kaspersky

Kaspersky Security Center Cloud Console

Sommario

Guida di Kaspersky Security Center Cloud Console

Novità Informazioni sulle novità della versione più recente dell'applicazione.	**Configurazione della protezione di rete** Gestire la sicurezza di un'organizzazione configurando le attività e i criteri dell'applicazione Kaspersky in conformità con i requisiti dell'organizzazione.
Requisiti hardware e software Controllare i sistemi operativi e le versioni delle applicazioni supportati.	**Applicazioni Kaspersky: aggiornamento periodico dei database e dei moduli del software** Gestire l'affidabilità del sistema di protezione.
Licensing di Kaspersky Security Center Cloud Console Informazioni sul funzionamento di Kaspersky Security Center Cloud Console in modalità di prova e in modalità commerciale.	**Monitoraggio e generazione di rapporti** Visualizzare l'infrastruttura, gli stati di protezione dei dispositivi di rete e le statistiche per gestire l'attuale stato di protezione dell'organizzazione. È possibile utilizzare anche i rapporti.
Configurazione iniziale Iniziare a utilizzare l'area di lavoro, configurare Kaspersky Security Center Cloud Console in base alle proprie esigenze.	**Vulnerability e patch management** Individuare e correggere le vulnerabilità nel software di terze parti.
Migrazione a Kaspersky Security Center Cloud Console Migrare i gruppi di amministrazione esistenti e gli oggetti correlati da Kaspersky Security Center in locale a Kaspersky Security Center Cloud Console.	**Esportazione di eventi nei sistemi SIEM** Configurare l'esportazione degli eventi nei sistemi SIEM utilizzando il protocollo Syslog.
Individuazione dei dispositivi nella rete Individuare i dispositivi nuovi ed esistenti nella rete dell'organizzazione.	**Utilizzo di un ambiente cloud** Proteggere le macchine virtuali negli ambienti cloud: Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.
Regolazione di punti di distribuzione e/o gateway di connessione Configurare i punti di distribuzione.	**Guida introduttiva per MSP (Managed Service Providers)** Ecco come utilizzare Kaspersky Security Center Cloud Console se si è un amministratore di MSP.
Applicazioni Kaspersky: distribuzione centralizzata Distribuire applicazioni Kaspersky.	

Novità

Aggiornamento aprile 2024

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Una nuova funzionalità di Cloud Discovery. Questa funzionalità consente di monitorare l'utilizzo dei servizi cloud nei dispositivi gestiti in cui viene eseguito Windows e di bloccare l'accesso ai servizi cloud considerati indesiderati. Cloud Discovery monitora i tentativi da parte degli utenti di ottenere l'accesso a questi servizi tramite i browser e le applicazioni desktop.

Aggiornamento febbraio 2024

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Nell'elenco dei dispositivi gestiti, è ora possibile selezionare uno o più dispositivi, quindi assegnare un'attività esistente da eseguire nei dispositivi selezionati. L'ambito del dispositivo corrente dell'attività verrà sostituito con i dispositivi selezionati.
- È ora possibile assegnare tag a più dispositivi o rimuovere i tag da più dispositivi contemporaneamente. Nell'elenco dei dispositivi gestiti, selezionare i dispositivi, quindi specificare i tag che si desidera assegnare o rimuovere dai dispositivi selezionati.
- Aspetto ed esperienza utente ottimizzati dell'elenco dei dispositivi gestiti. Aggiunta una nuova colonna **Tag** e la possibilità di filtrare i dispositivi in base ai tag assegnati ai dispositivi.

Aggiornamento gennaio 2024

Kaspersky Security Center Cloud Console ora supporta Kaspersky Endpoint Security 12.4 for Windows.

