristinare o disinfettare in un secondo momento senza il rischio di perdite di dati.
- **Ignora**. Consente di rimuovere l'oggetto dall'elenco degli oggetti rilevati.

La sezione **Altri oggetti** contiene gli oggetti rilevati che non sono dannosi ma che possono essere utilizzati dagli hacker per danneggiare il computer o i dati.

Elimina tutto

Questo pulsante consente di eliminare tutti gli oggetti rilevati dal computer.

Ignora tutto

Questo pulsante consente di rimuovere tutti gli oggetti rilevati dall'elenco degli oggetti rilevati nella sezione **Altri oggetti**.

•••

Questo pulsante consente di aprire un menu pop-up in cui è possibile selezionare una delle seguenti azioni da eseguire con un oggetto rilevato:

- **Elimina**. Consente di eliminare l'oggetto rilevato dal computer.
- **Ignora**. Consente di rimuovere l'oggetto dall'elenco degli oggetti rilevati.

La sezione **Backup** contiene le copie di backup degli oggetti rilevati.

Elimina tutto

Questo pulsante consente di eliminare tutte le copie di backup degli oggetti rilevati dal computer.

•••

Questo pulsante consente di aprire un menu pop-up in cui è possibile selezionare una delle seguenti azioni da eseguire con un oggetto sottoposto a backup:

- **Elimina copia sottoposta a backup**. Consente di eliminare la copia di backup dell'oggetto rilevato dal computer.
- **Ripristina file**. Consente di ripristinare la copia di backup del file selezionato nell'elenco nella posizione originale con lo stesso nome che il file originale aveva prima della disinfezione o dell'eliminazione. Se un oggetto con lo stesso nome esiste già nella posizione originale (se ad esempio Kaspersky Endpoint Security ha creato una copia del file originale prima della disinfezione o se ha disinfettato il file originale), viene visualizzato un avviso. È possibile modificare la posizione dell'oggetto da ripristinare o rinominarlo.

Finestra Licenza



Questo pulsante consente di tornare alla finestra precedente di Kaspersky Endpoint Security.



Questo pulsante consente di passare alla finestra successiva di Kaspersky Endpoint Security.

Nota: questa finestra varia a seconda del fatto che Kaspersky Endpoint Security sia attivato o meno e del tipo di licenza o abbonamento utilizzato.

La finestra può contenere le seguenti informazioni:

- Stato della licenza o dell'abbonamento
- Chiavi attive
- Chiavi di riserva (se presenti)
- Tipo di licenza e numero di computer in cui è possibile utilizzare l'applicazione con la licenza corrente o con un abbonamento
- Funzionalità dell'applicazione disponibili con la licenza o l'abbonamento correnti
- Data e ora di scadenza della licenza
- Numero di giorni rimanenti prima della scadenza della licenza

In questa finestra è possibile eseguire le seguenti azioni:

- Attivare l'applicazione immettendo un codice di attivazione.
- Accedere a un sito Web con le informazioni su come acquistare una licenza nel negozio online di Kaspersky.
- Aprire il sito Web del produttore di Kaspersky Endpoint Security con le informazioni sul rinnovo dell'abbonamento.
- Aggiornare lo stato dell'abbonamento.

Per ulteriori informazioni sulle licenze di Kaspersky Endpoint Security, contattare l'amministratore di sistema dell'organizzazione.

Finestra Ambito della protezione

Nella sezione **Ambito della protezione** è possibile visualizzare e modificare l'ambito di protezione.

Tutti i dischi rimovibili

Questa casella di controllo consente di abilitare o disabilitare la protezione in tempo reale di tutti i dischi rimovibili.

Questa casella di controllo è selezionata per impostazione predefinita.

Tutti i dischi interni

Questa casella di controllo consente di abilitare o disabilitare la protezione in tempo reale di tutti i dischi interni.

Questa casella di controllo è selezionata per impostazione predefinita.

Tutti i dischi di rete

Questa casella di controllo consente di abilitare o disabilitare la protezione in tempo reale di tutti i dischi di rete.

Questa casella di controllo è selezionata per impostazione predefinita.

+

Questo pulsante apre un elenco in cui è possibile selezionare gli elementi per la creazione dell'ambito di protezione:

- **File e cartelle**. Selezionando questa voce viene visualizzata una finestra di dialogo per aggiungere un file o una cartella all'ambito di protezione.
- **Tutti i dischi**. Selezionando questa voce, tutti i dischi rimovibili, i dischi interni e i dischi di rete del computer vengono aggiunti all'ambito di protezione.
- **Tutti i dischi rimovibili**. Selezionando questa voce, tutti i dischi rimovibili del computer vengono aggiunti all'ambito di protezione.
- **Tutti i dischi interni**. Selezionando questa voce, tutti i dischi interni del computer vengono aggiunti all'ambito di protezione.
- **Tutti i dischi di rete**. Selezionando questa voce, tutti i dischi di rete del computer vengono aggiunti all'ambito di protezione.
- **Memoria**. Selezionando questa voce, la memoria del computer viene aggiunta all'ambito della protezione.
- **Oggetti di avvio**. Selezionando questa voce, tutti i file eseguibili avviati all'avvio del sistema operativo vengono aggiunti all'ambito della protezione. La scansione degli oggetti di avvio rende possibile il rilevamento di rootkit.

La casella accanto a un elemento dell'elenco consente di abilitare o disabilitare la protezione in tempo reale degli oggetti associati all'elemento.

–

Questo pulsante consente di eliminare l'elemento selezionato dall'elenco dell'ambito di protezione.

Gli elementi inclusi nell'elenco dell'ambito di protezione per impostazione predefinita non possono essere eliminati.

Nella sezione **Ottimizzazione** è possibile specificare se Kaspersky Endpoint Security deve esaminare il volume di sistema di sola lettura.

Ignora la scansione del volume di sistema di sola lettura

Questa casella di controllo consente di disabilitare/abilitare la scansione del volume di sistema di sola lettura da parte di Kaspersky Endpoint Security.

Questa casella di controllo è selezionata per impostazione predefinita.

Importante: l'ottimizzazione potrebbe essere disabilitata per motivi di sicurezza.

Finestra Ambito della scansione

In questa finestra è possibile visualizzare e modificare l'ambito della scansione dell'attività Scansione rapida.

La casella di controllo accanto a un oggetto nell'elenco consente di abilitare o disabilitare la scansione dell'oggetto.

+

Questo pulsante apre un elenco per regolare l'ambito della scansione:

- **File e cartelle**. Selezionando questa voce viene visualizzata una finestra di dialogo per aggiungere un file o una cartella all'ambito della scansione.
- **Tutti i dischi**. Selezionando questa voce, tutti i dischi rimovibili, i dischi interni e i dischi di rete del computer vengono aggiunti all'ambito della scansione.
- **Tutti i dischi esterni**. Selezionando questa voce, tutti i dischi rimovibili del computer vengono aggiunti all'ambito della scansione.
- **Tutti i dischi interni**. Selezionando questa voce, tutti i dischi interni del computer vengono aggiunti all'ambito della scansione.
- **Tutti i dischi di rete**. Selezionando questa voce, tutti i dischi di rete del computer vengono aggiunti all'ambito della scansione.
- **Memoria**. Selezionando questa voce, la memoria del computer viene aggiunta all'ambito della scansione.
- **Oggetti di avvio**. Selezionando questa voce, tutti i file eseguibili avviati all'avvio del sistema operativo vengono aggiunti all'ambito della scansione. La scansione degli oggetti di avvio rende possibile il rilevamento di rootkit.

–

Questo pulsante consente di rimuovere l'elemento selezionato dall'elenco dell'ambito della scansione.

Gli elementi inclusi nell'elenco dell'ambito della scansione per impostazione predefinita non possono essere eliminati.

Nella sezione **Ottimizzazione** è possibile specificare se l'applicazione Kaspersky Endpoint Security deve esaminare il volume di sistema di sola lettura quando esegue un'attività di scansione.

Ignora la scansione del volume di sistema di sola lettura

Questa casella di controllo consente di disabilitare/abilitare la scansione del volume di sistema di sola lettura da parte di Kaspersky Endpoint Security.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non esamina il volume di sistema di sola lettura. Questo riduce notevolmente la durata scansione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esamina il volume di sistema di sola lettura.

Questa casella di controllo è selezionata per impostazione predefinita.

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Scheda Essenziale

Nella sezione **Generale** è possibile abilitare o disabilitare la protezione del computer da malware e altre minacce per la sicurezza.

Abilita la protezione

Questa casella di controllo consente di abilitare o disabilitare la protezione in tempo reale da malware e altre minacce per la sicurezza.

Questa casella di controllo è selezionata per impostazione predefinita.

Controlla connessioni protette (HTTPS)

Questa casella di controllo consente di abilitare o disabilitare la scansione delle connessioni crittografate (HTTPS) da parte di Kaspersky Endpoint Security e la visualizzazione delle notifiche quando Controllo Web blocca l'accesso dell'utente alle risorse Web pericolose.

Questa casella è deselezionata per impostazione predefinita.

Area attendibile

Questo pulsante consente di aprire una finestra in cui è possibile modificare l'area attendibile creando un elenco di oggetti attendibili e di cui non si desidera eseguire la scansione alla ricerca di malware.

Impostazioni

Questo pulsante consente di aprire una finestra in cui è possibile gestire l'elenco dei certificati radice attendibili e selezionare l'archivio dei certificati per il controllo del traffico HTTPS criptato nel browser Mozilla Firefox.

Nella sezione **Protezione minacce file** è possibile abilitare o disabilitare Protezione Minacce File e selezionare l'azione eseguita da Kaspersky Endpoint Security in caso di rilevamento di file infetti.

Abilita Protezione minacce file

Questa casella di controllo consente di abilitare o disabilitare Protezione minacce file.

Questa casella di controllo è selezionata per impostazione predefinita.

Ambito della protezione

Questo pulsante apre la finestra in cui è possibile creare l'ambito della protezione.

Disinfetta o elimina gli oggetti dannosi automaticamente

Kaspersky Endpoint Security blocca l'accesso al file infetto e tenta di disinfettarlo senza richiedere una conferma da parte dell'utente. Prima di eseguire la disinfezione, Kaspersky Endpoint Security salva una copia di backup del file in Backup. Se la disinfezione restituisce esito positivo, Kaspersky Endpoint Security salva il file nella posizione originale con il nome originale. Se la disinfezione fallisce, Kaspersky Endpoint Security mantiene il file infetto in uno stato bloccato nella posizione originale. Le informazioni sul rilevamento dell'oggetto infetto vengono registrate nel rapporto **Oggetti elaborati**.

Richiedi l'intervento dell'utente

Kaspersky Endpoint Security visualizza una finestra di notifica con informazioni sull'oggetto dannoso che è sospettato di aver infettato il file e richiede all'utente di scegliere l'azione che deve essere eseguita da Kaspersky Endpoint Security. Le azioni disponibili possono variare in base allo stato dell'oggetto.

Questa azione è selezionata per impostazione predefinita.

Nella sezione **Protezione minacce Web** è possibile abilitare o disabilitare Protezione Minacce Web e selezionare l'azione eseguita da Kaspersky Endpoint Security in caso di rilevamento di oggetti del traffico Web pericolosi.

Abilita Protezione minacce Web

Questa casella di controllo consente di abilitare o disabilitare Protezione minacce Web.

Questa casella di controllo è selezionata per impostazione predefinita.

Blocca automaticamente gli oggetti del traffico Web pericolosi

Kaspersky Endpoint Security blocca l'accesso ai siti Web in cui è stato rilevato un oggetto del traffico Web pericoloso senza richiedere conferma.

Richiedi l'intervento dell'utente

Kaspersky Endpoint Security visualizza una finestra di notifica con informazioni sull'oggetto del traffico Web pericoloso rilevato e richiede all'utente di scegliere l'azione che deve essere eseguita da Kaspersky Endpoint Security. Le azioni disponibili possono variare in base allo stato dell'oggetto.

Questa azione è selezionata per impostazione predefinita.

Nella sezione **Protezione minacce di posta** è possibile abilitare o disabilitare Protezione minacce di posta e selezionare l'azione eseguita da Kaspersky Endpoint Security in caso di rilevamento di oggetti dannosi.

Abilita Protezione minacce di posta

Questa casella di controllo consente di abilitare o disabilitare Protezione minacce di posta.

Questa casella di controllo è selezionata per impostazione predefinita.

Elimina oggetti dannosi automaticamente

Quando Kaspersky Endpoint Security rileva un oggetto infetto in un messaggio e-mail, elimina l'oggetto infetto e sostituisce il contenuto dell'oggetto con il testo "The requested file infected with <nome virus> has been deleted".

Blocca oggetti dannosi automaticamente

Quando Kaspersky Endpoint Security rileva un oggetto infetto in un messaggio e-mail, sostituisce l'oggetto del messaggio e-mail con "Message is infected: <oggetto originale>", dove <oggetto originale> è l'oggetto originale. L'oggetto del messaggio e-mail viene sostituito solo per il protocollo POP3.

Nella sezione **Protezione minacce di rete** è possibile abilitare o disabilitare Protezione minacce di rete.

Abilita Protezione minacce di rete

Questa casella di controllo consente di abilitare o disabilitare Protezione minacce di rete.

Questa casella di controllo è selezionata per impostazione predefinita.

Impostazioni

Questo pulsante apre una finestra in cui è possibile creare un elenco di computer attendibili o visualizzare e modificare l'elenco dei computer bloccati.



Questo pulsante impedisce agli utenti senza privilegi amministratore di modificare le impostazioni dell'applicazione Kaspersky Endpoint Security.



Con questo pulsante viene visualizzata la richiesta di immissione delle credenziali di amministratore. Dopo l'immissione delle credenziali di un amministratore, le impostazioni dell'applicazione diventano modificabili.

Scheda Applicazioni attendibili

Nella scheda **Applicazioni attendibili** è possibile creare un elenco di applicazioni che l'applicazione Kaspersky Endpoint Security non deve monitorare.

Per impostazione predefinita, l'elenco di oggetti dell'area attendibile è vuoto.

+

Quando si fa clic su questo pulsante, viene aperta una finestra in cui è possibile immettere il percorso di un'applicazione, specificare i requisiti di firma del codice e selezionare i tipi di attività che Kaspersky Endpoint Security non dovrà monitorare.

–

Questo pulsante consente di rimuovere dall'Area attendibile l'applicazione selezionata.

Modifica

Questo pulsante consente di aprire una finestra in cui è possibile modificare i parametri dell'applicazione attendibile.

Finestra Aggiungi applicazione attendibile

Percorso

Il percorso di un'applicazione la cui attività di rete o file non verrà monitorata da Kaspersky Endpoint Security.

> **Nota:** i collegamenti simbolici non possono essere utilizzati per specificare i percorsi in questo campo.

Seleziona

Questo pulsante apre una finestra in cui è possibile selezionare un'applicazione la cui attività di rete non verrà monitorata da Kaspersky Endpoint Security. In questo caso, i valori dei campi **Requisito di firma del codice** e **Percorso** vengono inseriti automaticamente.

Requisito di firma del codice

Requisiti per la firma del codice dell'applicazione la cui attività non sarà monitorata da Kaspersky Endpoint Security.

Si tratta di un parametro facoltativo.

Nella sezione **Opzioni** è possibile selezionare il tipo di attività che non si desidera venga monitorata dall'applicazione Kaspersky Endpoint Security.

Non monitorare l'attività del file

Questa casella di controllo consente di abilitare/disabilitare il monitoraggio delle operazioni sui file di un'applicazione in un computer client.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non monitora l'attività dell'applicazione sui file.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security monitora l'attività dell'applicazione sui file.

Questa casella di controllo è selezionata per impostazione predefinita.

Non monitorare l'attività di rete

Questa casella di controllo consente di abilitare/disabilitare il monitoraggio del traffico Internet in entrata e in uscita dell'applicazione in un computer client.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non monitora l'attività di rete dell'applicazione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security monitora l'attività di rete dell'applicazione.

Questa casella di controllo è selezionata per impostazione predefinita.

Annulla

Questo pulsante consente di chiudere la finestra senza salvare le modifiche.

OK

Questo pulsante consente di salvare i parametri dell'applicazione attendibile e di chiudere la finestra.

Scheda File e cartelle attendibili

Nella scheda **File e cartelle** è possibile creare un elenco di file e cartelle che l'applicazione Kaspersky Endpoint Security non deve monitorare.

Per impostazione predefinita, l'elenco di oggetti dell'area attendibile è vuoto.

+
Questo pulsante consente di aprire una finestra di dialogo per la selezione di un file o di una cartella.
–
Questo pulsante consente di rimuovere l'oggetto selezionato dall'area attendibile.

Scheda Indirizzi Web attendibili

Nella scheda **Indirizzi Web** è possibile creare un elenco di indirizzi Web che l'applicazione Kaspersky Endpoint Security non deve monitorare.

Per impostazione predefinita, l'elenco di oggetti dell'area attendibile è vuoto.

+
Questo pulsante consente di aggiungere un campo per l'immissione di un indirizzo Web.
È possibile utilizzare i seguenti simboli quando si specifica l'indirizzo del sito Web:

- Il simbolo dell'asterisco (`*`) sostituisce qualsiasi set di caratteri, tranne i caratteri `\` e `/`.
- Due asterischi consecutivi (`**`) sostituiscono qualsiasi set di caratteri (compreso un set vuoto), inclusi i caratteri `\` e `/`.
- Il punto interrogativo (`?`) sostituisce qualsiasi singolo carattere nel nome del file o della cartella, ad eccezione dei caratteri `\` e `/`.

–

Questo pulsante consente di rimuovere dall'Area attendibile l'indirizzo Web selezionato.

Finestra impostazioni Protezione minacce di posta

Ignora archivi superiori a <valore> MB

Se questa casella di controllo è selezionata, Protezione minacce di posta esclude dalla scansione gli archivi allegati ai messaggi e-mail se le loro dimensioni superano il valore specificato.

Se questa casella di controllo è deselezionata, Protezione minacce di posta esegue la scansione degli archivi degli allegati e-mail di qualsiasi dimensione.

Il valore predefinito è 8 MB.

Questa casella di controllo è selezionata per impostazione predefinita.

Limita il tempo per il controllo degli archivi a <value> sec

Se questa casella di controllo è selezionata, il tempo assegnato per la scansione degli archivi allegati ai messaggi e-mail è limitato al periodo specificato.

Se questa casella di controllo è deselezionata, il tempo allocato per la scansione degli archivi non è limitato.

Il valore predefinito è 5 secondi.

Questa casella di controllo è selezionata per impostazione predefinita.

Finestra "Impostazioni"

Nella scheda **Computer attendibili** è possibile creare un elenco di computer attendibili. L'applicazione Kaspersky Endpoint Security non blocca automaticamente gli indirizzi IP di questi computer nemmeno in seguito al rilevamento di attività di rete pericolosa.

Per impostazione predefinita, l'elenco dei computer attendibili è vuoto.

+

Questo pulsante aggiunge un campo per l'immissione dell'indirizzo IP di un computer attendibile.

–

Questo pulsante consente di eliminare dall'elenco dei computer attendibili l'indirizzo IP selezionato.

Modifica

Facendo clic su questo pulsante l'indirizzo IP selezionato diventa disponibile per la modifica.

Nella scheda **Computer bloccati** è possibile visualizzare e modificare l'elenco dei computer bloccati.

L'applicazione Kaspersky Endpoint Security blocca il computer con questo indirizzo IP per un'ora in seguito al rilevamento di attività di rete pericolosa.

Indirizzo IP

Questa colonna visualizza l'indirizzo IP del computer bloccato.

Ora dell'evento

Questa colonna visualizza la data e l'ora in cui è stata rilevata l'attività di rete pericolosa nel computer.

Sblocca

Questo pulsante consente di eliminare dall'elenco dei computer bloccati l'indirizzo IP selezionato.