Aggiornamento dicembre 2023

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- È ora possibile verificare la connessione a un sistema SIEM.
- Kaspersky Security Center Cloud Console ora supporta il polling di un controller di dominio Microsoft Active Directory e di un controller di dominio Samba tramite un punto di distribuzione basato su Linux.
- Diagnostica remota dei dispositivi gestiti basati su Linux.
- Kaspersky Security Center Cloud Console adesso supporta le seguenti applicazioni Kaspersky:
  - Kaspersky Endpoint Security for Windows versione 12.3 Patch A
  - Kaspersky Endpoint Security 12.0 for Linux
  - Kaspersky Endpoint Security 12.0 for Mac

- Kaspersky Endpoint Agent 3.16
- Kaspersky Embedded Systems Security 3.3 for Windows

- Due sezioni dell'interfaccia sono state nascoste dal menu principale perché fuori dall'ambito della funzionalità dell'applicazione:
  - Eventi di criptaggio (**Operazioni** → **Criptaggio e protezione dei dati** → **Eventi di criptaggio**)
  - Intervalli IP (**Individuazione e distribuzione** → **Individuazione** → **Intervalli IP**)
- È stato aggiornato il testo dell'Accordo di elaborazione dei dati di Kaspersky Security Center Cloud Console.
- Diverse versioni obsolete dei browser non sono più supportate (versioni di Firefox ESR precedenti alla 102).

Aggiornamento settembre 2023

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Kaspersky Security Center Cloud Console ora supporta Kaspersky Embedded Systems Security 3.3 for Linux.
- Kaspersky Security Center Cloud Console ora supporta Kaspersky Endpoint Security 12.2 for Windows.
- Ottimizzazione dell'interfaccia utente quando si lavora con l'elenco utenti nella sezione **Risorse (dispositivi)**.

Aggiornamento giugno 2023

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- È stata rilasciata una nuova Guida di protezione avanzata. Si consiglia vivamente di leggere attentamente la guida e di seguire i suggerimenti di sicurezza per configurare Kaspersky Security Center Cloud Console e l'infrastruttura di rete.
- Kaspersky Security Center Cloud Console ora supporta Kaspersky Endpoint Security 11.3 for Mac.
- Kaspersky Security Center Cloud Console ora supporta Kaspersky Endpoint Security 11.4 for Linux.
- È possibile utilizzare Kaspersky Security Center Cloud Console per esportare le selezioni di eventi in un file, e quindi importare le selezioni di eventi in Kaspersky Security Center Windows o Kaspersky Security Center Linux.
- È ora possibile utilizzare un punto di distribuzione come server push per i dispositivi gestiti da Network Agent. Questa funzionalità consente di assicurarsi che sia stata stabilita una connettività costante tra un dispositivo gestito e l'Administration Server.
- Riorganizzazione della sezione con le impostazioni per integrare Kaspersky Security Center Cloud Console con altre applicazioni Kaspersky.
- Riorganizzazione dell'interfaccia utente della sezione **Diagnostica remota**.
- Ora è possibile salvare contemporaneamente le informazioni su tutti i dispositivi inclusi in una selezione di dispositivi in un file CSV.

- Una serie di miglioramenti nell'interfaccia utente e nell'usabilità, inclusa la possibilità di selezionare tutti gli elementi in una tabella.

Aggiornamento marzo 2023

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Kaspersky Security Center Cloud Console ora supporta cluster e array di server come dispositivi gestiti. Se un'applicazione Kaspersky è installata in un nodo del cluster, Network Agent invia queste informazioni ad Administration Server. In Web Console, i cluster e gli array di server sono elencati separatamente dagli altri dispositivi gestiti. Ogni cluster o array di server viene gestito come un singolo oggetto inseparabile.

- Kaspersky Security Center Cloud Console ora supporta Kaspersky Endpoint Security 12.0 for Windows.

- Il numero massimo di voci che un rapporto può includere è stato aumentato fino a 2500 per un rapporto in Web Console e fino a 10.000 per un rapporto esportato in un file.

- Ora è possibile scegliere se includere o meno i dispositivi gestiti con lo stato *OK* nel rapporto sullo stato della protezione.

- È ora possibile attivare Kaspersky Security Center Cloud Console utilizzando una delle seguenti licenze o aggiungere le chiavi delle licenze elencate a un'area di lavoro esistente:

  - Kaspersky Symphony Security

  - Kaspersky Symphony EDR

  - Kaspersky Symphony MDR

  - Kaspersky Symphony XDR

- È stata rilasciata un'edizione speciale di Network Agent per Windows XP.

- Il Network Agent per Linux aggiornato supporta il servizio proxy KSN. Oltre ai punti di distribuzione basati su Windows, è ora possibile utilizzare i punti di distribuzione basati su Linux per inoltrare le richieste di Kaspersky Security Network (KSN) dai dispositivi gestiti. Questa funzionalità consente di ridistribuire e ottimizzare il traffico nella rete.

- Il Network Agent per Linux aggiornato supporta la funzionalità del registro delle applicazioni. Network Agent può compilare un elenco delle applicazioni installate in un dispositivo gestito basato su Linux, quindi trasmette questo elenco ad Administration Server.

- È possibile utilizzare Kaspersky Security Center Cloud Console per esportare criteri e attività in un file, e quindi importare i criteri e le attività in Kaspersky Security Center Windows o Kaspersky Security Center Linux.

Aggiornamento novembre 2022

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Kaspersky Security Center Cloud Console ora supporta Kaspersky Endpoint Security 11.3 for Linux.

- Kaspersky Security Center Cloud Console adesso supporta Kaspersky Managed Detection and Response 2.1.18.

- Kaspersky Security Center Cloud Console ora supporta le versioni aggiornate di Kaspersky Endpoint Security for Mac 11.2 e 11.2.1, per supportare macOS 13.
- I video nella sezione **Presentazione e tutorial** sono stati aggiornati.

Aggiornamento ottobre 2022

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- È stato aggiornato il testo dell'Accordo di elaborazione dei dati di Kaspersky Security Center Cloud Console.
- L'infrastruttura di Kaspersky Security Center Cloud Console ora avvisa se un'area di lavoro non dispone di una chiave di licenza attiva e potrebbe essere eliminata se non si aggiunge una nuova chiave di licenza.
- Kaspersky Security Center Cloud Console ora supporta Kaspersky Endpoint Security 11.11.0 for Windows.
- Kaspersky Security Center Cloud Console adesso supporta Kaspersky Endpoint Detection and Response Optimum 2.3.
- Kaspersky Embedded Systems Security 3.2 for Windows è supportato.

Aggiornamento settembre 2022

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Adesso è possibile assegnare amministratori dedicati per Administration Server virtuali. Creare un account utente per un amministratore, quindi concedere all'amministratore i diritti di accesso a un Administration Server virtuale. L'amministratore assegnato ha accesso solo all'Administration Server virtuale selezionato e non può connettersi all'Administration Server primario o ad altri Administration Server secondari, fisici o virtuali.
- Esperienza utente ottimizzata quando si elimina una chiave di licenza per Kaspersky Security Center Cloud Console. Il nuovo meccanismo impedisce di eliminare accidentalmente l'ultima chiave di licenza attiva.
- Adesso è possibile utilizzare i punti di distribuzione basati su Linux per scaricare i database anti-virus per le applicazioni di protezione Kaspersky tramite l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.
- Network Agent adesso è disponibile nella localizzazione giapponese.
- Nell'interfaccia di Kaspersky Security Center Cloud Console anziché usare lo stile "tutte maiuscole" nei nomi delle sezioni, adesso viene riportata in maiuscolo solo la prima parola di ogni frase.

Aggiornamento agosto 2022

Nuova lingua supportata: Kaspersky Security Center Cloud Console è completamente disponibile in lingua giapponese.