Scheda Regole per i pacchetti di rete

Nome regola

Nome regola dei pacchetti di rete

Nella sezione **Azione** è possibile selezionare l'azione che Kaspersky Endpoint Security deve eseguire quando rileva l'attività di rete.

Nella sezione **Protocollo** è possibile specificare il protocollo a cui si applica la regola di rete.

Nella sezione **Direzione** è possibile specificare la direzione dell'attività di rete monitorata.

Nella sezione **TTL** è possibile specificare la durata dei pacchetti di rete monitorati.

Nella sezione **Schede di rete** è possibile specificare le schede di rete a cui si applica la regola di rete.

Nella sezione **Indirizzo remoto** è possibile specificare gli indirizzi di rete dei dispositivi remoti in grado di inviare e ricevere pacchetti di rete:

Nella sezione **Indirizzo locale** è possibile specificare gli indirizzi di rete locali dei dispositivi in grado di inviare e ricevere pacchetti di rete:

Registra eventi

Questa casella di controllo consente di abilitare o disabilitare la registrazione degli eventi Firewall.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security registra gli eventi Firewall nel rapporto.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security non registra gli eventi Firewall nel rapporto.

Questa casella è deselezionata per impostazione predefinita.

Finestra Scheda di rete

Nome della scheda

Nome della scheda di rete.

Tipo di interfaccia

Da questo elenco a discesa è possibile selezionare il tipo di interfaccia della scheda di rete.

Indirizzi IP

Elenco degli indirizzi IP

Indirizzi MAC

Elenco degli indirizzi MAC

Finestra Schede di rete

Nome

Questa colonna contiene il nome della scheda di rete.

Tipo di interfaccia

Questa colonna contiene il tipo di interfaccia della scheda di rete.

Indirizzi IP

Questa colonna contiene gli indirizzi IP della scheda di rete.

Indirizzi MAC

Questa colonna visualizza gli indirizzi MAC della scheda di rete.

Finestra Indirizzi locali

Indirizzi locali

Questa colonna contiene gli indirizzi locali.

Finestra Indirizzo locale

Tipo

Questo elenco a discesa consente di specificare il tipo di voce IP locale a cui si desidera applicare la regola di rete.

Indirizzo IP

Campo di immissione Indirizzo IP. Questo campo è disponibile solo se si seleziona **Indirizzo IP** nell'elenco a discesa **Tipo**.

Inizio intervallo

Campo di immissione di inizio intervallo di indirizzi IP. Questo campo è disponibile solo se si seleziona **Intervallo di indirizzi IP** nell'elenco a discesa **Tipo**.

Fine intervallo

Campo di immissione di fine intervallo di indirizzi IP. Questo campo è disponibile solo se si seleziona **Intervallo di indirizzi IP** nell'elenco a discesa **Tipo**.

Finestra Indirizzi remoti

Indirizzi remoti

Questa colonna contiene gli indirizzi remoti.

Finestra Indirizzo remoto

Tipo

Questo elenco a discesa consente di specificare il tipo di voce indirizzo remoto a cui si desidera applicare la regola di rete.

Indirizzo

Campo di immissione dell'indirizzo IP o del nome DNS. Questo campo è disponibile solo se si seleziona **Indirizzo IP o nome DNS** nell'elenco a discesa **Tipo**.

Inizio intervallo

Campo di immissione di inizio intervallo di indirizzi IP. Questo campo è disponibile solo se si seleziona **Intervallo di indirizzi IP** nell'elenco a discesa **Tipo**.

Fine intervallo

Campo di immissione di fine intervallo di indirizzi IP. Questo campo è disponibile solo se si seleziona **Intervallo di indirizzi IP** nell'elenco a discesa **Tipo**.

Finestra Modelli

Modelli regole di rete

Questa colonna contiene i modelli delle regole di rete.

Scheda Regole per i pacchetti di rete

Nome

Nome della regola di rete.

Azione

Azione che Firewall deve eseguire durante il rilevamento del tipo di attività di rete.

Indirizzo

Indirizzi di rete a cui viene applicata la regola di rete.

Scheda Reti disponibili

Nome

Questa colonna contiene il nome della rete.

Stato della rete

Questa colonna contiene lo stato della rete.

Indirizzo IP

Questa colonna contiene gli indirizzi IP della rete.

Finestra Rete disponibile

Nome della rete

Nome della rete.

Stato della rete

Elenco a discesa dello stato della rete.

Indirizzo IP

Indirizzo IP della rete.

Finestra Indirizzo MAC

Tipo

Questo elenco a discesa consente di specificare il tipo di voce indirizzo MAC a cui si desidera applicare la regola di rete.

Indirizzo MAC

Campo di immissione Indirizzo MAC. Questo campo è disponibile solo se si seleziona **Indirizzo MAC** nell'elenco a discesa **Tipo**.

Maschera

Campo di immissione della maschera dell'indirizzo MAC. Questo campo è disponibile solo se si seleziona **Maschera per gli indirizzi MAC** nell'elenco a discesa **Tipo** elenco a discesa.

Inizio intervallo

Campo di immissione di inizio intervallo di indirizzi MAC. Questo campo è disponibile solo se si seleziona **Intervallo di indirizzi MAC** nell'elenco a discesa **Tipo**.

Fine intervallo

Campo di immissione di fine intervallo di indirizzi MAC. Questo campo è disponibile solo se si seleziona **Intervallo di indirizzi MAC** nell'elenco a discesa **Tipo**.

Scheda Avanzate

Nella sezione **KSN** è possibile leggere le condizioni dell'Informativa su Kaspersky Security Network e accettare o rifiutare la partecipazione a Kaspersky Security Network.

Mostra Informativa KSN

Facendo clic su questo pulsante verrà visualizzata una finestra con il testo dell'Informativa di Kaspersky Security Network.

Kaspersky Endpoint Security può utilizzare l'infrastruttura KSN Globale o KSN Privato. Se si partecipa a Kaspersky Security Network, Kaspersky Endpoint Security utilizza le informazioni sulla reputazione di file, risorse Web e applicazioni ricevute da Kaspersky Security Network e fornisce i dati necessari per il funzionamento dei servizi di rilevamento a Kaspersky Security Network.

Partecipa a Kaspersky Security Network

Questa casella di controllo consente di abilitare o disabilitare la partecipazione a Kaspersky Security Network.

Partecipa a Kaspersky Private Security Network

Questa casella di controllo consente di abilitare o disabilitare la partecipazione a Kaspersky Private Security Network. Per ulteriori informazioni sulla partecipazione a Kaspersky Private Security Network, contattare l'amministrazione di sistema dell'organizzazione.

Abilita modalità KSN estesa

Questa casella di controllo consente di abilitare/disabilitare il provisioning di dati aggiuntivi a Kaspersky Security Network. Questi dati vengono utilizzati per migliorare la protezione del computer e l'usabilità di Kaspersky Endpoint Security. L'elenco dei dati è disponibile nell'Informativa su Kaspersky Security Network e nella Guida di Kaspersky Endpoint Security.

Questa casella di controllo viene selezionata automaticamente se la casella di controllo **Partecipa a Kaspersky Security Network** è selezionata, ma è possibile deselezionarla.

Abilita modalità cloud

La modalità cloud fa riferimento alla modalità operativa dell'applicazione in cui Kaspersky Endpoint Security utilizza una versione light dei database anti-malware. Questa modalità è disponibile solo se la partecipazione a Kaspersky Security Network è abilitata. La versione light dei database anti-malware consente di utilizzare circa la metà della RAM del computer che verrebbe usata con i database completi. Se non si partecipa a Kaspersky Security Network o se la modalità cloud è disabilitata, Kaspersky Endpoint Security scarica la versione completa dei database anti-malware dai server Kaspersky.

Se l'interruttore è attivato, Kaspersky Endpoint Security utilizza la versione light dei database anti-malware, che riduce il carico sul sistema operativo.

Nota: dopo che la casella di controllo è stata selezionata, Kaspersky Endpoint Security scarica la versione light dei database anti-malware durante l'aggiornamento successivo.

Se l'interruttore è disattivato, Kaspersky Endpoint Security utilizza la versione completa dei database anti-malware.

Nota: dopo che la casella di controllo è stata deselezionata, Kaspersky Endpoint Security scarica la versione completa dei database anti-malware durante l'aggiornamento successivo.

Nella sezione **Rilevamento del comportamento** è possibile abilitare/disabilitare il componente Rilevamento del Comportamento e selezionare un'azione da eseguire quando viene rilevata un'attività malware.

Abilita Rilevamento del comportamento

Questa casella di controllo consente di abilitare/disabilitare il componente Rilevamento del Comportamento, che riceve informazioni sulle azioni delle applicazioni nel computer e le fornisce ad altri componenti della protezione per migliorarne le prestazioni.

Blocca l'attività malware

Se questa opzione è selezionata, Kaspersky Endpoint Security chiude un'applicazione quando viene rilevata attività dannosa.

Elimina l'oggetto pericoloso rilevato

Se questa opzione è selezionata, Kaspersky Endpoint Security elimina il file eseguibile di un'applicazione dannosa e crea una copia di backup del file in Backup quando viene rilevata un'attività dannosa.

Richiedi l'intervento dell'utente

Se questa opzione è selezionata, quando viene rilevata attività malware, l'applicazione Kaspersky Endpoint Security visualizza una finestra di notifica con le informazioni sull'oggetto dannoso e richiede all'utente di scegliere l'azione che l'applicazione Kaspersky Endpoint Security deve intraprendere. Le azioni disponibili possono variare in base allo stato dell'oggetto.



Questo pulsante impedisce agli utenti senza privilegi amministratore di modificare le impostazioni dell'applicazione Kaspersky Endpoint Security.



Con questo pulsante viene visualizzata la richiesta di immissione delle credenziali di amministratore. Dopo l'immissione delle credenziali di un amministratore, le impostazioni dell'applicazione diventano modificabili.

Scheda Scansione

Elenco delle attività di scansione anti-malware

Contiene le attività di scansione anti-malware preimpostate:

- **Scansione completa**. Scansione anti-malware della memoria del computer, degli oggetti di avvio e di tutti i dischi interni del computer.
- **Scansione rapida**. Scansione anti-malware delle sole aree critiche del computer: memoria, oggetti di avvio e cartelle di sistema.
- **Scansione personalizzata**. Scansione anti-malware di un oggetto specificato (file, cartella, disco interno o rimovibile).
- **Scansione dischi esterni**. Scansione malware dei dischi esterni eseguita quando un disco esterno viene connesso al computer.

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Nella sezione **Ambito della scansione** è possibile visualizzare e modificare l'ambito della scansione per l'attività Scansione rapida.

Modifica

Questo pulsante apre una finestra in cui è possibile visualizzare e modificare l'ambito della scansione.

Questo pulsante viene visualizzato solo quando l'attività Scansione rapida è selezionata nell'elenco.

Nella sezione **Azione** è possibile selezionare l'azione che Kaspersky Endpoint Security deve eseguire se viene rilevato un file infetto e pianificare una scansione.

Disinfetta o elimina gli oggetti dannosi automaticamente

Kaspersky Endpoint Security blocca l'accesso al file infetto e tenta di disinfettarlo senza richiedere una conferma da parte dell'utente. Prima di eseguire la disinfezione, Kaspersky Endpoint Security salva una copia di backup del file in Backup. Se la disinfezione restituisce esito positivo, Kaspersky Endpoint Security salva il file nella posizione originale con il nome originale. Se la disinfezione fallisce, Kaspersky Endpoint Security mantiene il file infetto in uno stato bloccato nella posizione originale. Le informazioni sul rilevamento dell'oggetto infetto vengono registrate nel rapporto Oggetti elaborati.

Richiedi l'intervento dell'utente al termine della scansione

Kaspersky Endpoint Security rimanda l'elaborazione di file infetti rilevati fino al completamento della scansione. Al termine della scansione, Kaspersky Endpoint Security visualizza finestre di notifica con informazioni su ciascun oggetto infetto rilevato e permette di selezionare ulteriori azioni. Le azioni disponibili possono variare in base allo stato dell'oggetto.

Questa azione è selezionata per impostazione predefinita.

Nella sezione **Quando si connette un disco esterno** della scheda **Scansione dischi esterni**, è possibile selezionare l'azione che Kaspersky Endpoint Security deve eseguire quando viene connesso un disco esterno al computer.

Scansione

Se questa opzione è selezionata, Kaspersky Endpoint Security avvia un'attività di scansione malware per il disco esterno connesso.

Questa opzione è selezionata per impostazione predefinita.

Non eseguire alcuna operazione

Se questa opzione è selezionata, Kaspersky Endpoint Security non esegue la scansione del disco esterno connesso.

Nella sezione **Ottimizzazione** è possibile specificare se Kaspersky Endpoint Security deve esaminare il volume di sistema di sola lettura quando esegue un'attività di Scansione rapida o Scansione completa.

Ignora la scansione del volume di sistema di sola lettura

Questa casella di controllo consente di disabilitare/abilitare la scansione del volume di sistema di sola lettura da parte di Kaspersky Endpoint Security.

Questa casella di controllo è selezionata per impostazione predefinita per un'attività di Scansione rapida e deselezionata per impostazione predefinita per un'attività di Scansione completa.

Importante: l'ottimizzazione potrebbe essere disabilitata per motivi di sicurezza.

Utilizzo della CPU

Questo pulsante consente di aprire una finestra di dialogo in cui è possibile abilitare o disabilitare la limitazione dell'uso da parte dell'applicazione della CPU del dispositivo protetto per le attività di scansione. Se l'opzione **Limita l'utilizzo della CPU per le scansioni a** è selezionata, è possibile specificare l'utilizzo massimo consentito della CPU nel campo corrispondente.

Nota: questo è un limite cumulativo per tutti i core della CPU. L'utilizzo della CPU mostrato in Activity Monitor corrisponde alla somma dell'utilizzo di ciascun core della CPU e pertanto può superare il 100%.

L'abilitazione di questa opzione può influire negativamente sulle prestazioni di Kaspersky Endpoint Security.

Per impostazione predefinita, questa opzione è disabilitata.

Pianifica

Questo pulsante consente di aprire una finestra di dialogo in cui è possibile pianificare le attività Scansione completa o Scansione rapida.



Questo pulsante impedisce agli utenti senza privilegi amministratore di modificare le impostazioni dell'applicazione Kaspersky Endpoint Security.



Con questo pulsante viene visualizzata la richiesta di immissione delle credenziali di amministratore. Dopo l'immissione delle credenziali di un amministratore, le impostazioni dell'applicazione diventano modificabili.

Scheda Minacce

Nella sezione **Oggetti da rilevare** è possibile configurare l'elenco di oggetti da rilevare.

Virus, worm, Trojan, strumenti dannosi, adware e auto-dialer

Questa categoria include i seguenti tipi di programmi:

- Tutti i tipi di malware.
- Applicazioni che visualizzano pubblicità (ad esempio banner) nel computer o sostituiscono i risultati di ricerca nel browser Web con siti Web pubblicitari.
- Applicazioni che stabiliscono connessioni telefoniche nascoste tramite un modem del computer.

Kaspersky Endpoint Security controlla sempre questo tipo di programmi.

La casella è sempre selezionata e non può essere deselezionata.

Software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali dell'utente

Questa casella di controllo consente di abilitare o disabilitare il controllo delle applicazioni legittime potenzialmente utilizzabili da utenti malintenzionati per danneggiare i dati o il computer dell'utente, come ad esempio le applicazioni di amministrazione remota.

Questa casella è deselezionata per impostazione predefinita.

Nella sezione **Backup** è possibile specificare il periodo di archiviazione degli oggetti in Backup.

Elimina oggetti sottoposti a backup dopo <value> giorni

Questa casella di controllo consente di abilitare o disabilitare la rimozione degli oggetti da Backup dopo il periodo specificato.

Se la casella di controllo è selezionata, l'applicazione elimina gli oggetti da Backup dopo il periodo di tempo specificato nel campo del numero accanto alla casella di controllo. Se la casella di controllo è deselezionata, gli oggetti vengono archiviati in Backup per un tempo indeterminato.

Questa casella di controllo è selezionata per impostazione predefinita e gli oggetti rimangono archiviati in Backup per 30 giorni.

Nella sezione **Esclusioni** è possibile creare un elenco di file, cartelle, applicazioni e siti Web considerati attendibili e che non si desidera sottoporre a scansione per la ricerca di malware.

Area attendibile

Questo pulsante consente di aprire una finestra in cui è possibile modificare l'area attendibile creando un elenco di oggetti attendibili e di cui non si desidera eseguire la scansione alla ricerca di malware.

Nota: Quando un amministratore configura il criterio per proibire la modifica dell'Area attendibile, gli utenti non possono accedere alle impostazioni dell'Area attendibile.



Questo pulsante impedisce agli utenti senza privilegi amministratore di modificare le impostazioni dell'applicazione Kaspersky Endpoint Security.



Con questo pulsante viene visualizzata la richiesta di immissione delle credenziali di amministratore. Dopo l'immissione delle credenziali di un amministratore, le impostazioni dell'applicazione diventano modificabili.

Scheda Aggiornamento

Nella sezione **Database** è possibile configurare la modalità di aggiornamento dei database di Kaspersky Endpoint Security.

Scarica gli aggiornamenti automaticamente

Questa casella di controllo consente di abilitare o disabilitare gli aggiornamenti automatici dei database dell'applicazione.

Questa casella di controllo è selezionata per impostazione predefinita.

Nella sezione **Proxy** è possibile configurare l'utilizzo di un server proxy per l'aggiornamento di Kaspersky Endpoint Security.

Usa server proxy

Questa casella di controllo consente di abilitare o disabilitare l'utilizzo di un server proxy per la connessione a Internet durante l'aggiornamento dei database anti-malware e dei moduli dell'applicazione.

Questa casella di controllo è selezionata per impostazione predefinita.

Impostazioni

Questo pulsante apre una finestra in cui è possibile configurare le impostazioni di connessione al server proxy.

Nella sezione **Rollback** è possibile eseguire il rollback alla versione precedente dei database dell'applicazione. Potrebbe essere necessario eseguire il rollback degli aggiornamenti quando la nuova versione dei database dell'applicazione contiene una firma errata e Kaspersky Endpoint Security blocca un'applicazione sicura.

Rollback aggiornamento

Questo pulsante esegue il rollback dei database dell'applicazione.



Questo pulsante impedisce agli utenti senza privilegi amministratore di modificare le impostazioni dell'applicazione Kaspersky Endpoint Security.



Con questo pulsante viene visualizzata la richiesta di immissione delle credenziali di amministratore. Dopo l'immissione delle credenziali di un amministratore, le impostazioni dell'applicazione diventano modificabili.

Finestra Impostazioni del server proxy

Usa le impostazioni di sistema per il server proxy

Kaspersky Endpoint Security utilizza le impostazioni del server proxy specificate nelle impostazioni di sistema del Mac.

Questa azione è selezionata per impostazione predefinita.

Usa le impostazioni specificate per il server proxy

Kaspersky Endpoint Security utilizza le impostazioni del server proxy specificate in questa finestra.

Indirizzo

Campo per immettere l'indirizzo IP o il nome di dominio di un server proxy.

Il campo è disponibile se l'opzione **Usa le impostazioni specificate per il server proxy** è selezionata.

Porta

Campo di immissione per il numero della porta del server proxy utilizzata per aggiornare Kaspersky Endpoint Security.

Il campo è disponibile se l'opzione **Usa le impostazioni specificate per il server proxy** è selezionata.

Il valore predefinito è 80.

Usa autenticazione

L'*autenticazione* è il processo di verifica del nome utente e della password al momento della connessione a un server proxy.

Questa casella di controllo consente di abilitare o disabilitare l'autenticazione durante la connessione a un server proxy.

Questa casella è deselezionata per impostazione predefinita.

Nome utente

Campo di immissione del nome utente per l'autenticazione durante la connessione al server proxy.

Il campo è disponibile se la casella **Usa autenticazione** è selezionata.

Password

Campo di immissione della password per l'autenticazione durante la connessione al server proxy.