Aggiornamento di luglio 2022

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Nuove versioni delle applicazioni Kaspersky supportate:
  - Kaspersky Endpoint Agent 3.13
  - Kaspersky Endpoint Security 11.2.1 for Mac
  - Kaspersky Security for iOS 1.0.0
  - Kaspersky Endpoint Security 11.10.0 for Windows
- È stato aggiornato il testo del Contratto e dell'Accordo di elaborazione dei dati per Kaspersky Security Center Cloud Console.
- Nuova lingua supportata: l'infrastruttura Kaspersky Security Center Cloud Console è ora disponibile in giapponese. Il supporto della lingua giapponese all'interno delle aree di lavoro di Kaspersky Security Center Cloud Console sarà presto disponibile.

Aggiornamento aprile 2022

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Kaspersky Security Center Cloud Console ora supporta Kaspersky Endpoint Security 11.9.0 for Windows.
- Kaspersky Security Center Cloud Console adesso supporta la localizzazione giapponese di Kaspersky Embedded Systems Security.

Aggiornamento 9 marzo 2022

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- È stata implementata l'integrazione con Kaspersky Endpoint Detection and Response Expert.
- È stata implementata la piattaforma IRP (Incident Response Platform). Adesso è possibile gestire gli incidenti di sicurezza tramite Kaspersky Security Center Cloud Console.
- Kaspersky Security Center Cloud Console ora accetta chiavi di licenza per Kaspersky Endpoint Detection and Response Expert. Il numero minimo di dispositivi per la licenza è 50.

Aggiornamento dell'11 febbraio

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Adesso sono supportate le licenze per Kaspersky Embedded Systems Security for Windows.
- Kaspersky Endpoint Security 11.8.0 for Windows è supportato.

- È possibile installare Kaspersky Endpoint Security 11.8.0 for Windows utilizzando un pacchetto di distribuzione in giapponese.
- È supportato Kaspersky Endpoint Agent 3.12.

Aggiornamento del 10 dicembre 2021

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- L'utilizzo da parte degli utenti interni è stato ottimizzato:
  - Adesso è possibile aggiungere nuovi utenti interni nel portale.
  - Adesso l'applicazione impedisce di ridurre i propri diritti.

Ultimo aggiornamento: 18 ottobre 2021

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Kaspersky Security Center Cloud Console adesso supporta Kaspersky Endpoint Detection and Response Optimum 2.0.
- Adesso è possibile gestire i dispositivi mobili che eseguono Android tramite Kaspersky Security Center Cloud Console.
- Kaspersky Marketplace è disponibile come nuova sezione del menu: è possibile cercare un'applicazione Kaspersky tramite Kaspersky Security Center Cloud Console.
- È disponibile una nuova sezione del menu: Annunci Kaspersky. Gli annunci Kaspersky tengono informati gli utenti fornendo informazioni relative alle applicazioni Kaspersky installate nei dispositivi gestiti. Kaspersky Security Center Cloud Console aggiorna periodicamente le informazioni nella sezione.
- Adesso è possibile gestire gli Administration Server secondari con sistemi operativi Linux tramite Kaspersky Security Center Cloud Console.

Ultimo aggiornamento: 07 settembre 2021

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Adesso è possibile utilizzare Active Directory Federation Services (ADFS) per accedere a Kaspersky Security Center Cloud Console utilizzando l'account Active Directory, senza creare un nuovo account utente.
- Kaspersky Security Center Cloud Console adesso è compatibile con i seguenti ambienti cloud: Amazon Web Services, Microsoft Azure e Google Cloud. Per proteggere le macchine virtuali (o istanze) in un ambiente cloud, è necessaria una delle licenze Kaspersky Hybrid Cloud Security. La Configurazione guidata ambiente cloud è disponibile.
- Il numero massimo di dispositivi per ogni area di lavoro adesso è 25.000.

- L'integrazione con i sistemi SIEM adesso è disponibile in Kaspersky Security Center Cloud Console. È possibile esportare eventi nei sistemi SIEM utilizzando il protocollo Syslog.

- Adesso è possibile creare Administration Server virtuali. Ogni Administration Server virtuale può avere la propria struttura di gruppi di amministrazione, criteri, attività, rapporti ed eventi. È possibile utilizzare Administration Server virtuali per la gestione di organizzazioni client con flussi di lavoro complessi all'interno dell'area di lavoro. Tuttavia, non è possibile eseguire la migrazione di Administration Server virtuali da Kaspersky Security Center in esecuzione in locale a Kaspersky Security Center Cloud Console.

- Adesso è possibile regolare la larghezza delle colonne nelle tabelle, ordinare e cercare i dati.

- È stata migliorata la stabilità e la disponibilità di Kaspersky Business Hub e Kaspersky Security Center Cloud Console.

Ultimo aggiornamento: 27 ottobre 2020

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Kaspersky Security Center Cloud Console adesso supporta Kaspersky Endpoint Security 11.6.0 for Windows, Kaspersky Endpoint Security 11.1 for Mac Patch A e Kaspersky Endpoint Agent 3.10 (nell'ambito di Kaspersky Endpoint Detection and Response Optimum).

- Ora è possibile utilizzare le seguenti licenze:

  - Kaspersky Endpoint Detection and Response Optimum

  - Kaspersky Endpoint Security for Business Advanced

  - Kaspersky Total Security for Business

- Vengono implementate le seguenti funzionalità:

  - Vulnerability e Patch Management

  - Gestione criptaggio

  - Controllo Applicazioni

  - Controllo adattivo delle anomalie

  - Sessioni RDP, inclusa Condivisione desktop Windows

- Il menu di navigazione adesso è verticale e ricorda l'interfaccia basata su Microsoft Management Console di Kaspersky Security Center Cloud Console.

- Sono ora disponibili video di formazione tecnica che aiuteranno a comprendere come funziona l'applicazione.

Ultimo aggiornamento: 30 giugno 2020

Questo aggiornamento di Kaspersky Security Center Cloud Console include le nuove funzionalità e i miglioramenti illustrati di seguito:

- Kaspersky Security Center Cloud Console ora supporta Kaspersky Security 11 for Windows Server (a partire da settembre 2020).
- Kaspersky Security Center Cloud Console ora supporta Kaspersky Endpoint Agent 3.9 e Kaspersky Endpoint Security 11.4.0 for Windows.
- L'Avvio rapido guidato è stato migliorato: alcuni passaggi sono stati rimossi, la sequenza dei passaggi è stata leggermente modificata e alcuni testi sono stati modificati per una maggiore facilità di utilizzo.
- Kaspersky Security Center Cloud Console è ora disponibile in italiano.
- Adesso è possibile revocare il Contratto di licenza con l'utente finale (EULA) per qualsiasi applicazione Kaspersky gestita tramite l'interfaccia di Kaspersky Security Center Cloud Console. È necessario disinstallare l'applicazione selezionata prima di revocarne il Contratto di licenza con l'utente finale.
- Adesso è possibile eliminare le aree di lavoro. Se si contrassegna un'area di lavoro per l'eliminazione, per impostazione predefinita questa viene automaticamente eliminata entro sette giorni. È tuttavia possibile forzare l'eliminazione dell'area di lavoro, in modo che venga eliminata immediatamente.
- È stata implementata la verifica in due passaggi per l'accesso alla console.

Kaspersky Security Center Cloud Console

Questa sezione contiene informazioni sulla funzione di Kaspersky Security Center Cloud Console, nonché sui relativi componenti e funzionalità principali.

Kaspersky Security Center Cloud Console è un'applicazione ospitata e gestita da Kaspersky. Non è necessario installare Kaspersky Security Center Cloud Console nel computer o nel server. Kaspersky Security Center Cloud Console consente all'amministratore di installare le applicazioni di protezione Kaspersky nei dispositivi in una rete aziendale, eseguire in remoto attività di scansione e aggiornamento e gestire i criteri di sicurezza delle applicazioni gestite. L'amministratore può utilizzare una dashboard dettagliata che fornisce una panoramica degli stati dei dispositivi aziendali, rapporti dettagliati e impostazioni granulari nei criteri di protezione.