Il campo è disponibile se la casella **Usa autenticazione** è selezionata.

Se il nome utente e la password non sono stati specificati oppure se il nome utente e la password specificati non vengono accettati dal server proxy, viene visualizzata una finestra in cui è necessario immettere il nome utente e la password per l'autenticazione nel server proxy. Se l'autenticazione va a buon fine e la casella **Memorizza la password** è selezionata nella finestra di richiesta, il nome utente e la password specificati saranno usati anche in seguito. Se la casella di controllo **Memorizza la password** nella finestra di immissione di nome utente e password è deselezionata, verrà richiesto di inserire nuovamente nome utente e password alla prossima connessione al server proxy.

Ignora il server proxy per gli indirizzi locali

Questa casella di controllo consente di abilitare o disabilitare l'utilizzo di un server proxy durante l'aggiornamento dell'applicazione da una cartella locale o di rete.

Questa casella di controllo è selezionata per impostazione predefinita.

Finestra di dialogo Autenticazione server proxy richiesta

Nome utente

Campo di immissione del nome utente per la connessione al server proxy.

Password

Campo di immissione della password.

Memorizza la password

Questa casella di controllo consente di abilitare o disabilitare la memorizzazione della password e del nome utente specificati per l'autenticazione sul server proxy.

Questa casella è deselezionata per impostazione predefinita.

Scheda Interfaccia

Nella sezione **Notifiche** è possibile configurare le notifiche che Kaspersky Endpoint Security mostra per informare dei diversi eventi.

Abilita notifiche per eventi

Questa casella di controllo consente di abilitare o disabilitare le notifiche relative agli eventi delle applicazioni.

Questa casella di controllo è selezionata per impostazione predefinita.

Attiva le notifiche acustiche al rilevamento del malware

Questa casella di controllo consente di abilitare o disabilitare le notifiche acustiche quando Kaspersky Endpoint Security rileva un oggetto dannoso.

Questa casella di controllo è selezionata per impostazione predefinita.

Nella sezione **Icona dell'applicazione** è possibile configurare la visualizzazione dell'icona dell'applicazione nella barra dei menu.

Mostra nella barra dei menu

Questa casella di controllo consente di abilitare o disabilitare la visualizzazione dell'icona dell'applicazione nella barra dei menu.

Nella sezione **Rapporti** è possibile abilitare o disabilitare la registrazione degli eventi non critici nei rapporti di Kaspersky Endpoint Security.

Registra eventi non critici

Questa casella di controllo consente di abilitare o disabilitare la registrazione di eventi informativi nei rapporti. Di solito questi eventi non sono importanti per la sicurezza del computer.

Nella sezione **Tracce** è possibile abilitare o disabilitare il tracciamento.

Il tracciamento è un modo per registrare informazioni dettagliate sulle attività dell'applicazione. Gli esperti dell'Assistenza tecnica di Kaspersky usano i file di traccia per la risoluzione dei problemi. È possibile abilitare la registrazione degli eventi dell'applicazione per creare i file di traccia e inviarli all'Assistenza tecnica se richiesto. Per impostazione predefinita, la registrazione degli eventi dell'applicazione è disabilitata.

Importante: attivare il tracciamento solo quando richiesto da un esperto dell'Assistenza tecnica.

Abilita tracce

Questa casella di controllo consente di abilitare o disabilitare la creazione dei file di traccia.

Questa casella è deselezionata per impostazione predefinita.

Nella sezione **Protezione tramite password** è possibile abilitare la protezione tramite password delle azioni indesiderate nel computer.

Abilita protezione tramite password

Questa casella di controllo consente di abilitare/disabilitare la protezione tramite password per le azioni indesiderate.

Questa casella è deselezionata per impostazione predefinita.

Selezionando questa casella di controllo viene aperta una finestra in cui è possibile impostare e configurare la password amministratore.

Impostazioni

Questo pulsante consente di aprire una finestra in cui è possibile modificare i parametri di una password amministratore.



Questo pulsante impedisce agli utenti senza privilegi amministratore di modificare le impostazioni dell'applicazione Kaspersky Endpoint Security.



Con questo pulsante viene visualizzata la richiesta di immissione delle credenziali di amministratore. Dopo l'immissione delle credenziali di un amministratore, le impostazioni dell'applicazione diventano modificabili.

Finestra Imposta password amministratore

Password

Campo per l'immissione di una password per limitare le azioni indesiderate sul dispositivo.

Conferma password

Campo per la conferma di una password inserendola una seconda volta.

Opzioni

L'elenco delle azioni che possono essere protette dalla password. Selezionare le caselle di controllo richieste per proteggere le azioni corrispondenti nel dispositivo. È necessario selezionare almeno una casella di controllo.

Annulla

Questo pulsante consente di chiudere la finestra senza salvare le modifiche.

OK

Questo pulsante consente di salvare le impostazioni della password dell'amministratore e di chiudere la finestra. Dopo aver salvato le modifiche, viene richiesto di immettere la password quando si tenta di eseguire un'azione indesiderata sul dispositivo.

Rapporto Eventi di sistema

Il riquadro destro della finestra contiene un rapporto sul funzionamento di Kaspersky Endpoint Security.

Data/Ora

Questa colonna visualizza la data e l'ora dell'evento.

Evento

Questa colonna visualizza lo stato dell'evento.

Nome programma

Questa colonna consente di visualizzare il nome del programma in cui si è verificato l'evento.

Utente

Questa colonna visualizza il nome dell'utente che ha avviato l'evento.

Tipo di utente

Questa colonna consente di visualizzare il tipo di utente che ha avviato l'evento.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Oggetti elaborati

Nel riquadro destro della finestra viene visualizzato un elenco di tutti gli oggetti infetti e degli oggetti del traffico Web pericolosi rilevati dall'applicazione Kaspersky Endpoint Security.

Data/Ora

Questa colonna consente di visualizzare l'ora in cui è stato rilevato l'oggetto.

Oggetto

Questa colonna consente di visualizzare il percorso della posizione in cui è stato rilevato l'oggetto o l'indirizzo Web dell'oggetto.

Stato

Questa colonna consente di visualizzare l'azione eseguita dall'applicazione dopo il rilevamento dell'oggetto.

Rilevato

Questa colonna consente di visualizzare il tipo di oggetto rilevato in base alla classificazione della Virus Encyclopedia di Kaspersky.

Nome

Questa colonna consente di visualizzare il nome dell'oggetto rilevato in base alla classificazione dell'Enciclopedia dei virus di Kaspersky.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Aggiornamento database

Il riquadro destro della finestra contiene i rapporti relativi alle attività di aggiornamento eseguite dall'applicazione.

Data avvio

Questa colonna visualizza la data e l'ora di inizio di ogni attività di aggiornamento. Se l'elenco delle operazioni è espanso, questa colonna elenca anche le operazioni eseguite durante l'aggiornamento dell'applicazione e l'ora in cui sono state eseguite.

Stato

Questa colonna visualizza lo stato di un'attività di aggiornamento.

Dimensioni

Questa colonna visualizza le dimensioni dei file di aggiornamento scaricati.

Velocità media

Questa colonna visualizza la velocità di download del file di aggiornamento.

Ora di fine

Questa colonna visualizza l'ora di completamento di un aggiornamento.

Questo pulsante consente di espandere l'elenco di operazioni incluse nell'attività di aggiornamento.

Questo pulsante consente di comprimere l'elenco di operazioni incluse nell'attività di aggiornamento.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Scansione

Il riquadro destro della finestra contiene i rapporti relativi alle attività di scansione eseguite da Kaspersky Endpoint Security.

Attività

Questa colonna visualizza il nome di un'attività di scansione.

Stato

Questa colonna visualizza lo stato di un'attività di scansione o lo stato degli oggetti esaminati.

Data

Questa colonna visualizza la data e l'ora di un'attività di scansione.

Iniziatore

Questa colonna visualizza l'utente, l'applicazione o il processo che ha avviato un'attività di scansione.

Facendo clic su questo pulsante si espande l'elenco degli oggetti esaminati.

Facendo clic su questo pulsante si comprime l'elenco degli oggetti esaminati.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Protezione Minacce File

Il riquadro destro della finestra contiene un rapporto sull'esecuzione di Protezione Minacce File.

Data

Questa colonna visualizza la data e l'ora in cui l'applicazione ha eseguito l'accesso a un oggetto esaminato.

Percorso

Questa colonna visualizza il percorso della posizione originale di un oggetto esaminato.

Stato

Questa colonna visualizza lo stato di un oggetto esaminato.

Nome programma

Questa colonna visualizza l'applicazione che ha eseguito l'accesso a un oggetto esaminato.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Protezione Minacce Web

Il riquadro destro della finestra contiene un rapporto sull'esecuzione di Protezione Minacce Web.

Data

Questa colonna visualizza la data e l'ora in cui sono stati rilevati gli oggetti del traffico Web.

URL

Questa colonna visualizza gli oggetti del traffico Web rilevati da Protezione Minacce Web. Per ciascun oggetto del traffico Web rilevato, la colonna specifica l'indirizzo Web in cui è stato rilevato.

Stato

Questa colonna visualizza lo stato degli oggetti del traffico Web rilevati.

Nome programma

Questa colonna visualizza il programma che ha eseguito l'accesso agli oggetti del traffico Web rilevati.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Protezione minacce di posta

Il riquadro destro della finestra contiene un rapporto sull'esecuzione di Protezione minacce di posta.

Data

Questa colonna visualizza la data e l'ora in cui è stato rilevato un oggetto infetto in un messaggio e-mail.

Percorso

Questa colonna visualizza le informazioni sul messaggio e-mail in cui è stato rilevato l'oggetto infetto.

Stato

Questa colonna visualizza l'azione eseguita da Kaspersky Endpoint Security in seguito al rilevamento di un oggetto infetto.

Nome programma

Questa colonna visualizza il nome del client e-mail.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Protezione Minacce di Rete

Il riquadro destro della finestra contiene un rapporto sull'esecuzione di Protezione Minacce di Rete.

Data

Questa colonna visualizza la data e l'ora in cui è stata rilevata l'attività di rete pericolosa nel computer.

Indirizzo IP

Questa colonna visualizza l'indirizzo IP del computer da cui Kaspersky Endpoint Security ha rilevato attività di rete pericolosa.

Stato

Questa colonna visualizza l'azione eseguita da Kaspersky Endpoint Security in seguito al rilevamento di attività di rete pericolosa.

Tipo di attacco

Questa colonna visualizza il tipo di attacco di rete rilevato.

Porta locale

Questa colonna visualizza il numero della porta locale tramite la quale è stato effettuato un tentativo di intrusione.

Protocollo

Questa colonna visualizza il tipo di protocollo utilizzato per eseguire l'attacco.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Endpoint Detection and Response

Il riquadro destro della finestra contiene un rapporto sul funzionamento del componente Endpoint Detection and Response.

Data

Questa colonna visualizza la data e l'ora degli eventi.

Evento

Questa colonna visualizza lo stato degli eventi.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Firewall

Il riquadro destro della finestra contiene un rapporto sull'esecuzione del Firewall.

Data

Questa colonna visualizza la data e l'ora degli eventi.

Evento

Questa colonna visualizza lo stato degli eventi.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Prevenzione Exploit

Il riquadro destro della finestra contiene un rapporto sull'esecuzione di Prevenzione Exploit.

Data

Questa colonna visualizza la data e l'ora degli eventi.

Evento

Questa colonna visualizza lo stato degli eventi.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Controllo dispositivi

Il riquadro destro della finestra contiene un rapporto sull'esecuzione di Controllo dispositivi.

Data

Questa colonna visualizza la data e l'ora degli eventi.

Evento

Questa colonna visualizza lo stato degli eventi.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Rapporto Controllo sistema

Il riquadro destro della finestra contiene un rapporto sul funzionamento del componente Controllo sistema.

Data

Questa colonna visualizza la data e l'ora degli eventi.

Evento

Questa colonna visualizza lo stato degli eventi.



Questo pulsante consente di aprire una finestra da cui è possibile salvare il rapporto come file TXT.

Finestra Tipo di installazione

Nella sezione **Pacchetti da installare** è possibile selezionare i componenti dell'applicazione che verranno installati in un computer client.

Scansione

Questa casella di controllo consente di aggiungere il componente Scansione al pacchetto di installazione di Kaspersky Endpoint Security.

La casella di controllo è selezionata per impostazione predefinita e non può essere deselezionata.

Protezione minacce file

Questa casella di controllo consente di abilitare o disabilitare l'aggiunta del componente Protezione Minacce File al pacchetto di installazione di Kaspersky Endpoint Security.

Se la casella di controllo è selezionata, il componente Protezione Minacce File viene incluso nel pacchetto di installazione di Kaspersky Endpoint Security.

Se la casella di controllo è deselezionata, il componente Protezione Minacce File non viene incluso nel pacchetto di installazione di Kaspersky Endpoint Security.

Questa casella di controllo è selezionata per impostazione predefinita.

Protezione minacce Web

Questa casella di controllo consente di abilitare o disabilitare l'aggiunta del componente Protezione Minacce Web al pacchetto di installazione di Kaspersky Endpoint Security.

Se la casella di controllo è selezionata, il componente Protezione Minacce Web viene incluso nel pacchetto di installazione di Kaspersky Endpoint Security.

Se la casella di controllo è deselezionata, il componente Protezione Minacce Web non viene incluso nel pacchetto di installazione di Kaspersky Endpoint Security.

Questa casella di controllo è selezionata per impostazione predefinita.

Protezione minacce di rete

Questa casella di controllo consente di abilitare o disabilitare l'aggiunta del componente Protezione Minacce di Rete al pacchetto di installazione di Kaspersky Endpoint Security.

Se la casella di controllo è selezionata, il componente Protezione Minacce di Rete viene incluso nel pacchetto di installazione di Kaspersky Endpoint Security.

Se la casella di controllo è deselezionata, il componente Protezione Minacce di Rete non viene incluso nel pacchetto di installazione di Kaspersky Endpoint Security.

Questa casella di controllo è selezionata per impostazione predefinita.

Connettore per Network Agent

Questa casella di controllo consente di aggiungere il componente Connettore per Network Agent al pacchetto di installazione di Kaspersky Endpoint Security.

La casella di controllo è selezionata per impostazione predefinita e non può essere deselezionata.

Finestra Impostazioni di protezione tramite password

Password

Campo per l'immissione di una password per limitare le azioni indesiderate sui dispositivi degli utenti.

Fare clic su **Mostra** per visualizzare i simboli immessi.

Confermare la password

Campo per la conferma di una password inserendola una seconda volta.

Fare clic su **Mostra** per visualizzare i simboli immessi.

Richiedi password per le seguenti operazioni

L'elenco delle azioni che possono essere protette dalla password. Selezionare le caselle di controllo richieste per proteggere le azioni corrispondenti nel dispositivo dell'utente.

Finestra di dialogo "Concedi accesso"

Ottieni chiave di ripristino

Questo pulsante consente di generare una chiave di ripristino richiesta per accedere a un disco criptato in un computer client.

Sezione Protezione minacce avanzata

Nella sezione **Impostazioni KSN** è possibile configurare l'utilizzo di Kaspersky Security Network.

Kaspersky Security Network

L'interruttore **Kaspersky Security Network** consente di abilitare/disabilitare la partecipazione a Kaspersky Security Network.

Se l'interruttore **Kaspersky Security Network** è attivato, i computer client ai quali è applicato il criterio partecipano a Kaspersky Security Network.

Se l'interruttore **Kaspersky Security Network** è disattivato, i computer client ai quali è applicato il criterio non partecipano a Kaspersky Security Network.

Questo interruttore è disattivato per impostazione predefinita.

Modalità KSN estesa

L'interruttore **Modalità KSN estesa** consente di abilitare/disabilitare l'invio di dati aggiuntivi dal computer remoto a Kaspersky. Questi dati vengono utilizzati per migliorare la protezione dei computer client e l'usabilità di Kaspersky Endpoint Security.

Se **Modalità KSN estesa** è attivato, i computer client a cui si applica il criterio forniscono a Kaspersky Security Network sia i dati necessari per il funzionamento dei servizi di rilevamento che dati aggiuntivi.

Se **Modalità KSN estesa** è disattivato, i computer client a cui si applica il criterio forniscono solo i dati necessari per il funzionamento dei servizi di rilevamento. Non vengono forniti dati aggiuntivi a Kaspersky Security Network.

L'interruttore **Modalità KSN estesa** è disattivato per impostazione predefinita.

L'interruttore è attivato automaticamente se si attiva l'interruttore **Kaspersky Security Network**, ma è possibile disattivarlo.

Dati forniti a Kaspersky durante l'utilizzo di Kaspersky Security Network nell'infrastruttura KSN globale

Se l'interruttore **Kaspersky Security Network** è abilitato e l'interruttore **Modalità KSN estesa** è disabilitato, Kaspersky Endpoint Security in esecuzione nei computer client fornisce a Kaspersky i seguenti dati:

- Informazioni sulla licenza utilizzata: tipo di licenza e relativo periodo di validità, numero di giorni restanti prima della scadenza della licenza, identificatore del partner dal quale la licenza è stata acquistata, identificatore del Centro regionale di attivazione, checksum del codice di attivazione, hash del corpo del ticket calcolato tramite l'algoritmo SHA1, data e ora di creazione del ticket di licenza, identificatore dei dati della licenza, identificatore del ticket della licenza, identificatore di sequenza del ticket della licenza, identificatore univoco del computer dell'utente, data di inizio validità del ticket della licenza, data di fine validità del ticket della licenza, stato corrente del ticket della licenza, versione intestazione ticket, versione della licenza, identificatore certificato di firma intestazione ticket, checksum del file chiave, numero di serie firmatario intestazione ticket, token di autenticazione.

- Versione completa del Software installato;
  tipo di software installato;
  ID aggiornamento Software; ID del servizio di reputazione; ID del tipo di protocollo; ID di un centro di attivazione regionale; versione dell'elenco delle decisioni del servizio Software revocato; ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record dei database anti-virus del Software attivati; ID univoco dell'istanza di installazione dell'applicazione nel computer; data di attivazione della licenza; data di scadenza della licenza; identificatore della licenza; stato della licenza utilizzata dal software; tipo di checksum per l'oggetto elaborato; nome del malware rilevato o del software legittimo che può essere utilizzato per danneggiare i dati o il dispositivo dell'utente; checksum dell'oggetto elaborato; checksum del codice di attivazione del Software; versione completa del software; ID dispositivo univoco; ID Software; checksum del file chiave del Software; ID del modello di informazioni utilizzato per fornire la licenza Software; identificatore del certificato utilizzato per accedere all'intestazione del ticket della licenza

Software; data e ora di creazione del ticket di licenza Software; checksum del ticket di licenza Software; versione del ticket di licenza Software; versione del codice di attivazione del Software; formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; ID ticket licenza corrente; ID componente Software; risultato dell'azione del Software; codice errore; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); numero di porta; indirizzo Web dell'origine della richiesta del servizio Web (Referrer); chiave pubblica del certificato; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash.

Se gli interruttori **Kaspersky Security Network** e **Modalità KSN estesa** sono abilitati, Kaspersky Endpoint Security in esecuzione nei computer client fornisce a Kaspersky i seguenti dati:

- informazioni sulla versione del sistema operativo (OS) e dei service pack installati sul computer, sulla versione e sui checksum (MD5, SHA2-256, SHA1) del file kernel del sistema operativo e sui parametri della modalità di esecuzione del sistema operativo; versione del sistema operativo, numero build del sistema operativo, numero di aggiornamento del sistema operativo, edizione del sistema operativo, informazioni estese sull'edizione del sistema operativo; versione Service Pack del sistema operativo; data e ora di avvio del sistema operativo; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di analisi comportamentale; numero di eventi azione del sistema operativo del tipo corrente ritardati; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di difesa proattiva; numero di eventi azione del sistema operativo elaborati; numero di eventi azione del sistema operativo sincroni elaborati; ritardo totale di tutti gli eventi azione del sistema operativo del tipo corrente; ritardo di elaborazione dell'evento sull'azione del sistema operativo nel sottosistema di archiviazione degli eventi persistenti; ritardo totale di tutti gli eventi azione del sistema operativo; numero di eventi azione del sistema operativo sincroni in attesa; data e ora dell'evento ricevuto di un'azione nel sistema operativo.