Informazioni di Kaspersky Security Center Cloud Console

L'applicazione Kaspersky Security Center Cloud Console è destinata agli amministratori di reti aziendali e ai dipendenti responsabili della protezione dei dispositivi in un'ampia gamma di organizzazioni.

Kaspersky Security Center Cloud Console consente di eseguire le seguenti operazioni:

- Installare le applicazioni Kaspersky nei dispositivi della rete e gestire le applicazioni installate.
- Creare una gerarchia di gruppi di amministrazione per gestire una selezione di dispositivi client come una singola unità.
- Creare Administration Server virtuali e disporli in una gerarchia.
- Proteggere i dispositivi della rete, inclusi workstation e server:
  - Gestire un sistema di protezione anti-malware basato sulle applicazioni Kaspersky.
  - Utilizzare le funzionalità di rilevamento e risposta EDR e MDR (è necessaria una licenza per Kaspersky Endpoint Detection and Response e/o per Kaspersky Managed Detection and Response), tra cui:
    - Analisi e ricerca degli incidenti
    - Visualizzazione degli incidenti attraverso la creazione di un grafico della catena di sviluppo delle minacce
    - Accettazione o rifiuto manuale delle risposte o impostazione dell'accettazione automatica di tutte le risposte
- Utilizzare Kaspersky Security Center Cloud Console come applicazione multi-tenant.
- Gestire in remoto le applicazioni Kaspersky installate nei dispositivi client.
- Eseguire la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi client.
- Creare e gestire criteri di protezione per i dispositivi nella rete.
- Creare e gestire account utente.
- Creare e gestire ruoli utente (RBAC).
- Creare e gestire attività per le applicazioni installate nei dispositivi della rete.

- Visualizzare i rapporti sullo stato del sistema di sicurezza singolarmente per ogni organizzazione client.

È possibile gestire Kaspersky Security Center Cloud Console utilizzando un'Administration Console basata sul cloud che garantisce l'interazione tra il dispositivo e Administration Server tramite un browser. Administration Server è un'applicazione progettata per la gestione delle applicazioni Kaspersky installate nei dispositivi della rete. Quando si esegue la connessione a Kaspersky Security Center Cloud Console utilizzando il browser, questo stabilisce una connessione con Kaspersky Security Center Cloud Console Server.

L'Administration Server e il DBMS connesso sono distribuiti in un ambiente cloud e forniti come servizio. La manutenzione di Administration Server e del DBMS è garantita nell'ambito del servizio. Tutti i componenti software di Kaspersky Security Center Cloud Console vengono mantenuti aggiornati. L'Administration Server e gli oggetti creati (come criteri e attività) vengono sottoposti periodicamente a backup per motivi di sicurezza.

Kaspersky Security Center Cloud Console è un'applicazione multilingue. È possibile modificare la lingua dell'interfaccia in qualsiasi momento, senza riaprire l'applicazione.

Requisiti hardware e software per Kaspersky Security Center Cloud Console

Administration Console

Per un client, l'utilizzo di Kaspersky Security Center Cloud Console richiede solo un browser.

> È sufficiente utilizzare una singola finestra o scheda del browser per utilizzare Kaspersky Security Center Cloud Console.

I requisiti hardware e software relativi al dispositivo sono identici a quelli del browser utilizzato per Kaspersky Security Center Cloud Console.

Browser:

- Google Chrome versione 100.0.4896.88 o successiva (build ufficiale)
- Microsoft Edge versione 100 o successiva
- Safari 15 su macOS
- "Yandex" Browser 23.5.0.2271
- Mozilla Firefox Extended Support Release 102.0 o versione successiva

Network Agent

Requisiti hardware minimi:

- CPU con frequenza operativa di 1 GHz o superiore. Per un sistema operativo a 64 bit, la frequenza minima della CPU è di 1.4 GHz.
- RAM: 512 MB.
- Spazio disponibile su disco: 1 GB.

Requisiti hardware minimi per Vulnerability e Patch Management:

- CPU con frequenza operativa di 1.4 GHz o superiore. È richiesto un sistema operativo a 64 bit.
- RAM: 8 GB.
- Spazio disponibile su disco: 1 GB.

Sistemi operativi supportati da Network Agent

Sistemi operativi. Microsoft Windows	Microsoft Windows Embedded POSReady 2009 con il Service Pack più recente 32 bit Microsoft Windows Embedded 7 Standard con Service Pack 1 32 bit/64 bit Microsoft Windows Embedded 8.1 Industry Pro 32 bit/64 bit Microsoft Windows 10 Enterprise 2015 LTSB 32 bit/64 bit Microsoft Windows 10 Enterprise 2016 LTSB 32 bit/64 bit Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-bit/64 bit Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-bit/64 bit Microsoft Windows 10 Enterprise 2019 LTSC 32 bit/64 bit Microsoft Windows 10 IoT Enterprise versione 1703 32 bit/64 bit Microsoft Windows 10 IoT Enterprise versione 1709 32 bit/64 bit Microsoft Windows 10 IoT Enterprise versione 1803 32 bit/64 bit Microsoft Windows 10 IoT Enterprise versione 1809 32 bit/64 bit Microsoft Windows 10 20H2 IoT Enterprise 32 bit/64 bit Microsoft Windows 10 21H2 IoT Enterprise 32 bit/64 bit Microsoft Windows 10 IoT Enterprise 32 bit/64 bit Microsoft Windows 10 IoT Enterprise versione 1909 32 bit/64 bit Microsoft Windows 10 IoT Enterprise LTSC 2021 32 bit/64 bit Microsoft Windows 10 IoT Enterprise versione 1607 32 bit/64 bit Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32 bit/64 bit Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32 bit/64 bit Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32 bit/64 bit Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32 bit/64 bit Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32 bit/64 bit Microsoft Windows 10 Home RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit Microsoft Windows 10 Pro RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit Microsoft Windows 10 Pro for Workstations RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit Microsoft Windows 10 Enterprise RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit Microsoft Windows 10 Education RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit Microsoft Windows 10 Home RS5 (ottobre 2018) 32 bit/64 bit

Microsoft Windows 10 Pro RS5 (ottobre 2018) 32 bit/64 bit

Microsoft Windows 10 Pro for Workstations RS5 (ottobre 2018) 32 bit/64 bit

Microsoft Windows 10 Enterprise RS5 (ottobre 2018) 32 bit/64 bit

Microsoft Windows 10 Education RS5 (ottobre 2018) 32 bit/64 bit

Microsoft Windows 10 Home 19H1 32 bit/64 bit

Microsoft Windows 10 Pro 19H1 32 bit/64 bit

Microsoft Windows 10 Pro for Workstations 19H1 32 bit/64 bit

Microsoft Windows 10 Enterprise 19H1 32 bit/64 bit

Microsoft Windows 10 Education 19H1 32 bit/64 bit

Microsoft Windows 10 Home 19H2 32 bit/64 bit

Microsoft Windows 10 Pro 19H2 32 bit/64 bit

Microsoft Windows 10 Pro for Workstations 19H2 32 bit/64 bit

Microsoft Windows 10 Enterprise 19H2 32 bit/64 bit

Microsoft Windows 10 Education 19H2 32 bit/64 bit

Microsoft Windows 10 Home 20H1 (aggiornamento di maggio 2020) 32 bit/64 bit

Microsoft Windows 10 Pro 20H1 (aggiornamento di maggio 2020) 32 bit/64 bit

Microsoft Windows 10 Enterprise 20H1 (aggiornamento di maggio 2020) 32 bit/64 bit

Microsoft Windows 10 Education 20H1 (aggiornamento di maggio 2020) 32 bit/64 bit

Microsoft Windows 10 Home 20H2 (aggiornamento di ottobre 2020) 32 bit/64 bit

Microsoft Windows 10 Pro 20H2 (aggiornamento di ottobre 2020) 32 bit/64 bit

Microsoft Windows 10 Enterprise 20H2 (aggiornamento di ottobre 2020) 32 bit/64 bit