- Informazioni sull'ultimo riavvio non riuscito del sistema operativo: numero di riavvii non riusciti.

- Informazioni sull'applicazione installata dal Titolare dei diritti e sullo stato della protezione anti-virus: ID installazione Software (PCID); versione del record del database del Software; identificativo univoco dell'istanza di installazione dell'applicazione sul computer, tipo di applicazione, ID del tipo di applicazione, versione completa dell'applicazione installata, identificativo della versione delle impostazioni dell'applicazione, identificativo del tipo di computer, identificativo univoco del computer su cui è installata l'applicazione, identificativo univoco dell'Utente nei servizi del Titolare dei diritti, lingua locale e stato operativo, versione dei componenti del Software installato e relativo stato operativo, versione del protocollo utilizzato per connettersi ai servizi del Titolare dei diritti. versione completa del Software installato; tipo di software installato; ID aggiornamento Software; ID del servizio di reputazione; ID del tipo di protocollo; ID di un centro di attivazione regionale; versione dell'elenco delle decisioni del servizio Software revocato; ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record dei database anti-virus del Software attivati; ID univoco dell'istanza di installazione dell'applicazione nel computer; data di attivazione della licenza; data di scadenza della licenza; identificatore della licenza; stato della licenza utilizzata dal software; tipo di checksum per l'oggetto elaborato; nome del malware rilevato o del software legittimo che può essere utilizzato per danneggiare i dati o il dispositivo dell'utente; checksum dell'oggetto elaborato; checksum del codice di attivazione del Software; versione completa del software; ID Software; checksum del file chiave del Software; ID del modello di informazioni utilizzato per fornire la licenza Software; identificatore del certificato utilizzato per accedere all'intestazione del ticket della licenza Software; data e ora di creazione del ticket di licenza Software; checksum del ticket di licenza Software; versione del ticket di licenza Software; versione del codice di attivazione del Software; formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; ID ticket licenza corrente; ID componente Software; risultato dell'azione del Software; codice errore; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); numero di porta; indirizzo Web dell'origine della richiesta del servizio Web (Referrer); numero di cicli di applicazione degli aggiornamenti per i database anti-virus; data e ora dell'ultimo aggiornamento e dell'applicazione dei database anti-virus; data e ora di rilascio dei database del Software; versione del componente del Software; ID aggiornamento Software; tipo di software installato; data e ora di avvio di Controllo sistema; data e ora di installazione del Software; probabilità di invio statistiche da parte di Controllo sistema; codice dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; tempo di elaborazione del database dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; tempo massimo consentito per l'elaborazione di un evento da parte di Controllo sistema; tempo di elaborazione dell'evento che ha richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema; numero totale di eventi che hanno richiesto più tempo rispetto alla durata standard per l'elaborazione da parte di Controllo sistema.

- Informazioni su tutti gli oggetti elaborati e sulle operazioni: verdetto del Software sull'oggetto elaborato; codice directory; dimensioni dell'oggetto elaborato; checksum (SHA256) dell'oggetto elaborato; numero del software rilevato nel contesto Controllo sistema; data e ora di rilevamento del software da parte di Controllo sistema; caratteristiche di rilevamento; ID del record attivato nei database anti-virus del Software; motivo del rilevamento del software da parte di Controllo sistema; checksum (MD5) dell'oggetto elaborato; risultato del controllo dell'integrità del modulo; nome dell'oggetto elaborato; tipo di record dei database anti-virus del Software attivati; percorso dell'oggetto elaborato; nome dell'oggetto esaminato; data e ora della scansione; URL e indirizzi Referrer da cui è stato scaricato; dimensioni dei file esaminati e dei relativi percorsi; segno dell'archivio; data e ora di creazione del file; nome, dimensioni e checksum (MD5, SHA2-256) dello strumento di creazione dei pacchetti (se il file è stato compresso); l'entropia del file; tipo di file; codice del tipo di file; formato, ID e segno del file eseguibile; checksum dell'oggetto (MD5, SHA2-256); tipo e il valore del checksum supplementare dell'oggetto; dati relativi alla firma digitale dell'oggetto (certificato): dati sull'entità di pubblicazione del certificato, numero di avvii dell'oggetto dall'ultimo invio di dati statistici, ID dell'attività di scansione dell'applicazione, modalità di ricezione delle informazioni sulla reputazione dell'oggetto, valore del filtro di destinazione, parametri tecnici delle tecnologie di rilevamento applicabili; percorso dell'oggetto elaborato; codice directory.

- Per i file eseguibili: entropia delle sezioni dei file, flag di verifica della reputazione o flag di firma del file, nome, tipo, ID, checksum (MD5) e dimensione dell'applicazione caricata dall'oggetto in fase di convalida, percorso dell'applicazione e percorsi del template, attributo indicante la presenza nell'elenco di esecuzione automatica, data di inserimento, elenco di attributi, nome dello strumento di creazione dei pacchetti, informazioni sulla firma digitale dell'applicazione: certificato dell'autore, nome del file caricato nel formato MIME, data e ora di compilazione del file.

- Informazioni sulle applicazioni avviate e sui rispettivi moduli: checksum (MD5, SHA2-256) dei file in esecuzione, dimensioni, attributi, data di creazione, nome dello strumento di creazione dei pacchetti (se il file è stato inserito in un pacchetto), nomi dei file, informazioni sui processi in esecuzione nel sistema (ID processo (PID), nome processo, informazioni sull'account da cui è stato avviato il processo, l'applicazione e il comando che hanno avviato il processo, percorso completo dei file del processo e riga di comando iniziale, descrizione dell'applicazione alla quale appartiene il processo (nome dell'applicazione e informazioni sull'autore), certificati digitali utilizzati e informazioni necessarie per verificarne l'autenticità o informazioni sull'assenza della firma digitale di un file), nonché informazioni sui moduli caricati nei processi: nome, dimensione, tipo, data di creazione, attributi, checksum (MD5, SHA2-256, SHA1), percorsi, informazioni sull'intestazione dei file PE, nomi degli strumenti di creazione dei pacchetti (se il file è stato inserito in un pacchetto), informazioni sulla disponibilità e la validità di queste statistiche e ID della modalità utilizzata per generare le statistiche inviate.

- Se vengono identificate minacce o vulnerabilità, oltre alle informazioni sull'oggetto rilevato verranno fornite informazioni sull'identificatore, sulla versione e sul tipo di record nel database anti-virus, il nome della minaccia in base alla classificazione Kaspersky, la data e l'ora dell'ultimo aggiornamento del database anti-virus, il nome del file eseguibile, il checksum (MD5) del file dell'applicazione che ha richiesto l'URL in cui è stata rilevata la minaccia, l'indirizzo IP (IPv4 o IPv6) della minaccia rilevata, l'identificatore della vulnerabilità e il livello della minaccia, l'URL e il Referrer della pagina Web in cui è stata rilevata la vulnerabilità.

- Se viene rilevato un oggetto potenzialmente dannoso, le relative informazioni sui dati vengono trasmesse nella memoria dei processi.

- Informazioni sugli attacchi di rete: indirizzo IP del computer da cui proviene l'attacco e numero della porta nel computer dell'utente interessata dall'attacco di rete, ID del protocollo di attacco, nome e tipo di attacco.

- Informazioni sulle connessioni di rete: la versione e i checksum (MD5, SHA2-256, SHA1) del file da cui il processo è stato avviato che ha aperto la porta, il percorso del file del processo e la sua firma digitale, gli indirizzi IP locale e remoto, i numeri delle porte di connessione locali e remote, lo stato di connessione, il timestamp dell'apertura della porta.

- L'URL e l'indirizzo IP della pagina web su cui è stato rilevato il contenuto dannoso o sospetto, il nome, la dimensione e il checksum del file che ha richiesto l'URL, il codice identificativo, il peso e il grado della regola impiegata per raggiungere il verdetto, l'oggetto dell'attacco.

- Informazioni sugli aggiornamenti dell'applicazione installata e dei database anti-virus: stato di completamento dell'attività di aggiornamento, tipo di errore che potrebbe essersi verificato durante il processo di aggiornamento, numero di aggiornamenti non riusciti e identificatore del componente dell'applicazione che esegue gli aggiornamenti.

- Informazioni sull'utilizzo di Kaspersky Security Network (KSN): identificatore KSN, identificatore dell'applicazione, versione completa dell'applicazione, indirizzo IP depersonalizzato del dispositivo dell'Utente, indicatori della qualità di adempimento delle richieste KSN, indicatori della qualità di elaborazione dei pacchetti KSN, indicatori del numero di richieste KSN e informazioni sui tipi di richieste KSN, data e ora di inizio e fine dell'invio delle statistiche; Informazioni sugli aggiornamenti della configurazione KSN: identificatore della configurazione attiva, identificatore della configurazione ricevuta, codice di errore dell'aggiornamento della configurazione.

- Informazioni sugli eventi del registro di sistema: ora dell'evento, nome del registro in cui è stato rilevato l'evento, tipo e categoria dell'evento, nome dell'origine dell'evento e descrizione dell'evento.

- Informazioni per determinare la reputazione dei file e gli indirizzi URL: l'indirizzo URL a cui si chiede la reputazione e il Referrer, il tipo di protocollo della connessione, l'ID interno del tipo di applicazione, il numero della porta in uso, l'ID Utente, il checksum del file analizzato (MD5), il tipo di minaccia rilevata e le informazioni sul registro utilizzato per rilevare una minaccia (l'identificatore del registro per il database anti-virus, il tipo e la marca temporale); chiave pubblica del certificato; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash.

- Dati sulla distribuzione territoriale dell'applicazione: data di installazione e attivazione dell'applicazione, ID del partner che fornisce la licenza per l'attivazione dell'applicazione, ID dell'applicazione, ID localizzazione lingua applicazione, numero di serie della licenza di attivazione dell'applicazione, indicazione di partecipazione a KSN.

- Informazioni sulla licenza utilizzata: tipo di licenza e relativo periodo di validità, numero di giorni restanti prima della scadenza della licenza, identificatore del partner dal quale la licenza è stata acquistata, identificatore del Centro regionale di attivazione, checksum del codice di attivazione, hash del corpo del ticket calcolato tramite l'algoritmo SHA1, data e ora di creazione del ticket di licenza, identificatore dei dati della licenza, identificatore del ticket della licenza, identificatore di sequenza del ticket della licenza, identificatore univoco del computer dell'utente, data di inizio validità del ticket della licenza, data di fine validità del ticket della licenza, stato corrente del ticket della licenza, versione intestazione ticket, versione della licenza, identificatore certificato di firma intestazione ticket, checksum del file chiave, numero di serie firmatario intestazione ticket, token di autenticazione.

- - Informazioni sull'hardware installato nel computer; tipo, nome, nome del modello, versione firmware, parametri dei dispositivi integrati e collegati.

- Informazioni su dispositivo: ID dispositivo.

- Informazioni sul funzionamento del componente Controllo Web:
  versione del componente, motivo della categorizzazione, informazioni aggiuntive sul motivo della categorizzazione, URL categorizzato, indirizzo IP host dell'oggetto bloccato/categorizzato.

Modalità cloud

L'interruttore **Modalità cloud** consente di abilitare/disabilitare la modalità operativa dell'applicazione in cui Kaspersky Endpoint Security utilizza una versione light dei database anti-malware. Questa modalità è disponibile solo se la partecipazione a Kaspersky Security Network è abilitata. La versione light dei database anti-malware consente di utilizzare circa la metà della RAM del computer che verrebbe usata con i database completi. Se non si partecipa a Kaspersky Security Network o se la modalità cloud è disabilitata, Kaspersky Endpoint Security scarica la versione completa dei database anti-malware dai server Kaspersky.

Se l'interruttore è attivato, Kaspersky Endpoint Security utilizza la versione light dei database anti-malware, che riduce il carico sul sistema operativo.

Nota: dopo che la casella di controllo è stata selezionata, Kaspersky Endpoint Security scarica la versione light dei database anti-malware durante l'aggiornamento successivo.

Se l'interruttore è disattivato, Kaspersky Endpoint Security utilizza la versione completa dei database anti-malware.

Nota: dopo che la casella di controllo è stata deselezionata, Kaspersky Endpoint Security scarica la versione completa dei database anti-malware durante l'aggiornamento successivo.

Informativa KSN

Questo collegamento apre una finestra in cui è possibile leggere il testo dell'Informativa su Kaspersky Security Network e accettare le condizioni di partecipazione a Kaspersky Security Network.

Nota: se si gestisce Kaspersky Endpoint Security tramite Kaspersky Security Center Web Console e in base alle impostazioni di Kaspersky Security Center, è possibile partecipare a Kaspersky Private Security Network anziché a Kaspersky Security Network. Se si gestisce Kaspersky Endpoint Security tramite Kaspersky Security Center Cloud Console, la partecipazione a Kaspersky Private Security Network non è disponibile. Per informazioni dettagliate sulla partecipazione a Kaspersky Private Security Network, vedere la Guida di Kaspersky Security Center.

Nella sezione **Impostazioni proxy KSN** è possibile configurare le impostazioni del proxy KSN.

Usa proxy KSN

Questa casella di controllo consente di abilitare o disabilitare l'utilizzo di un server proxy durante la connessione a Kaspersky Security Network.

Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza un server proxy per la connessione a Kaspersky Security Network.

Se la casella di controllo è deselezionata, Kaspersky Endpoint Security si connette direttamente a Kaspersky Security Network.

Questa casella di controllo è deselezionata per impostazione predefinita.

Usa i server Kaspersky quando il proxy KSN non è disponibile

La casella di controllo consente di abilitare o disabilitare l'utilizzo dei server Kaspersky se il proxy KSN non è disponibile.

Se la casella di controllo è selezionata, Kaspersky Endpoint Security utilizza i server Kaspersky quando il proxy KSN non è disponibile.

Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non utilizza i server Kaspersky quando il proxy KSN non è disponibile.

Questa casella di controllo è deselezionata per impostazione predefinita.

Questa casella di controllo è disponibile se la casella di controllo **Usa proxy KSN** è selezionata.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra "Partecipazione a Kaspersky Security Network/Kaspersky Private Security Network"

Ulteriori informazioni

Questo collegamento apre una nuova finestra del browser in cui è possibile leggere il testo dell'Informativa su Kaspersky Security Network o dell'Informativa su Kaspersky Private Security Network.

Accetto le condizioni di partecipazione a Kaspersky Security Network/Kaspersky Private Security Network

I computer ai quali viene applicato il criterio partecipano a Kaspersky Security Network/Kaspersky Private Security Network.

Non accetto le condizioni di partecipazione a Kaspersky Security Network/Kaspersky Private Security Network

I computer ai quali viene applicato il criterio non partecipano a Kaspersky Security Network/Kaspersky Private Security Network.

Nota: se si gestisce Kaspersky Endpoint Security tramite Kaspersky Security Center Cloud Console, la partecipazione a Kaspersky Private Security Network non è disponibile. Per informazioni dettagliate sulla partecipazione a Kaspersky Private Security Network, vedere la Guida di Kaspersky Security Center.

Sezione Protezione Minacce Essenziale

Protezione minacce file

Questo collegamento apre una finestra in cui è possibile configurare le impostazioni di Protezione Minacce File.

Protezione minacce Web

Questo collegamento apre una finestra in cui è possibile configurare le impostazioni di Protezione Minacce Web.

Protezione minacce di rete

Questo collegamento apre una finestra in cui è possibile configurare le impostazioni di Protezione Minacce di Rete.

Protezione minacce di posta

Questo collegamento apre una finestra in cui è possibile configurare le impostazioni di Protezione minacce di posta.

Firewall

Questo collegamento apre una finestra in cui è possibile configurare le impostazioni di Firewall.

Finestra Protezione minacce file

Protezione Minacce File

L'interruttore **Protezione Minacce File** consente di abilitare/disabilitare Protezione Minacce File.

Se l'interruttore **Protezione Minacce File** è attivato, Kaspersky Endpoint Security esegue il monitoraggio in tempo reale del file system dei computer client ai quali è applicato il criterio.

Se l'interruttore **Protezione Minacce File** è disattivato, Kaspersky Endpoint Security non protegge il file system dei computer client ai quali è applicato il criterio.

Questo interruttore è attivato per impostazione predefinita.

Nella sezione **Ambito della protezione** è possibile configurare un ambito della protezione selezionando uno degli elementi preimpostati o aggiungendo file o cartelle a scelta.

Aggiungi

Questo pulsante apre una finestra di dialogo in cui è possibile specificare un file, una cartella o una maschera da aggiungere all'elenco degli oggetti inclusi nell'ambito della protezione.

Elimina

Questo pulsante consente di rimuovere un oggetto dall'ambito della protezione.

Questo pulsante è disponibile se si seleziona un oggetto nell'elenco degli oggetti protetti.

Non è possibile eliminare gli oggetti predefiniti inclusi nell'ambito della protezione.

Ambito della protezione

Questa colonna contiene gli oggetti che Kaspersky Endpoint Security esamina quando Protezione Minacce File è abilitato.

Per impostazione predefinita, Kaspersky Endpoint Security esamina i seguenti oggetti:

- **Tutti i dischi rimovibili**. Kaspersky Endpoint Security esamina tutte le unità rimovibili.
- **Tutti i dischi interni**. Kaspersky Endpoint Security esamina tutte le unità interne.
- **Tutti i dischi di rete**. Kaspersky Endpoint Security esamina tutte le unità di rete.

Stato

Se l'interruttore in questa colonna è attivato, Kaspersky Endpoint Security esamina l'oggetto corrispondente nella colonna **Ambito della protezione** quando Protezione Minacce File è abilitato.

Se l'interruttore in questa colonna è disattivato, Kaspersky Endpoint Security non esamina l'oggetto corrispondente nella colonna **Ambito della protezione** quando Protezione Minacce File è abilitato.

Avanzate

Questa colonna indica se Kaspersky Endpoint Security esamina le sottocartelle dell'oggetto corrispondente.

Nella sezione **Se viene rilevato un oggetto dannoso** è possibile selezionare l'azione che Kaspersky Endpoint Security deve eseguire al rilevamento di un oggetto dannoso.

Richiedi l'intervento dell'utente

Kaspersky Endpoint Security visualizza una finestra di notifica con informazioni sull'oggetto dannoso che ha infettato il file e richiede all'utente di scegliere l'azione che deve essere eseguita da Kaspersky Endpoint Security. Le azioni disponibili possono variare in base allo stato dell'oggetto.

Questa opzione è selezionata per impostazione predefinita.

Disinfetta (se la disinfezione non riesce, elimina)

Kaspersky Endpoint Security blocca l'accesso al file infetto e tenta di disinfettarlo senza richiedere una conferma da parte dell'utente.

Se la disinfezione restituisce esito positivo, Kaspersky Endpoint Security salva il file nella posizione originale con il nome originale. Se la disinfezione non va a buon fine, Kaspersky Endpoint Security elimina il file infetto.

Disinfetta (se la disinfezione non riesce, blocca)

Kaspersky Endpoint Security blocca l'accesso al file infetto e tenta di disinfettarlo senza richiedere una conferma da parte dell'utente.

Se la disinfezione restituisce esito positivo, Kaspersky Endpoint Security salva il file nella posizione originale con il nome originale. Se la disinfezione fallisce, Kaspersky Endpoint Security mantiene il file infetto in uno stato bloccato nella posizione originale.

Nella sezione **Ottimizzazione** è possibile configurare le prestazioni della scansione e selezionare l'algoritmo di scansione.

Esamina solo file nuovi e modificati

Questa casella di controllo consente di abilitare o disabilitare la scansione dei soli file riconosciuti da Kaspersky Endpoint Security come nuovi o modificati rispetto all'ultima scansione.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina solo i file che vengono riconosciuti come nuovi o modificati rispetto all'ultima scansione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esegue la scansione di tutti i file.

Questa casella di controllo è selezionata per impostazione predefinita.

Ignora la scansione del volume di sistema di sola lettura

Questa casella di controllo consente di disabilitare/abilitare la scansione del volume di sistema di sola lettura da parte di Kaspersky Endpoint Security.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non esamina il volume di sistema di sola lettura. Questo riduce notevolmente la durata scansione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esamina il volume di sistema di sola lettura.

Questa casella di controllo è selezionata per impostazione predefinita.

Usa iSwift

Questa casella di controllo consente di abilitare o disabilitare l'utilizzo della tecnologia iSwift durante la scansione. iSwift consente a Kaspersky Endpoint Security di utilizzare un algoritmo speciale per escludere alcuni oggetti dalla scansione, operazione che permette di aumentare la velocità di scansione.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security utilizza iSwift durante la scansione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security non utilizza iSwift durante la scansione.

Questa casella di controllo è selezionata per impostazione predefinita.

Nella sezione **Tipi di file** è possibile selezionare i file che verranno esaminati da Kaspersky Endpoint Security quando Protezione Minacce File è abilitato.

Esamina tutti i file

Kaspersky Endpoint Security esamina tutti gli oggetti del file system eseguiti, aperti o salvati.

Esamina applicazioni e documenti in base al contenuto

Kaspersky Endpoint Security esamina solo gli oggetti potenzialmente infetti in base al relativo contenuto.

Esamina applicazioni e documenti in base all'estensione

Kaspersky Endpoint Security esamina solo gli oggetti potenzialmente infetti in base alla relativa estensione.

L'elenco delle estensioni è definito da Kaspersky ed è incluso nei database di Kaspersky Endpoint Security.

Kaspersky Endpoint Security esamina sempre i file senza estensioni.

Nella sezione **File compositi** è possibile selezionare i tipi di file compositi esaminati da Kaspersky Endpoint Security quando Protezione Minacce File è abilitato.

Esamina archivi

Questa casella di controllo consente di abilitare o disabilitare la scansione degli archivi. Per l'elenco delle estensioni, fare riferimento alla Guida di Kaspersky Endpoint Security.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina gli archivi.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security ignora gli archivi durante le scansioni.

Esamina pacchetti di installazione

Questa casella di controllo consente di abilitare o disabilitare la scansione dei pacchetti di installazione.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina i pacchetti di installazione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security ignora i pacchetti di installazione durante le scansioni.

Esamina oggetti OLE incorporati

Questa casella di controllo consente di abilitare o disabilitare la scansione degli oggetti incorporati in un file, ad esempio fogli di calcolo di Excel, macro o allegati e-mail.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina gli oggetti OLE incorporati.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security ignora gli oggetti OLE incorporati durante le scansioni.

Non estrarre gli archivi superiori a MB

Questa casella di controllo consente di abilitare o disabilitare un limite per la dimensione degli archivi da esaminare.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security ignora gli archivi di dimensioni superiori al valore specificato durante le scansioni.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security estrae gli archivi e ne esegue la scansione indipendentemente dalle relative dimensioni.

Questa casella di controllo è disponibile se la casella di controllo **Esamina archivi** è selezionata.

Rimanda estrazione degli archivi di dimensioni superiori a MB

Questa opzione consente di limitare la dimensione degli archivi da esaminare.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina tutti gli archivi le cui dimensioni superano il limite impostato, ma con una priorità inferiore e due minuti dopo il rilevamento dell'archivio.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esamina tutti gli archivi con la stessa priorità.

Questa casella di controllo è disponibile se la casella di controllo **Esamina archivi** è selezionata.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra di dialogo "Aggiungi ambito della protezione"

Campo di immissione Immettere un nome file, un nome cartella o una maschera

Percorso di un file, di una cartella o maschera per file/cartelle.

L'oggetto è una cartella

Questa casella di controllo consente di abilitare o disabilitare la scansione di un oggetto come una cartella.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina l'oggetto specificato nel campo **Immettere un nome file, un nome cartella o una maschera** come una cartella.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esamina l'oggetto specificato nel campo **Immettere un nome file, un nome cartella o una maschera** come un file.

Questa casella di controllo è selezionata per impostazione predefinita.

Includi sottocartelle

Questa casella di controllo consente di abilitare o disabilitare la scansione delle sottocartelle della cartella specificata nel campo **Immettere un nome file, un nome cartella o una maschera**.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina le sottocartelle durante le scansioni anti-malware.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esamina solo i file che si trovano direttamente nella cartella specificata nel campo **Immettere un nome file, un nome cartella o una maschera** durante le scansioni anti-malware.

Questa casella di controllo è selezionata per impostazione predefinita.

Finestra "Protezione Minacce Web"

Protezione Minacce Web

L'interruttore **Protezione Minacce Web** consente di abilitare/disabilitare Protezione Minacce Web.

Se l'interruttore **Protezione Minacce Web** è attivato, Protezione Minacce Web esamina i dati inviati e ricevuti dal computer tramite i protocolli HTTP e HTTPS in Safari, Google Chrome o Firefox.

Se l'interruttore **Protezione Minacce Web** è disattivato, Protezione Minacce Web non esamina i dati inviati e ricevuti dal computer tramite i browser Web.

Questo interruttore è attivato per impostazione predefinita.

Nella sezione **Se viene rilevato un oggetto dannoso** è possibile selezionare l'azione che Kaspersky Endpoint Security deve eseguire al rilevamento di un oggetto dannoso.

Richiedi l'intervento dell'utente

Kaspersky Endpoint Security visualizza una finestra di notifica con informazioni sul tipo di malware che ha infettato l'oggetto del traffico Web e richiede all'utente di scegliere l'azione che deve essere eseguita da Kaspersky Endpoint Security su tale oggetto. Le azioni disponibili possono variare in base allo stato dell'oggetto.

Questa azione è selezionata per impostazione predefinita.

Blocca automaticamente

Kaspersky Endpoint Security blocca automaticamente l'accesso agli oggetti pericolosi del traffico Web.

Nella sezione **Indirizzi Web attendibili** è possibile creare o modificare un elenco di indirizzi Web attendibili e abilitare o disabilitare la scansione del traffico dagli indirizzi Web presenti nell'elenco.

Non esaminare il traffico Web proveniente da indirizzi Web attendibili

Questa casella di controllo consente di abilitare o disabilitare la scansione dei traffico Web per gli indirizzi Web attendibili.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non esamina il traffico Web per gli indirizzi Web attendibili.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esamina il traffico Web per gli indirizzi Web attendibili.

Questa casella di controllo è deselezionata per impostazione predefinita.

Elenco degli indirizzi Web

Questo elenco contiene gli indirizzi Web attendibili.

È possibile deselezionare la casella di controllo accanto a un indirizzo Web nell'elenco. Se la casella di controllo è deselezionata, Protezione Minacce Web esamina il traffico Web per l'indirizzo Web.

L'elenco è disponibile se la casella di controllo **Non esaminare il traffico Web proveniente da indirizzi Web attendibili** è selezionata.

Aggiungi

Questo pulsante apre una finestra di dialogo cui è possibile immettere un indirizzo Web o una maschera per gli indirizzi Web da aggiungere all'elenco degli indirizzi Web attendibili.

Elimina

Questo pulsante consente di rimuovere l'indirizzo Web o la maschera per gli indirizzi Web selezionata dall'elenco.

Questo pulsante è disponibile se è selezionato un indirizzo Web o una maschera per gli indirizzi Web nell'elenco degli indirizzi Web attendibili.

Indirizzo Web

Questa colonna contiene gli indirizzi Web attendibili.

Stato

Se l'interruttore in questa colonna è attivato, Kaspersky Endpoint Security non esamina l'oggetto corrispondente della colonna **Indirizzo Web** quando Protezione Minacce Web è abilitato e la casella di controllo **Non esaminare il traffico Web proveniente da indirizzi Web attendibili** è selezionata.

Se l'interruttore in questa colonna è disattivato, Kaspersky Endpoint Security esamina l'oggetto corrispondente della colonna **Indirizzo Web** quando Protezione Minacce Web è abilitato e la casella di controllo **Non esaminare il traffico Web proveniente da indirizzi Web attendibili** è selezionata.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra di dialogo "Aggiungi indirizzo Web"

Campo di immissione Indirizzo Web.

Un indirizzo Web o una maschera indirizzi Web il cui traffico non verrà esaminato da Protezione Minacce Web.

Nella sezione **Stato** è possibile definire se Kaspersky Endpoint Security esamina il traffico da questo indirizzo Web o gruppo di indirizzi Web.

Disabilita

L'indirizzo Web o la maschera indirizzi Web viene aggiunto all'elenco **Indirizzi Web attendibili**, ma Kaspersky Endpoint Security esamina il relativo traffico.

Abilita

L'indirizzo Web o la maschera indirizzi Web viene aggiunto all'elenco **Indirizzi Web attendibili** e Kaspersky Endpoint Security non esamina il relativo traffico.

Finestra "Protezione Minacce di Rete"

Protezione Minacce di Rete

L'interruttore **Protezione Minacce di Rete** consente di abilitare/disabilitare Protezione Minacce di Rete.

Se l'interruttore **Protezione Minacce di Rete** è attivato, Kaspersky Endpoint Security protegge il computer remoto dagli attacchi di rete.

Se l'interruttore **Protezione Minacce di Rete** è disattivato, Kaspersky Endpoint Security non protegge il computer remoto dagli attacchi di rete.

Questo interruttore è attivato per impostazione predefinita.

Nella sezione **Impostazioni di Protezione minacce di rete** è possibile modificare il periodo per cui Kaspersky Endpoint Security blocca i computer da cui hanno origine gli attacchi.

Blocca computer da cui ha origine l'attacco per min

Questa casella di controllo consente di abilitare o disabilitare l'aggiunta dei computer da cui ha origine l'attacco all'elenco dei computer bloccati per il periodo specificato.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security aggiunge i computer da cui ha avuto origine l'attacco all'elenco dei computer bloccati per il periodo specificato.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security non blocca i computer da cui ha avuto origine l'attacco.

Questa casella di controllo è selezionata per impostazione predefinita.

Per impostazione predefinita, i computer da cui ha avuto origine l'attacco sono bloccati per 60 minuti.

Nella sezione **Esclusioni** è possibile creare o modificare un elenco di indirizzi IP dei computer remoti le cui attività della rete non verranno mai bloccate da Kaspersky Endpoint Security.

Elenco degli indirizzi IP

Questo elenco contiene gli indirizzi IP dei computer remoti la cui attività di rete non viene mai bloccata da Kaspersky Endpoint Security.

Aggiungi

Questo pulsante apre una finestra di dialogo in cui è possibile immettere l'indirizzo IP di un computer remoto.

Elimina

Questo pulsante consente di rimuovere dall'elenco l'indirizzo IP selezionato.

Questo pulsante è disponibile se l'indirizzo IP di un computer remoto è selezionato nell'elenco degli indirizzi IP.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra di dialogo "Aggiungi esclusione"

Campo di immissione Indirizzo IP

Indirizzo IP di un computer remoto.

Sezione "Controlli di sicurezza"

Controllo Web

L'interruttore **Controllo Web** consente di abilitare/disabilitare Controllo Web.

Se l'interruttore **Controllo Web** è attivato, è possibile creare le regole per gestire i siti Web che gli utenti visitano nei computer remoti.

Se l'interruttore **Controllo Web** è disattivato, non è possibile gestire i siti Web che gli utenti visitano nei computer remoti.

Questo interruttore è disattivato per impostazione predefinita.

Elenco di regole

Questo elenco contiene le regole create per gestire i siti Web visitati dagli utenti nei computer remoti.

L'ordinamento delle regole determina la priorità della relativa applicazione da parte di Kaspersky Endpoint Security.

Aggiungi

Questo pulsante apre una finestra in cui è possibile creare una nuova regola per Controllo Web.

Elimina

Questo pulsante consente di eliminare la regola selezionata dall'elenco delle regole.

Questo pulsante è disponibile se la casella di controllo accanto alla regola è selezionata.

Su

Questo pulsante sposta verso l'alto la regola selezionata nell'elenco delle regole e ne aumenta la priorità di applicazione da parte di Kaspersky Endpoint Security.

Giù

Questo pulsante sposta verso il basso la regola selezionata nell'elenco delle regole e ne riduce la priorità di applicazione da parte di Kaspersky Endpoint Security.

Nome

Nome della regola.

Condizione

L'interruttore in questa colonna definisce se la regola è attiva oppure no.

È possibile abilitare/disabilitare l'interruttore accanto alla regola corrispondente per modificare lo stato della regola.

Azione

Un'azione eseguita da Kaspersky Endpoint Security quando l'utente visita un determinato indirizzo Web, gruppo di indirizzi Web o categoria di siti Web interessati dalla regola.

È possibile modificare l'azione assegnata selezionando un'altra opzione nel menu di scelta rapida corrispondente in questa colonna.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra "Modifica regola"

Campo di immissione Nome regola

Nome della regola.

Nella sezione **Condizione** è possibile impostare la regola come attiva o inattiva.

Attiva

Se questa opzione è selezionata, la regola creata sarà attiva. Verrà applicata al computer remoto subito dopo l'applicazione del criterio.

Inattiva

Se questa opzione è selezionata, la regola creata sarà inattiva. Verrà impostata come in sospeso al momento dell'applicazione del criterio.

Nella sezione **Azione** è possibile selezionare l'azione eseguita da Kaspersky Endpoint Security quando l'utente visita un determinato indirizzo Web, gruppo di indirizzi Web o categoria di siti Web interessati dalla regola.

Consenti

Se questa opzione è selezionata, Kaspersky Endpoint Security consente all'utente di visitare l'indirizzo Web, il gruppo di indirizzi Web o la categoria di siti Web interessati dalla regola.

Nota: Kaspersky Endpoint Security consente di visitare le risorse Web nel computer remoto se l'interruttore **Controllo connessioni sicure (HTTPS)** è attivato nella finestra **Rete** della Creazione guidata nuovo criterio.

Questa opzione è selezionata per impostazione predefinita.

Blocca

Se questa opzione è selezionata, Kaspersky Endpoint Security impedisce all'utente di visitare l'indirizzo Web, il gruppo di indirizzi Web o la categoria di siti Web interessati dalla regola.

Nota: Kaspersky Endpoint Security visualizza notifiche quando l'utente accede alle risorse Web bloccate da Controllo Web nel computer remoto se l'interruttore **Controllo connessioni sicure (HTTPS)** è attivato nella finestra **Rete** della Creazione guidata nuovo criterio.

Mostra avviso

Se questa opzione è selezionata, Kaspersky Endpoint Security visualizza un avviso quando l'utente tenta di visitare l'indirizzo Web, il gruppo di indirizzi Web o la categoria di siti Web interessati dalla regola.

Nella sezione **Area della regola** è possibile scegliere di creare una regola per uno specifico indirizzo Web, per un gruppo di indirizzi Web o per categorie di siti Web.

Categorie

Se questa opzione è selezionata, verrà creata una regola per le categorie di siti Web.

Seleziona categorie

Questo collegamento consente di aprire una finestra di dialogo in cui è possibile selezionare le categorie di siti Web interessate dalla regola.

Indirizzi singoli

Se questa opzione è selezionata, verrà creata una regola per uno specifico indirizzo Web o per un gruppo di indirizzi Web.

Questa opzione è selezionata per impostazione predefinita.

Aggiungi

Questo pulsante apre una finestra di dialogo in cui è possibile specificare un indirizzo Web o una maschera indirizzi Web interessati dalla regola.

Elimina

Questo pulsante consente di rimuovere l'indirizzo Web selezionato o la maschera indirizzi Web selezionata dall'elenco degli indirizzi Web interessati dalla regola.

Questo pulsante è disponibile se la casella di controllo accanto all'indirizzo Web o alla maschera indirizzi Web è selezionata.

Indirizzo

Indirizzi Web o maschere indirizzi Web interessati dalla regola.

Finestra di dialogo "Aggiungi indirizzo Web"

Campo di immissione Indirizzo Web.

L'indirizzo Web o la maschera indirizzi Web che saranno interessati dalla regola.

Finestra di dialogo "Categorie di contenuti"

Elenco delle categorie di contenuti

Questo elenco contiene l'elenco delle categorie di siti Web che è possibile aggiungere alla regola.

La casella di controllo accanto al nome di una categoria di siti Web aggiunge/rimuove i siti Web appartenenti a tale categoria nella regola.

Tutte le caselle di controllo sono deselezionate per impostazione predefinita.

Sezione Detection and Response

Managed Detection and Response

Questo collegamento consente di aprire una finestra in cui è possibile configurare le impostazioni di Managed Detection and Response.

Endpoint Detection and Response

Questo collegamento consente di aprire una finestra in cui è possibile configurare le impostazioni di Endpoint Detection and Response.

Endpoint Detection and Response Expert (on-premise)

Questo collegamento consente di aprire una finestra in cui è possibile configurare le impostazioni di Endpoint Detection and Response Expert (on-premise).

Finestra "Managed Detection and Response"

Managed Detection and Response

L'interruttore **Managed Detection and Response** consente di abilitare/disabilitare il componente Managed Detection and Response che interagisce con il servizio Kaspersky Managed Detection and Response. Questo servizio rileva ed elimina costantemente le minacce per la protezione rivolte all'organizzazione.

Se l'interruttore **Managed Detection and Response** è attivato e il file di configurazione MDR viene importato, il componente Managed Detection and Response è abilitato.

Se l'interruttore **Managed Detection and Response** è disattivato, il componente Managed Detection and Response è disabilitato.

Questo interruttore è disattivato per impostazione predefinita.

Importa

Questo pulsante consente di aprire una finestra in cui è possibile importare il file di configurazione MDR nel criterio di Kaspersky Endpoint Security.

Elimina file di configurazione

Questo pulsante consente di eliminare il file di configurazione MDR dal criterio di Kaspersky Endpoint Security.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra Endpoint Detection and Response

Endpoint Detection and Response

L'interruttore **Endpoint Detection and Response** consente di abilitare/disabilitare il componente Endpoint Detection and Response che interagisce con la soluzione Kaspersky Endpoint Detection and Response. Questa soluzione protegge i computer dalle minacce complesse, inclusi nuovi exploit, ransomware e attacchi senza file.

Se l'interruttore **Endpoint Detection and Response** è attivato, il componente Endpoint Detection and Response è abilitato.

Se l'interruttore **Endpoint Detection and Response** è disattivato, il componente Endpoint Detection and Response è disabilitato.

Questo interruttore è disattivato per impostazione predefinita.

Nella sezione **Isolamento di rete** è possibile configurare le impostazioni per isolare i computer dalla rete in risposta al rilevamento di un indicatore di compromissione.

Configura le impostazioni di sblocco del computer

Questo collegamento consente di aprire una finestra in cui è possibile specificare il ritardo per la disattivazione automatica dell'Isolamento di rete.

Esclusioni

Questo collegamento consente di aprire una finestra in cui è possibile specificare le connessioni di rete che non vengono bloccate nel computer dopo l'abilitazione automatica dell'Isolamento di rete.

Nella sezione **Prevenzione dell'esecuzione** è possibile configurare le impostazioni per l'esecuzione di file eseguibili e script e per l'apertura di file in formato Office.

Prevenzione dell'esecuzione

L'interruttore **Prevenzione dell'esecuzione** consente di abilitare/disabilitare Prevenzione dell'esecuzione.

Se l'interruttore **Prevenzione dell'esecuzione** è attivato, è possibile creare e modificare l'elenco delle regole di prevenzione dell'esecuzione e selezionare un'azione da eseguire quando gli oggetti vietati vengono eseguiti o aperti.

Se l'interruttore **Prevenzione dell'esecuzione** è disattivato, non è possibile gestire gli oggetti eseguiti o aperti dagli utenti nei dispositivi.

Questo interruttore è disattivato per impostazione predefinita.

Azione in caso di esecuzione o apertura di un oggetto vietato

Blocca e scrivi nel rapporto

Se questa modalità è selezionata, l'applicazione blocca l'esecuzione di oggetti o l'apertura di documenti che soddisfano i criteri della regola di prevenzione. L'applicazione pubblica anche un evento sui tentativi di esecuzione di oggetti o di documenti aperti nel registro eventi di Kaspersky Security Center e nel sistema di registrazione unificato.

Registra solo gli eventi

Se questa modalità è selezionata, Kaspersky Endpoint Security pubblica un evento sui tentativi di esecuzione di oggetti eseguibili o di documenti aperti che corrispondono ai criteri della regola di prevenzione nel registro eventi di Kaspersky Security Center e nel sistema di registrazione unificato, ma non blocca il tentativo di eseguire o aprire l'oggetto o il documento. Questa modalità è selezionata per impostazione predefinita.

Aggiungi

Questo pulsante consente di aprire una finestra di dialogo in cui è possibile creare una nuova regola di prevenzione dell'esecuzione.

Modifica

Questo pulsante consente di aprire una finestra di dialogo in cui è possibile modificare una regola di prevenzione esistente.

Questo pulsante è disponibile se viene selezionata una regola nell'elenco delle regole.

Elimina

Questo pulsante consente di rimuovere una regola di prevenzione dell'esecuzione dall'elenco delle regole.

Questo pulsante è disponibile se viene selezionata una regola nell'elenco delle regole.

Nella sezione delle **Impostazioni di sandbox cloud** è possibile abilitare o disabilitare il componente Cloud Sandbox.

Sandbox cloud

L'interruttore **Cloud Sandbox** consente di abilitare/disabilitare la tecnologia Cloud Sandbox che aiuta a rilevare le minacce avanzate su un computer. Kaspersky Endpoint Security inoltra automaticamente i file rilevati a sandbox cloud per l'analisi. Sandbox cloud esegue questi file in un ambiente isolato per identificare le attività dannose e decidere in merito alla reputazione. I dati su questi file vengono quindi inviati a Kaspersky Security Network. Pertanto, se Cloud Sandbox rileva un file dannoso, Kaspersky Endpoint Security eseguirà l'azione appropriata per eliminare la minaccia in tutti i computer in cui viene rilevato questo file.

Se l'interruttore **Cloud Sandbox** è attivato, la tecnologia Cloud Sandbox è abilitata.

Se l'interruttore **Cloud Sandbox** è disattivato, la tecnologia Cloud Sandbox è disabilitata.

Questo interruttore è disattivato per impostazione predefinita.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra delle impostazioni di sblocco del computer

Sblocca automaticamente il computer isolato tra

Questa casella di controllo consente di abilitare/disabilitare la disattivazione automatica dell'Isolamento di rete dopo un periodo di tempo specificato.

Se questa casella di controllo è selezionata, è possibile specificare il ritardo per la disattivazione automatica dell'Isolamento di rete di un computer.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security disattiva l'Isolamento della rete 8 ore dopo l'inizio dell'isolamento.

Questa casella di controllo è selezionata per impostazione predefinita.

Ore

L'intervallo dopo il quale l'Isolamento di rete verrà disattivato automaticamente.

Questo campo è disponibile per la modifica solo se la casella di controllo **Sblocca automaticamente il computer isolato tra** è selezionata.

Finestra Esclusioni dall'isolamento di rete

Esclusioni dall'isolamento di rete

Questo elenco contiene le connessioni di rete aggiunte come Esclusioni dall'isolamento di rete.

Aggiungi

Questo pulsante consente di aprire una finestra in cui è possibile specificare manualmente le impostazioni della connessione di rete da aggiungere come esclusione.

Aggiungi dal profilo

Questo pulsante consente di aprire una finestra in cui è possibile selezionare i profili di rete standard per la configurazione delle esclusioni.

Elimina

Questo pulsante consente di rimuovere una connessione di rete dall'elenco delle Esclusioni dall'isolamento di rete.

Questo pulsante è disponibile se viene selezionata una connessione nell'elenco delle Esclusioni dall'isolamento di rete.

Finestra Proprietà delle regole

Nome regola

Nome di una regola di Esclusione dall'isolamento di rete.

Si tratta di un parametro facoltativo.

Direzione

Direzione del traffico.

Protocollo

Tipo di protocollo.

Numero

Numero di protocollo.

Il valore deve essere conforme all'elenco IANA dei numeri di protocollo Internet assegnati.

Questo campo è disponibile se è selezionato il tipo di protocollo **Personalizzato**.

Porta locale o intervallo

Porta locale o intervallo del computer per cui vengono configurate le Esclusioni dall'isolamento di rete.

Porta remota o intervallo

Porta remota o intervallo del computer per cui vengono configurate le Esclusioni dall'isolamento di rete.

Indirizzo remoto

Indirizzo di rete del computer per cui vengono configurate le Esclusioni dall'isolamento di rete.

Applicazioni

Questa casella di controllo consente di aggiungere un'applicazione autorizzata ad avviare una connessione di rete aggiunta alle Esclusioni dall'isolamento di rete nel computer isolato.

Se questa casella di controllo è selezionata, è possibile aggiungere tale applicazione.

Se questa casella di controllo è deselezionata, una connessione di rete aggiunta alle Esclusioni dall'isolamento di rete può essere avviata da qualsiasi applicazione nel computer isolato.

Questa casella di controllo è deselezionata per impostazione predefinita.

Aggiungi

Questo pulsante consente di aprire una finestra in cui è possibile specificare un percorso a un'applicazione a cui è consentito avviare una connessione di rete aggiunta alle Esclusioni dall'isolamento di rete.

Modifica

Questo pulsante consente di aprire una finestra in cui è possibile modificare il percorso di un'applicazione aggiunta.

Questo pulsante è disponibile se è selezionata un'applicazione nell'elenco.

Elimina

Questo pulsante consente di eliminare un'applicazione aggiunta.

Questo pulsante è disponibile se è selezionata un'applicazione nell'elenco.

Finestra Regole di prevenzione

Nome

Nome della regola.

Tipo

Tipo dell'oggetto che si desidera bloccare.

Nella sezione **Percorso dell'oggetto** è possibile selezionare se specificare il percorso completo dell'oggetto da vietare. Se si seleziona di specificare il percorso, immetterne il valore nel campo corrispondente.

Nella sezione **Checksum oggetti** è possibile selezionare se specificare il checksum per l'oggetto da vietare. Se si seleziona di specificare il checksum, selezionarne il tipo e immettere il valore nel campo corrispondente.

Finestra Endpoint Detection and Response (KATA)

Endpoint Detection and Response Expert (on-premise)

L'interruttore **Endpoint Detection and Response Expert (on-premise)** consente di abilitare/disabilitare il componente Endpoint Detection and Response Expert (on-premise) che interagisce con la soluzione Kaspersky Anti Targeted Attack Platform. Questa soluzione rileva prontamente le minacce avanzate, come attacchi mirati, minacce persistenti avanzate, attacchi zero-day e altro.

Se l'interruttore **Endpoint Detection and Response Expert (on-premise)** è attivato, il componente Endpoint Detection and Response Expert (on-premise) è abilitato.

Se l'interruttore **Endpoint Detection and Response Expert (on-premise)** è disattivato, il componente Endpoint Detection and Response Expert (on-premise) è disabilitato.

Questo interruttore è disattivato per impostazione predefinita.

Endpoint Detection and Response Expert (7.1 o versione precedente)

Se questa opzione è selezionata, il componente Endpoint Detection and Response Expert (on-premise) opera in modalità di compatibilità con Endpoint Detection and Response Expert (7.1 o versione precedente).

Endpoint Detection and Response Expert (8.0 o versione successiva)

Se questa opzione è selezionata, il componente Endpoint Detection and Response Expert (on-premise) opera in modalità di compatibilità con Endpoint Detection and Response Expert (8.0 o versione successiva).

Eredita le impostazioni di connessione dal criterio

Se questa opzione è selezionata, le impostazioni della connessione ai server di raccolta della telemetria, i server di raccolta della telemetria, le impostazioni di trasmissione dei dati dei server di raccolta della telemetria, i limiti sul numero di eventi inviati ai server di raccolta della telemetria, le impostazioni di connessione ai server di risposta e i server di risposta vengono ereditati dal criterio padre e diventano non disponibili per la modifica.

Questa opzione è disponibile se è selezionata la modalità **Endpoint Detection and Response Expert (8.0 o versione successiva)**.

Questa opzione è selezionata per impostazione predefinita.

Utilizza impostazioni di connessione personalizzate

Se questa opzione è selezionata, le impostazioni della connessione ai server di raccolta della telemetria, i server di raccolta della telemetria, le impostazioni di trasmissione dei dati dei server di raccolta della telemetria, i limiti sul numero di eventi inviati ai server di raccolta della telemetria, le impostazioni di connessione ai server di risposta e i server di risposta non vengono ereditati dal criterio padre e restano disponibili per la modifica.

Questa opzione è disponibile se è selezionata la modalità **Endpoint Detection and Response Expert (8.0 o versione successiva)**.

A seconda della modalità selezionata nella sezione **Connessione ai server KATA** o **Connessione ai server di raccolta della telemetria** è possibile configurare la connessione alle impostazioni del server.

Impostazioni di connessione

Questo collegamento consente di aprire una finestra di dialogo in cui è possibile configurare le impostazioni per la connessione ai server.

Invia la richiesta di sincronizzazione al server ogni (min)

L'intervallo tra le richieste di sincronizzazione inviate a un server KATA.

Il valore predefinito è 5 minuti.

Questa opzione è disponibile se è selezionata la modalità **Endpoint Detection and Response Expert (8.0 o versione successiva)**.

Aggiungi

Questo pulsante consente di aprire una finestra in cui è possibile configurare una connessione a un server.

Modifica

Questo pulsante consente di aprire una finestra in cui è possibile modificare una connessione esistente a un server.

Questo pulsante è disponibile se è stato selezionato un server nell'elenco dei server.

Elimina

Questo pulsante consente di rimuovere dall'elenco il server selezionato.

Questo pulsante è disponibile se è selezionato un server nell'elenco.

Indirizzo

Indirizzo IP di un server.

Porta

Numero di porta di un server.

Nella sezione **Impostazioni trasmissione dati** è possibile configurare le impostazioni per l'invio dei dati ai server.

Invia telemetria a KATA

Questa casella di controllo abilita/disabilita l'invio di eventi al server KATA.

Se questa casella di controllo è selezionata, gli eventi vengono inviati al server KATA.

Se questa casella di controllo è deselezionata, gli eventi non vengono inviati al server KATA.

Questa opzione è disponibile se è selezionata la modalità **Endpoint Detection and Response Expert (7.1 o versione precedente)**.

Questa casella di controllo è deselezionata per impostazione predefinita.

Invia la telemetria ai server di raccolta della telemetria

Questa casella di controllo consente di abilitare/disabilitare l'invio di eventi al server di raccolta della telemetria.

Se questa casella di controllo è selezionata, gli eventi vengono inviati al server di raccolta della telemetria.

Se questa casella di controllo è deselezionata, gli eventi non vengono inviati al server di raccolta della telemetria.

Questa casella di controllo è disponibile se è selezionata la modalità **Endpoint Detection and Response Expert (8.0 o versione successiva)**.

Questa casella di controllo è deselezionata per impostazione predefinita.

Ritardo massimo trasmissione eventi (s)

L'intervallo con cui Kaspersky Endpoint Security invia gli eventi a un server.

Il valore predefinito è 30 secondi.

Nella sezione **Limitazione delle richieste** è possibile limitare il numero di eventi trasmessi.

Abilita limitazione delle richieste

Questa casella di controllo consente di abilitare/disabilitare il numero di eventi inviati da Kaspersky Endpoint Security a un server KATA.

Se questa casella di controllo è selezionata, il numero di eventi inviati dall'applicazione è limitato.

Se questa casella di controllo è deselezionata, il numero di eventi inviati dall'applicazione non viene limitato.

Questa casella di controllo è selezionata per impostazione predefinita.

Numero massimo di eventi all'ora

Il numero massimo di eventi che Kaspersky Endpoint Security invia a un server KATA all'ora. Kaspersky Endpoint Security riprende l'invio degli eventi dopo un'ora.

Il valore predefinito è 3000 eventi all'ora.

Percentuale di eccedenza limite eventi

La soglia per gli eventi dello stesso tipo (in percentuale).

Kaspersky Endpoint Security limita la trasmissione di eventi di un particolare tipo se il rapporto tra gli eventi di quel tipo e il numero totale di eventi supera la soglia configurata.

Il valore predefinito è 15 percento.

Nella sezione **Connessione ai server di risposta** è possibile configurare la connessione alle impostazioni dei server di risposta.

Impostazioni di connessione

Questo collegamento consente di aprire una finestra di dialogo in cui è possibile configurare le impostazioni per la connessione ai server.

Invia la richiesta di sincronizzazione al server ogni (min)

L'intervallo tra le richieste di sincronizzazione inviate a un server KATA.

Il valore predefinito è 5 minuti.

Questa opzione è disponibile se è selezionata la modalità **Endpoint Detection and Response Expert (8.0 o versione successiva)**.

Aggiungi

Questo pulsante consente di aprire una finestra in cui è possibile configurare una connessione a un server.

Modifica

Questo pulsante consente di aprire una finestra in cui è possibile modificare una connessione esistente a un server.

Questo pulsante è disponibile se è stato selezionato un server nell'elenco dei server.

Elimina

Questo pulsante consente di rimuovere dall'elenco il server selezionato.

Questo pulsante è disponibile se è selezionato un server nell'elenco.

Indirizzo

Indirizzo IP di un server.

Porta

Numero di porta di un server.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra server KATA

Indirizzo

Indirizzo IP di un server KATA.

Porta

Numero di porta di un server KATA.

Il valore predefinito è 443.

Finestra Impostazioni di connessione al server

Timeout (s)

Il timeout di risposta del server KATA. Allo scadere del timeout, Kaspersky Endpoint Security tenta di connettersi a un altro server KATA.

Il valore predefinito è 10 secondi.

Nella sezione **Certificato TLS del server** è possibile aggiungere o rimuovere un certificato TLS e visualizzare le informazioni sul certificato aggiunto.

Aggiungi certificato TLS

Questo pulsante consente di aprire una finestra in cui è possibile selezionare un certificato TLS che verrà utilizzato per stabilire una connessione attendibile con un server KATA.

Rimuovi

Questo pulsante consente di rimuovere il certificato TLS corrente.

Questo pulsante è disponibile se è stato aggiunto un certificato TLS.

Nella sezione **Sicurezza connessione aggiuntiva** è possibile configurare la protezione ottimizzata per la connessione tra Kaspersky Endpoint Security e un server KATA.

Usa autenticazione a due vie

Questa casella di controllo consente di abilitare/disabilitare la verifica bidirezionale che rende più sicura la connessione tra Kaspersky Endpoint Security e un server KATA. Per utilizzare la verifica bidirezionale, è necessario caricare un contenitore criptato.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security utilizza la verifica bidirezionale per connettersi a un server KATA.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security non utilizza la verifica bidirezionale per connettersi a un server KATA.

Questa casella di controllo è deselezionata per impostazione predefinita.

Carica contenitore crittografico

Facendo clic su questo pulsante viene aperta una finestra in cui è possibile selezionare un contenitore criptato che verrà utilizzato per la verifica bidirezionale. Il file del contenitore criptato ha l'estensione .PFX.

Nota: il contenitore criptato deve essere protetto da password. Non è possibile aggiungere un contenitore criptato con una password vuota.

Password contenitore crittografico

La password per il contenitore criptato utilizzato per la verifica bidirezionale.

Sezione "Aggiornamento"

Aggiorna moduli dell'applicazione

Questa casella di controllo consente di abilitare o disabilitare gli aggiornamenti dei moduli dell'applicazione. I database dell'applicazione sono sempre aggiornati.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security aggiorna i moduli dell'applicazione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security non aggiorna i moduli dell'applicazione.

Questa casella di controllo è selezionata per impostazione predefinita.

Sorgenti degli aggiornamenti

Questo elenco contiene gli indirizzi delle risorse da cui Kaspersky Endpoint Security scarica e installa gli aggiornamenti dei database e dei moduli dell'applicazione. È possibile specificare una cartella locale o di rete oppure un server FTP o HTTP come sorgente degli aggiornamenti.

Per impostazione predefinita, l'elenco delle sorgenti degli aggiornamenti contiene i server degli aggiornamenti Kaspersky.

Se si gestisce Kaspersky Endpoint Security tramite Kaspersky Security Center Web Console, l'elenco delle sorgenti degli aggiornamenti include anche i server Kaspersky Security Center per impostazione predefinita.

Se si gestisce Kaspersky Endpoint Security tramite Kaspersky Security Center Cloud Console, l'elenco delle sorgenti degli aggiornamenti include anche i punti di distribuzione per impostazione predefinita. Per informazioni dettagliate sui punti di distribuzione, vedere la Guida di Kaspersky Security Center.

Non è possibile rimuovere le sorgenti degli aggiornamenti predefinite dall'elenco.

Aggiungi

Questo pulsante apre una finestra di dialogo in cui è possibile specificare il percorso di una cartella locale o di rete o l'indirizzo Web da aggiungere all'elenco delle sorgenti degli aggiornamenti.

Elimina

Questo pulsante consente di rimuovere dall'elenco la sorgente degli aggiornamenti selezionata.

Questo pulsante è disponibile se la casella di controllo accanto alla sorgente degli aggiornamenti è selezionata.

Sorgente degli aggiornamenti

Questa colonna contiene le sorgenti degli aggiornamenti per Kaspersky Endpoint Security.

Stato

Se l'interruttore in questa colona è attivato, Kaspersky Endpoint Security utilizza la sorgente degli aggiornamenti corrispondente dalla colonna **Sorgente degli aggiornamenti** per ricevere gli aggiornamenti.

Se l'interruttore in questa colona è disattivato, Kaspersky Endpoint Security non utilizza la sorgente degli aggiornamenti corrispondente dalla colonna **Sorgente degli aggiornamenti** per ricevere gli aggiornamenti.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra di dialogo "Aggiungi sorgente degli aggiornamenti"

Campo di immissione Immettere il percorso di una cartella locale o di rete o un indirizzo Web

Indirizzo della risorsa da cui Kaspersky Endpoint Security copia gli aggiornamenti.

È possibile specificare il percorso di una cartella locale o di rete oppure l'indirizzo Web o IP di un server FTP o HTTP come indirizzo della risorsa.

È possibile specificare l'indirizzo Web di un server FTP nel seguente formato: ftp://<nome utente>:<password>@<host>:<porta>.

Nella sezione **Stato** è possibile definire se Kaspersky Endpoint Security utilizza l'indirizzo Web specificato come sorgente degli aggiornamenti.

Disabilitato

L'indirizzo Web viene aggiunto all'elenco delle sorgenti degli aggiornamenti, ma Kaspersky Endpoint Security non utilizza questo indirizzo Web come sorgente degli aggiornamenti.

Abilitato

L'indirizzo Web viene aggiunto all'elenco delle sorgenti degli aggiornamenti e Kaspersky Endpoint Security utilizza questo indirizzo Web come sorgente degli aggiornamenti.

Sezione "Criptaggio dei dati"

Criptaggio disco FileVault

L'interruttore **Criptaggio disco FileVault** consente di abilitare/disabilitare la gestione di Criptaggio disco FileVault.

Se l'interruttore **Criptaggio disco FileVault** è attivato, Criptaggio disco FileVault può essere applicato ai computer client da Kaspersky Security Center.

Se l'interruttore **Criptaggio disco FileVault** è disattivato, Criptaggio disco FileVault non può essere applicato ai computer client da Kaspersky Security Center.

Questo interruttore è disattivato per impostazione predefinita.

Nota: se l'interruttore **Criptaggio disco FileVault** è disattivato, gli utenti con i diritti di amministratore possono criptare e decriptare i propri dischi di avvio Mac dalle impostazioni di sistema. Per ulteriori informazioni su FileVault, fare riferimento alla documentazione di Apple.

Cripta disco

Kaspersky Endpoint Security richiede le credenziali dell'account del computer nei computer client ai quali è applicato il criterio. Quando l'utente immette le credenziali, Kaspersky Endpoint Security avvia il criptaggio del disco di avvio dell'utente.

Se l'interruttore **Criptaggio disco FileVault** è attivato e l'opzione **Cripta disco** è selezionata, gli utenti con i diritti di amministratore non possono decriptare il disco di avvio del Mac dalle impostazioni di sistema.

Decripta disco

Kaspersky Endpoint Security richiede le credenziali dell'account del computer nei computer client ai quali è applicato il criterio. Quando l'utente immette le credenziali, Kaspersky Endpoint Security avvia il decriptaggio del disco di avvio dell'utente.

Se l'interruttore **Criptaggio disco FileVault** è attivato e l'opzione **Decripta disco** è selezionata, gli utenti con i diritti di amministratore non possono criptare il disco di avvio del Mac dalle impostazioni di sistema.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra Impostazioni di telemetria

Aggiungi

Questo pulsante apre una finestra in cui è possibile aggiungere una regola all'area attendibile.

Modifica

Questo pulsante apre una finestra in cui è possibile modificare la regola selezionata.

Elimina

Questo pulsante consente di rimuovere dall'Area attendibile la regola selezionata.

Stato

L'interruttore in questa colonna disabilita/abilita la regola aggiunta all'Area attendibile.

Se l'interruttore è abilitato, la regola è attiva.

Se l'interruttore è disabilitato, la regola è inattiva.

Nome regola

Questa colonna contiene i nomi delle regole aggiunti all'Area attendibile.

Descrizione

Un commento con informazioni sulla regola aggiunta all'Area attendibile.

Finestra Aggiungi/modifica regola di esclusione

Stato

Questo interruttore abilita/disabilita la regola aggiunta all'Area attendibile.

Se l'interruttore è abilitato, la regola è attiva.

Se l'interruttore è disabilitato, la regola è inattiva.

Nome regola

Nome della regola aggiunta all'Area attendibile.

Descrizione

Un commento con informazioni sulla regola aggiunta all'Area attendibile.

Indicatori di attacco (IOA)

Campo per l'immissione dei GUID degli indicatori di attacco.

Sezione Impostazioni avanzate

Protezione

Questo collegamento apre la finestra **Protezione**, in cui è possibile gestire le impostazioni generali per Kaspersky Endpoint Security installato nei computer degli utenti e selezionare i tipi di oggetti che Kaspersky Endpoint Security rileverà.

Rapporti e backup

Questo collegamento apre la finestra **Rapporti e backup**, in cui è possibile gestire le impostazioni di rapporti e backup.

Interazione utente

Questo collegamento apre la finestra **Interazione utente**, in cui è possibile configurare le notifiche visualizzate da Kaspersky Endpoint Security, la lingua visualizzata per gli eventi visualizzati in Kaspersky Security Center e le impostazioni avanzate per Kaspersky Endpoint Security.

Rete

Questo collegamento consente di aprire la finestra **Rete** in cui è possibile gestire le impostazioni del server proxy, abilitare o disabilitare la scansione delle connessioni criptate (HTTPS), selezionare l'archivio certificati per il controllo del traffico HTTPS criptato nel browser Mozilla Firefox e configurare le porte monitorate.

Area attendibile

Questo collegamento apre la finestra **Area attendibile**, in cui è possibile aggiungere le esclusioni per Protezione Minacce File o per le attività di scansione e configurare le applicazioni attendibili.

Finestra Protezione

Nella sezione **Generali** è possibile abilitare o disabilitare la protezione dei file in un computer remoto e configurare l'avvio automatico dell'applicazione all'accensione del computer o dopo il riavvio del sistema operativo.

Apri l'applicazione all'avvio del computer

Questa casella di controllo consente di abilitare o disabilitare l'avvio automatico di Kaspersky Endpoint Security all'accensione di un computer remoto o dopo il riavvio del sistema operativo.

Se la casella di controllo è selezionata, Kaspersky Endpoint Security viene avviato automaticamente all'accensione del computer remoto o dopo il riavvio del sistema operativo.

Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non viene avviato automaticamente all'accensione del computer remoto o dopo il riavvio del sistema operativo.

Questa casella di controllo è selezionata per impostazione predefinita.

Importante: se si seleziona questa casella di controllo quando Kaspersky Endpoint Security non è in esecuzione, le modifiche verranno applicate solo dopo l'avvio dell'applicazione in locale o utilizzando Kaspersky Security Center.

Abilita la protezione

Questa casella di controllo consente di abilitare o disabilitare la protezione di un computer remoto in cui è installato Kaspersky Endpoint Security.

Se questa casella di controllo è selezionata, la protezione del computer remoto è abilitata.

Se questa casella di controllo è deselezionata, la protezione del computer remoto è disabilitata.

Questa casella di controllo è selezionata per impostazione predefinita.

Nella sezione **Tipi di oggetti da rilevare** è possibile selezionare i tipi di oggetti che Kaspersky Endpoint Security rileverà.

Virus, worm, Trojan, strumenti dannosi, adware e auto-dialer

Questa casella di controllo consente di abilitare o disabilitare il rilevamento dei seguenti tipi di programmi:

- Tutti i tipi di malware.
- Applicazioni che visualizzano pubblicità (ad esempio banner) nel computer o sostituiscono i risultati di ricerca nel browser Web con siti Web pubblicitari.
- Applicazioni che stabiliscono connessioni telefoniche nascoste tramite un modem del computer.

La casella di controllo è selezionata per impostazione predefinita e non può essere deselezionata.

Software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali dell'utente

Questa casella di controllo consente di abilitare o disabilitare il rilevamento delle applicazioni che non sono dannose o pericolose, ma che in determinate circostanze possono essere utilizzate per danneggiare il computer di un utente.

Se la casella di controllo è selezionata, Kaspersky Endpoint Security rileva il software legittimo che può essere utilizzato da intrusi per danneggiare il computer o i dati personali di un utente.

Se la casella di controllo è deselezionata, Kaspersky Endpoint Security non rileva il software legittimo che può essere utilizzato da intrusi per danneggiare il computer o i dati personali di un utente.

Questa casella di controllo è deselezionata per impostazione predefinita.

La sezione **Avanzate** consente di abilitare la modalità di risparmio energetico.

Ignora attività pianificate durante l'alimentazione a batteria

Questa casella di controllo consente di abilitare o disabilitare l'avvio delle attività di scansione pianificate nei computer alimentati a batteria.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non avvia le attività di scansione pianificate nei computer alimentati a batteria.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security avvia le attività di scansione pianificate nei computer alimentati a batteria.

Questa casella di controllo è selezionata per impostazione predefinita.

Limita l'uso della CPU per le scansioni

Kaspersky Endpoint Security limita l'utilizzo della CPU del dispositivo protetto per le attività di scansione su richiesta in base al valore specificato nel campo di immissione corrispondente.

L'abilitazione di questa opzione può influire negativamente sulle prestazioni di Kaspersky Endpoint Security.

Per impostazione predefinita, questa opzione è disabilitata.

Limite superiore (in percentuali)

Utilizzo massimo della CPU consentito per le attività di scansione da parte di Kaspersky Endpoint Security.

Il campo di immissione è disponibile se l'opzione **Limita l'uso della CPU per le scansioni** è selezionata.

Nota: questo è un limite cumulativo per tutti i core della CPU. L'utilizzo della CPU mostrato in Activity Monitor corrisponde alla somma dell'utilizzo di ciascun core della CPU e pertanto può superare il 100%.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra Rapporti e backup

Nella sezione **Rapporti** è possibile configurare le impostazioni per la generazione e l'archiviazione dei rapporti sugli eventi che si verificano durante l'esecuzione di Kaspersky Endpoint Security.

Elimina i rapporti dopo giorni

Questa casella di controllo consente di abilitare o disabilitare l'eliminazione dei rapporti dopo il periodo specificato.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security elimina i rapporti dopo il periodo specificato. Per impostazione predefinita, Kaspersky Endpoint Security archivia i rapporti per 30 giorni.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security archivia i rapporti a tempo indeterminato.

Questa casella di controllo è selezionata per impostazione predefinita.

Registra eventi non critici

Questa casella di controllo consente di abilitare o disabilitare la registrazione nel rapporto degli eventi non critici (ad esempio, gli eventi informativi). Gli eventi non critici non influiscono sulla sicurezza.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security registra gli eventi informativi nel rapporto.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security non registra gli eventi informativi nel rapporto.

Questa casella di controllo è deselezionata per impostazione predefinita.

Mantieni solo eventi recenti

Questa casella di controllo consente di abilitare o disabilitare la conservazione delle sole informazioni sugli eventi importanti dell'esecuzione precedente dell'attività.

Se questa casella di controllo è selezionata, ogni volta che un'attività viene avviata, Kaspersky Endpoint Security rimuove le informazioni sugli eventi non critici dall'esecuzione precedente dell'attività, ma mantiene nel rapporto le informazioni importanti (ad esempio, sul malware rilevato).

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security mantiene tutte le informazioni relative all'esecuzione precedente dell'attività.

Questa casella di controllo è deselezionata per impostazione predefinita.

Nella sezione **Backup** è possibile specificare il periodo di archiviazione degli oggetti in Backup.

Elimina oggetti dopo giorni

Questa casella di controllo consente di abilitare o disabilitare la rimozione degli oggetti da Backup dopo il periodo specificato.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security rimuove gli oggetti da Backup dopo il periodo specificato. Il periodo di archiviazione predefinito è di 30 giorni.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security archivia gli oggetti in Backup a tempo indeterminato.

Questa casella di controllo è selezionata per impostazione predefinita.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra Interazione utente

Nella sezione **Interfaccia dell'applicazione** è possibile determinare se l'icona dell'applicazione viene visualizzata nella barra dei menu in un computer remoto e se un utente può aprire la finestra principale di Kaspersky Endpoint Security e utilizzare l'interfaccia dell'applicazione.

Mostra icona dell'applicazione nella barra dei menu

Questa casella di controllo consente di abilitare o disabilitare la visualizzazione dell'icona dell'applicazione nella barra dei menu di un computer remoto.

Se questa casella di controllo è selezionata, l'icona dell'applicazione viene visualizzata nella barra dei menu.

Se questa casella di controllo è deselezionata, l'icona dell'applicazione viene nascosta dalla barra dei menu.

Questa casella di controllo è selezionata per impostazione predefinita.

Consenti all'utente di aprire l'applicazione

Questa casella di controllo consente di abilitare/disabilitare la capacità di un utente di aprire la finestra principale di Kaspersky Endpoint Security e utilizzare l'interfaccia dell'applicazione in un computer remoto.

Se questa casella di controllo è selezionata, un utente può aprire la finestra principale di Kaspersky Endpoint Security e utilizzare l'interfaccia dell'applicazione in un computer remoto.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security impedisce a un utente di aprire la finestra principale dell'applicazione e nasconde l'interfaccia dell'applicazione in un computer remoto.

Questa casella di controllo è selezionata per impostazione predefinita.

Nella sezione **Notifiche** è possibile abilitare le notifiche sugli eventi di Kaspersky Endpoint Security e scegliere il tipo di notifica desiderato.

Notifiche

L'interruttore **Notifiche** consente di abilitare/disabilitare le notifiche relative agli eventi di Kaspersky Endpoint Security.

Se l'interruttore **Notifiche** è attivato, Kaspersky Endpoint Security mostra le notifiche sugli eventi che si verificano mentre sono in esecuzione i componenti di Kaspersky Endpoint Security.

Se l'interruttore **Notifiche** è disattivato, Kaspersky Endpoint Security non mostra le notifiche sugli eventi che si verificano mentre sono in esecuzione i componenti di Kaspersky Endpoint Security.

Questo interruttore è attivato per impostazione predefinita.

Notifiche utente

Questo collegamento apre una finestra in cui è possibile selezionare i tipi di notifiche da utilizzare per tutti i tipi di eventi.

Nella sezione **Consenti all'utente di chiudere l'applicazione** è possibile stabilire se Kaspersky Endpoint Security può essere chiuso da un utente in un computer remoto.

Mostra il comando Esci nel menu di scelta rapida dell'icona dell'applicazione

Questa casella di controllo consente di abilitare o disabilitare la disponibilità della voce **Esci** nel menu di scelta rapida dell'icona dell'applicazione visualizzata nella barra dei menu.

Se questa casella di controllo è selezionata, la voce **Esci** è disponibile nel menu di scelta rapida dell'icona dell'applicazione. L'utente di un computer remoto può chiudere Kaspersky Endpoint Security nel computer remoto.

Se questa casella di controllo è deselezionata, la voce **Esci** non è disponibile nel menu di scelta rapida dell'icona dell'applicazione. L'utente di un computer remoto non può chiudere Kaspersky Endpoint Security nel computer remoto.

Questa casella di controllo è selezionata per impostazione predefinita.

Nella sezione **Eventi in Kaspersky Security Center** è possibile selezionare la lingua di visualizzazione per gli eventi di Kaspersky Endpoint Security in Kaspersky Security Center.

Lingua visualizzata

Da questo elenco a discesa è possibile selezionare la lingua di visualizzazione per gli eventi di Kaspersky Endpoint Security in Kaspersky Security Center.

Nella sezione **Restrizioni** è possibile abilitare la gestione locale delle chiavi e degli aggiornamenti di Kaspersky Endpoint Security in un computer remoto.

Consenti all'utente di gestire gli aggiornamenti in locale

Questa casella di controllo consente di abilitare o disabilitare la gestione locale degli aggiornamenti di Kaspersky Endpoint Security in un computer remoto.

Se questa casella di controllo è selezionata, la gestione locale degli aggiornamenti di Kaspersky Endpoint Security in un computer remoto è abilitata.

Se questa casella di controllo è deselezionata, gli aggiornamenti di Kaspersky Endpoint Security in un computer remoto possono essere gestiti solo tramite il plug-in di amministrazione di Kaspersky Endpoint Security in Kaspersky Security Center.

Questa casella di controllo è selezionata per impostazione predefinita.

Consenti all'utente di gestire le chiavi in locale

Questa casella di controllo consente di abilitare o disabilitare la gestione locale delle chiavi di Kaspersky Endpoint Security in un computer remoto.

Se la casella di controllo è selezionata, la gestione locale delle chiavi di Kaspersky Endpoint Security in un computer remoto è abilitata.

Se la casella di controllo è deselezionata, le chiavi di Kaspersky Endpoint Security in un computer remoto possono essere gestite solo tramite il plug-in di amministrazione di Kaspersky Endpoint Security in Kaspersky Security Center.

Questa casella di controllo è selezionata per impostazione predefinita.

Nella sezione **Protezione tramite password** è possibile impostare e configurare la password per limitare le azioni indesiderate sui dispositivi dell'utente.

Protezione tramite password

L'interruttore di **Protezione tramite password** consente di abilitare/disabilitare la protezione tramite password delle azioni indesiderate nei dispositivi degli utenti.

Se l'interruttore **Protezione tramite password** è attivato, è possibile impostare e configurare una password per limitare le azioni dell'utente nei dispositivi.

Se l'interruttore **Protezione tramite password** è disattivato, un utente può eseguire un'azione indesiderata senza immettere una password.

Questo interruttore è disattivato per impostazione predefinita.

Questo pulsante consente di aprire una finestra in cui è possibile configurare la password per limitare le azioni indesiderate nei dispositivi degli utenti.

Impostazioni

Questo pulsante consente di aprire una finestra in cui è possibile configurare la password per limitare le azioni indesiderate nei dispositivi degli utenti.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra Notifiche utente

Eventi

In questa colonna sono elencati gli eventi che possono verificarsi durante l'esecuzione di Kaspersky Endpoint Security:

- **Eventi critici**. Eventi di importanza critica in termini di protezione.
- **Errore funzionale**. Eventi che determinano problemi del sistema.
- **Eventi importanti**. Eventi a cui l'utente deve prestare attenzione.
- **Eventi informativi**. Eventi di natura informativa.

Notifiche

Una notifica è un messaggio pop-up che informa l'utente di un evento.

La casella di controllo nella colonna **Notifiche** consente di abilitare o disabilitare le notifiche pop-up sugli eventi di una determinata categoria.

Suono

Notifica acustica associata a un evento.

La casella di controllo nella colonna **Suono** consente di abilitare o disabilitare le notifiche acustiche per gli eventi di una determinata categoria.

Finestra "Area attendibile": sezione "File e cartelle"

Aggiungi

Questo pulsante apre una finestra di dialogo in cui è possibile aggiungere un file o una cartella all'area attendibile.

Elimina

Questo pulsante rimuove un file selezionato o una cartella selezionata dall'elenco delle esclusioni.

Questo pulsante è disponibile se la casella di controllo accanto al file o alla cartella è selezionata.

File o cartella

Questa colonna contiene file o cartelle aggiunti all'area attendibile.

Stato

L'interruttore in questa colonna consente di abilitare/disabilitare la scansione del file o della cartella aggiunti all'area attendibile.

Se l'interruttore è attivato, Kaspersky Endpoint Security non esamina il file o la cartella corrispondente.

Se l'interruttore è disattivato, Kaspersky Endpoint Security esamina il file o la cartella corrispondente.

Commento

Informazioni sul file aggiunto o sulla cartella aggiunta all'area attendibile.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra di dialogo "Aggiungi esclusione"

Campo di immissione Immettere un nome file, un nome cartella o una maschera

Percorso di un file o di una cartella oppure maschera per il file o la cartella da escludere dall'ambito della protezione.

Includi sottocartelle

Questa casella di controllo consente di abilitare o disabilitare la scansione delle sottocartelle della cartella specificata nel campo **Immettere un nome file, un nome cartella o una maschera**.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non esamina le sottocartelle della cartella specificata durante le scansioni anti-malware.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esclude solo i file che si trovano direttamente nella cartella specificata nel campo **Immettere un nome file, un nome cartella o una maschera** durante le scansioni anti-malware. Le sottocartelle della cartella specificata vengono esaminate.

Questa casella di controllo è selezionata per impostazione predefinita.

Nella sezione **Componenti** è possibile selezionare i componenti che non esamineranno il file specificato o la cartella specificata.

Qualsiasi

Né il componente Scansione né il componente Protezione Minacce File esamineranno il file specificato o la cartella specificata.

Dall'elenco

Questa opzione consente di selezionare i componenti.

Protezione minacce file

Se questa casella di controllo è selezionata, il componente Protezione Minacce File non esaminerà il file o la cartella specificati.

Questa casella di controllo è disponibile se l'opzione **Dall'elenco** è selezionata.

Scansione

Se questa casella di controllo è selezionata, il componente Scansione non esaminerà il file specificato o la cartella specificata.

Questa casella di controllo è disponibile se l'opzione **Dall'elenco** è selezionata.

Campo di immissione Commento

Informazioni sul file aggiunto o sulla cartella aggiunta all'area attendibile.

Nella sezione **Stato** è possibile selezionare se l'esclusione è attiva o meno.

Disabilitato

Kaspersky Endpoint Security esamina il file o la cartella corrispondenti.

Abilitato

Kaspersky Endpoint Security non esamina il file o la cartella corrispondenti.

Finestra "Area attendibile": sezione "Applicazioni attendibili"

Elenco delle applicazioni attendibili

Un elenco di applicazioni attendibili la cui attività di rete non verrà monitorata da Kaspersky Endpoint Security.

Aggiungi

Questo pulsante apre una finestra di dialogo in cui è possibile immettere il percorso di un'applicazione la cui attività di rete non verrà monitorata da Kaspersky Endpoint Security.

Elimina

Questo pulsante consente di rimuovere dall'elenco l'applicazione attendibile selezionata.

Questo pulsante è disponibile se la casella di controllo accanto all'applicazione attendibile è selezionata.

Applicazione

Questa colonna contiene il nome dell'applicazione o l'ultimo segmento del percorso di un'applicazione.

Stato

Questa colonna contiene un interruttore che indica lo stato del monitoraggio dell'attività della rete dell'applicazione.

Se lo stato è **Abilitato** l'attività della rete dell'applicazione corrispondente non viene monitorata da Kaspersky Endpoint Security.

Se lo stato è **Disabilitato** l'attività della rete dell'applicazione corrispondente viene monitorata da Kaspersky Endpoint Security.

Percorso

Questa colonna contiene il percorso dell'applicazione nel computer client, da aggiungere manualmente.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra di dialogo "Aggiungi applicazione"

Campo di immissione del percorso

Il percorso di un'applicazione il cui file o la cui attività di rete non verranno monitorati dall'applicazione Kaspersky Endpoint Security.

Requisito di firma del codice

Requisiti per la firma del codice dell'applicazione la cui attività non sarà monitorata da Kaspersky Endpoint Security.

Si tratta di un parametro facoltativo.

Opzioni

In questa sezione è possibile selezionare i tipi di attività che non si desidera vengano monitorati dall'applicazione Kaspersky Endpoint Security.

Non monitorare le attività sui file

Questa casella di controllo consente di abilitare/disabilitare il monitoraggio delle operazioni sui file di un'applicazione in un computer client.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non monitora l'attività dell'applicazione sui file.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security monitora l'attività dell'applicazione sui file.

Questa casella di controllo è selezionata per impostazione predefinita.

Non monitorare l'attività di rete

Questa casella di controllo consente di abilitare/disabilitare il monitoraggio del traffico Internet in entrata e in uscita dell'applicazione in un computer client.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non monitora l'attività di rete dell'applicazione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security monitora l'attività di rete dell'applicazione.

Questa casella di controllo è selezionata per impostazione predefinita.

Finestra Rete

Nella sezione **Impostazioni del server proxy** è possibile configurare l'utilizzo di un server proxy e le impostazioni da usare per la connessione a un server proxy.

Non usare un server proxy

Se questa opzione è selezionata, Kaspersky Endpoint Security non utilizza un server proxy per la connessione alle sorgenti degli aggiornamenti per i database e i moduli dell'applicazione.

Usa le impostazioni per il server proxy del sistema

Se questa opzione è selezionata, Kaspersky Endpoint Security si connette alle sorgenti degli aggiornamenti per i database e i moduli dell'applicazione utilizzando le impostazioni del server proxy configurate nel sistema operativo.

Questa opzione è selezionata per impostazione predefinita.

Usa le impostazioni per il server proxy specificate

Se questa opzione è selezionata, Kaspersky Endpoint Security si connette alle sorgenti degli aggiornamenti per i database e i moduli dell'applicazione utilizzando le impostazioni del server proxy specificate.

Indirizzo

Indirizzo IP o nome simbolico di un server proxy.

Il campo è disponibile se l'opzione **Usa le impostazioni per il server proxy specificate** è selezionata.

Porta

Numero di porta del server proxy.

Il numero di porta predefinito è 8080.

Il campo è disponibile se l'opzione **Usa le impostazioni per il server proxy specificate** è selezionata.

Usa autenticazione

Questa casella di controllo consente di abilitare o disabilitare l'utilizzo dell'autenticazione durante la connessione a un server proxy.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security richiede le credenziali dell'utente per la connessione a un server proxy.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security non richiede le credenziali dell'utente per la connessione a un server proxy.

Questa casella di controllo è selezionata per impostazione predefinita.

La casella di controllo è disponibile se l'opzione **Usa le impostazioni per il server proxy specificate** è selezionata.

Nome utente

Nome utente per la connessione al server proxy.

Il campo è disponibile se l'opzione **Usa le impostazioni per il server proxy specificate** e **Usa autenticazione** sono selezionate.

Password

Password per il nome utente specificato.

Il campo è disponibile se l'opzione **Usa le impostazioni per il server proxy specificate** e **Usa autenticazione** sono selezionate.

Mostra

Questo pulsante mostra i caratteri della password immessa nel campo **Password**.

Ignora il server proxy per gli indirizzi locali

Questa casella di controllo consente di abilitare o disabilitare l'utilizzo di un server proxy durante l'aggiornamento dei database e dei moduli dell'applicazione da una cartella locale o di rete.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non utilizza un server proxy durante l'aggiornamento dei database e dei moduli dell'applicazione da una cartella locale o di rete.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security utilizza un server proxy durante l'aggiornamento dei database e dei moduli dell'applicazione da una cartella locale o di rete.

Questa casella di controllo è selezionata per impostazione predefinita.

La casella di controllo è disponibile se l'opzione **Usa le impostazioni per il server proxy specificate** è selezionata.

Nella sezione **Controlla connessioni sicure** è possibile definire se Kaspersky Endpoint Security esamina le connessioni sicure (HTTPS).

Controllo connessioni sicure (HTTPS)

L'interruttore **Controllo connessioni sicure (HTTPS)** consente di abilitare o disabilitare la scansione delle connessioni sicure stabilite tramite il protocollo HTTPS e la visualizzazione delle notifiche quando Controllo Web blocca l'accesso dell'utente alle risorse Web pericolose.

Se l'interruttore **Controllo connessioni sicure (HTTPS)** è attivato, Kaspersky Endpoint Security esegue le seguenti operazioni:

- Protezione Minacce Web esamina i dati inviati e ricevuti dal computer tramite il protocollo HTTPS in Safari, Google Chrome o Firefox.
- L'applicazione visualizza notifiche quando l'utente accede alle risorse Web bloccate da Controllo Web nel computer remoto.

Se l'interruttore **Controllo connessioni sicure (HTTPS)** è disattivato, Kaspersky Endpoint Security esegue le seguenti operazioni:

- Protezione Minacce Web non esamina i dati inviati e ricevuti dal computer tramite il protocollo HTTPS.
- L'applicazione non visualizza notifiche quando l'utente accede alle risorse Web bloccate da Controllo Web nel computer remoto.

Questo interruttore è attivato per impostazione predefinita.

Nella sezione **Seleziona l'archivio certificati che Firefox deve utilizzare** è possibile selezionare l'archivio certificati per il controllo del traffico HTTPS criptato nel browser Mozilla Firefox.

Keychain System Roots (scelta consigliata)

Se questa opzione è selezionata, Kaspersky Endpoint Security utilizza un certificato radice dalla keychain System Roots per eseguire la verifica del traffico HTTPS criptato nel browser Mozilla Firefox.

Questa opzione è selezionata per impostazione predefinita.

Archivio certificati dalle impostazioni del browser Mozilla Firefox

Se questa opzione è selezionata, Kaspersky Endpoint Security utilizza il certificato dall'archivio certificati del browser.

In questo caso, è necessario aggiungere manualmente il certificato Kaspersky Endpoint Security all'archivio certificati del browser Mozilla Firefox. Per ulteriori informazioni, fare riferimento alla sezione Come aggiungere il certificato Kaspersky all'archivio dei certificati di Mozilla Firefox.

Nella sezione **Certificati radice attendibili** è possibile gestire l'elenco dei certificati radice attendibili.

Gestisci certificati radice attendibili

Questo collegamento consente di aprire una finestra in cui è possibile creare un elenco di certificati radice attendibili per stabilire la connessione ai server corrispondenti senza notifiche.

Nella sezione **Porte monitorate** è possibile configurare le porte monitorate da Kaspersky Endpoint Security.

Porte selezionate

Questo collegamento consente di aprire una finestra in cui è possibile configurare un elenco di porte monitorate da Kaspersky Endpoint Security.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra "Gestire i certificati radice attendibili"

Aggiungi

Questo pulsante consente di aprire una finestra di dialogo per l'aggiunta dei certificati che verranno considerati attendibili.

Elimina

Questo pulsante consente di rimuovere dall'elenco il certificato selezionato.

Elenco dei certificati attendibili

Un elenco che mostra i nomi dei certificati radice attendibili.

Per impostazione predefinita, l'elenco è vuoto.

Applica

Quando l'interruttore **Applica** è attivato, Kaspersky Endpoint Security impedisce la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Quando l'interruttore **Applica** è disattivato, Kaspersky Endpoint Security consente la modifica dei valori delle impostazioni dell'attività, delle impostazioni dell'applicazione, dei criteri dei sottogruppi e degli Administration Server secondari in un computer locale.

Finestra Porte monitorate

Elenco delle porte monitorate

Un elenco di porte per le quali è possibile configurare il monitoraggio dei dati trasmessi.

Per impostazione predefinita, l'elenco delle porte contiene le porte che vengono utilizzate di frequente dai servizi più comuni.

Aggiungi

Questo pulsante consente di aprire una finestra di dialogo in cui è possibile aggiungere una porta che si desidera venga monitorata da Kaspersky Endpoint Security.

Elimina

Questo pulsante consente di rimuovere dall'elenco la porta selezionata.

Questo pulsante è disponibile se la casella di controllo accanto alla porta è selezionata.

Porta

Questa colonna contiene i numeri delle porte.

Stato

Questa colonna contiene un interruttore che indica lo stato del monitoraggio dei dati trasmessi tramite la porta.

Se lo stato è **Monitorata**, il traffico trasmesso tramite la porta corrispondente viene esaminato da Kaspersky Endpoint Security.

Se lo stato è **Non monitorata**, il traffico trasmesso tramite la porta corrispondente non viene esaminato da Kaspersky Endpoint Security.

Descrizione

Questa colonna contiene una descrizione della porta.

Finestra di dialogo "Aggiungi porta"

Campo di immissione della porta

Il numero di una porta per la quale si desidera che Kaspersky Endpoint Security esamini i dati trasmessi.

Campo di immissione Descrizione

Informazioni aggiuntive sulla porta, ad esempio il tipo di porta.

Finestra "Informazioni sulla licenza"

Nella finestra **Informazioni sulla licenza** è possibile visualizzare le informazioni su una licenza, inclusa la data di scadenza, il numero di computer nei quali è possibile utilizzare Kaspersky Endpoint Security con la licenza e il tipo di licenza.

Aggiungi come chiave di riserva

Questa casella di controllo consente di abilitare o disabilitare l'aggiunta di uno specifico file chiave o codice di attivazione come chiave di riserva.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security aggiunge il file chiave o il codice di attivazione specificato come chiave di riserva.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security aggiunge il file chiave o il codice di attivazione specificato come chiave attiva.

Questa casella di controllo è deselezionata per impostazione predefinita.

Finestra "Scansione"

Ambito della scansione

Questo collegamento apre una finestra in cui è possibile creare l'ambito della scansione.

Nella sezione **Se viene rilevato un oggetto dannoso** è possibile selezionare l'azione che Kaspersky Endpoint Security deve eseguire al rilevamento di un oggetto infetto.

Richiedi all'utente di eseguire un'azione dopo la scansione

Kaspersky Endpoint Security non elabora gli oggetti fino al completamento della scansione. A questo punto, Kaspersky Endpoint Security visualizza una notifica con le informazioni su ciascun oggetto infetto e richiede all'utente di scegliere l'azione da eseguire. Le opzioni disponibili dipendono dal tipo di oggetto.

Questa opzione è selezionata per impostazione predefinita.

Richiedi all'utente di eseguire subito un'azione

Kaspersky Endpoint Security visualizza una notifica con le informazioni su ciascun oggetto infetto rilevato dall'applicazione e richiede all'utente di scegliere un'azione. Le opzioni disponibili dipendono dal tipo di oggetto.

Non richiedere l'intervento dell'utente

Kaspersky Endpoint Security registra le informazioni sugli oggetti rilevati nel rapporto senza elaborarle.

Disinfetta automaticamente

Questa casella di controllo consente di abilitare o disabilitare la disinfezione degli oggetti infetti rilevati da Kaspersky Endpoint Security senza chiedere conferma all'utente.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security disinfetta automaticamente gli oggetti infetti.

Se la casella di controllo è deselezionata, Kaspersky Endpoint Security ignora gli oggetti infetti.

La casella di controllo è disponibile se l'opzione **Non richiedere l'intervento dell'utente** è selezionata.

Questa casella di controllo è selezionata per impostazione predefinita.

Disinfetta (se la disinfezione non riesce, elimina)

Questa casella di controllo consente di abilitare o disabilitare la rimozione degli oggetti potenzialmente infetti dopo un tentativo di disinfezione non riuscito.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security elimina automaticamente gli oggetti infetti che non possono essere disinfettati.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security non rimuove gli oggetti infetti che non possono essere disinfettati.

Questa casella di controllo è visualizzata se l'opzione **Non richiedere l'intervento dell'utente** e la casella di controllo **Disinfetta automaticamente** sono selezionate.

Questa casella di controllo è selezionata per impostazione predefinita.

Nella sezione **Tipi di file** è possibile selezionare il formato dei file che devono essere esaminati da Kaspersky Endpoint Security.

Esamina tutti i file

Kaspersky Endpoint Security esamina tutti gli oggetti del file system eseguiti, aperti o salvati.

Esamina applicazioni e documenti in base al contenuto

Kaspersky Endpoint Security esamina solo gli oggetti potenzialmente infetti in base al formato dei file.

L'elenco dei formati di file è definito da Kaspersky ed è incluso nei database di Kaspersky Endpoint Security.

Esamina applicazioni e documenti in base all'estensione

Kaspersky Endpoint Security esamina solo gli oggetti potenzialmente infetti in base alla relativa estensione.

L'elenco delle estensioni di file è definito da Kaspersky ed è incluso nei database di Kaspersky Endpoint Security.

Kaspersky Endpoint Security esamina sempre i file senza estensioni.

Nella sezione **Ottimizzazione** è possibile configurare le prestazioni della scansione.

Esamina solo file nuovi e modificati

Questa casella di controllo consente di abilitare o disabilitare la scansione dei soli file riconosciuti da Kaspersky Endpoint Security come nuovi o modificati rispetto all'ultima scansione.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina solo i file che vengono riconosciuti come nuovi o modificati rispetto all'ultima scansione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esegue la scansione di tutti i file.

Ignora la scansione del volume di sistema di sola lettura

Questa casella di controllo consente di disabilitare/abilitare la scansione del volume di sistema di sola lettura da parte di Kaspersky Endpoint Security.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security non esamina il volume di sistema di sola lettura. Questo riduce notevolmente la durata scansione.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esamina il volume di sistema di sola lettura.

Questa casella di controllo è selezionata per impostazione predefinita.

Ignora file di dimensioni superiori a MB

Questa casella di controllo consente di abilitare o disabilitare l'esclusione dalla scansione dei file di dimensioni superiori alla dimensione specificata.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security ignora i file di dimensioni superiori alla dimensione specificata.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esegue la scansione dei file indipendentemente dalle relative dimensioni.

Questa casella di controllo è deselezionata per impostazione predefinita.

Per impostazione predefinita, la dimensione è 100 MB.

Ignora se la scansione impiega più di s

Questa casella di controllo consente di abilitare o disabilitare il limite per la durata delle scansioni dei file. Kaspersky Endpoint Security ignora un file se la relativa scansione supera il limite di tempo specificato.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security ignora un file se la relativa scansione supera il limite di tempo specificato.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esegue la scansione dei file indipendentemente dal tempo che può richiedere.

Il valore predefinito è 30 secondi.

Nella sezione **File compositi** è possibile selezionare i tipi di file compositi esaminati da Kaspersky Endpoint Security.

Esamina archivi

Questa casella di controllo consente di abilitare o disabilitare la scansione degli archivi.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina gli archivi.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security ignora gli archivi durante le scansioni.

Tutti

Kaspersky Endpoint Security esamina tutti gli archivi.

Questa opzione è disponibile se la casella di controllo **Esamina archivi** è selezionata.

Solo nuovi

Kaspersky Endpoint Security esamina solo i nuovi archivi.

Questa opzione è disponibile se la casella di controllo **Esamina archivi** è selezionata.

Esamina archivi protetti da password

Questa casella di controllo consente di abilitare o disabilitare la scansione degli archivi protetti da password.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina gli archivi protetti da password.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security ignora gli archivi protetti da password durante le scansioni.

Esamina oggetti OLE incorporati

Questa casella di controllo consente di abilitare o disabilitare la scansione degli oggetti incorporati in un file, ad esempio fogli di calcolo di Excel, macro o allegati e-mail.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina gli oggetti OLE incorporati.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security ignora gli oggetti OLE incorporati durante le scansioni.

Tutti

Kaspersky Endpoint Security esamina tutti gli oggetti OLE.

Questa opzione è disponibile se la casella di controllo **Esamina oggetti OLE incorporati** è selezionata.

Solo nuovi

Kaspersky Endpoint Security esamina solo i nuovi oggetti OLE incorporati.

Questa opzione è disponibile se la casella di controllo **Esamina oggetti OLE incorporati** è selezionata.

Esamina formati file e-mail

Questa casella di controllo consente di abilitare o disabilitare la scansione dei file nei formati e-mail e dei database e-mail.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esegue la scansione dei file nei formati e-mail e dei database e-mail.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security ignora i file nei formati e-mail e i database e-mail durante le scansioni.

Finestra Ambito della scansione

Aggiungi

Questo pulsante apre una finestra di dialogo in cui è possibile specificare un file, una cartella o una maschera per il file o la cartella da aggiungere all'ambito della scansione.

Elimina

Questo pulsante consente di rimuovere un oggetto dall'ambito della scansione.

Questo pulsante è disponibile se la casella di controllo accanto all'oggetto è selezionata.

Non è possibile eliminare gli oggetti predefiniti inclusi nell'ambito della scansione.

Ambito della scansione

Questa colonna contiene gli oggetti esaminati durante una scansione anti-malware.

Stato

L'interruttore in questa colonna consente di abilitare/disabilitare la scansione degli oggetti aggiunti all'ambito della scansione.

Se l'interruttore è attivato, Kaspersky Endpoint Security esamina l'oggetto corrispondente.

Se l'interruttore è disattivato, Kaspersky Endpoint Security non esamina l'oggetto corrispondente.

Avanzate

Questa colonna indica se Kaspersky Endpoint Security esamina le sottocartelle dell'oggetto corrispondente.

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Finestra di dialogo "Aggiungi ambito della scansione"

Immettere un nome file, un nome cartella o una maschera

Percorso di un file, di una cartella o maschera per file/cartelle.

L'oggetto è una cartella

Questa casella di controllo consente di abilitare o disabilitare la scansione di un oggetto come una cartella.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina l'oggetto specificato nel campo **Immettere un nome file, un nome cartella o una maschera** come una cartella.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esamina l'oggetto specificato nel campo **Immettere un nome file, un nome cartella o una maschera** come un file.

Questa casella di controllo è selezionata per impostazione predefinita.

Includi sottocartelle

Questa casella di controllo consente di abilitare o disabilitare la scansione delle sottocartelle della cartella specificata nel campo **Immettere un nome file, un nome cartella o una maschera**.

Se questa casella di controllo è selezionata, Kaspersky Endpoint Security esamina le sottocartelle durante le scansioni anti-malware.

Se questa casella di controllo è deselezionata, Kaspersky Endpoint Security esamina solo i file che si trovano direttamente nella cartella specificata nel campo **Immettere un nome file, un nome cartella o una maschera** durante le scansioni anti-malware.

Questa casella di controllo è selezionata per impostazione predefinita.

Nota: Kaspersky Endpoint Security non esegue la scansione dei file che si trovano nell'archivio OneDrive o iCloud o in altri archivi cloud. Escludere questi file dall'ambito della scansione. In caso contrario, l'attività di scansione potrebbe terminare con l'errore *File infetto non eliminato*.

Finestra Parametri file

Sono supportati i seguenti tipi di hash del file:

- **MD5**

  Un hash di questo tipo deve avere una lunghezza di 32 caratteri e contenere 0-9, af, AF.

- **SHA256**

  Un hash di questo tipo deve avere una lunghezza di 64 caratteri e contenere 0-9, af, AF.