Microsoft Windows 10 Education 20H2 (aggiornamento di ottobre 2020) 32 bit/64 bit

Microsoft Windows 10 Home 21H1 (aggiornamento di maggio 2021) 32 bit/64 bit

Microsoft Windows 10 Pro 21H1 (aggiornamento di maggio 2021) 32 bit/64 bit

Microsoft Windows 10 Enterprise 21H1 (aggiornamento di maggio 2021) 32 bit/64 bit

Microsoft Windows 10 Education 21H1 (aggiornamento di maggio 2021) 32 bit/64 bit

Microsoft Windows 10 Home 21H2 (aggiornamento di ottobre 2021) 32 bit / 64 bit

Microsoft Windows 10 Pro 21H2 (aggiornamento di ottobre 2021) 32 bit / 64 bit

Microsoft Windows 10 Enterprise 21H2 (aggiornamento di ottobre 2021) 32 bit / 64 bit

Microsoft Windows 10 Education 21H2 (aggiornamento di ottobre 2021) 32 bit / 64 bit

Microsoft Windows 10 Home 22H2 (aggiornamento di ottobre 2023) 32 bit/64 bit

Microsoft Windows 10 Pro 22H2 (aggiornamento di ottobre 2023) 32 bit/64 bit

Microsoft Windows 10 Enterprise 22H2 (aggiornamento di ottobre 2023) 32 bit/64 bit

Microsoft Windows 10 Education 22H2 (aggiornamento di ottobre 2023) 32 bit/64 bit

Microsoft Windows 11 Home 64 bit

Microsoft Windows 11 Pro 64 bit

Microsoft Windows 11 Enterprise 64 bit

Microsoft Windows 11 Education 64 bit

Microsoft Windows 11 22H2

Microsoft Windows 8.1 Pro 32 bit/64 bit

Microsoft Windows 8.1 Enterprise 32 bit/64 bit

Microsoft Windows 8 Pro 32 bit/64 bit

Microsoft Windows 8 Enterprise 32 bit/64 bit

Microsoft Windows 7 Professional con Service Pack 1 e versioni successive 32 bit/64 bit

Microsoft Windows 7 Enterprise / Ultimate con Service Pack 1 e versioni successive 32 bit/64 bit

Microsoft Windows 7 Home Basic/Premium con Service Pack 1 e versioni successive 32 bit/64 bit

Microsoft Windows XP Professional Service Pack 3 e versioni successive 32 bit

Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32 bit

Windows MultiPoint Server 2011 Standard/Premium 64 bit

Windows Server 2008 Foundation con Service Pack 2 32 bit/64 bit

Windows Server 2008 Service Pack 2 (tutte le edizioni) 32 bit/64 bit

Windows Server 2008 R2 Datacenter Service Pack 1 e versioni successive 64 bit

Windows Server 2008 R2 Enterprise Service Pack 1 e versioni successive 64 bit

Windows Server 2008 R2 Foundation con Service Pack 1 e versioni successive 64 bit

Windows Server 2008 R2 Core Mode Service Pack 1 e versioni successive 64 bit

Windows Server 2008 R2 Standard Service Pack 1 e versioni successive 64 bit

Windows Server 2008 R2 Service Pack 1 (tutte le edizioni) 64 bit

Windows Server 2012 Server Core 64 bit

Windows Server 2012 Datacenter 64 bit

Windows Server 2012 Essentials 64 bit

Windows Server 2012 Foundation 64 bit

Windows Server 2012 Standard 64 bit

Windows Server 2012 R2 Server Core 64 bit

Windows Server 2012 R2 Datacenter 64 bit

	Windows Server 2012 R2 Essentials 64 bit Windows Server 2012 R2 Foundation 64 bit Windows Server 2012 R2 Standard 64 bit Windows Server 2016 Datacenter (LTSB) 64 bit Windows Server 2016 Standard (LTSB) 64 bit Windows Server 2016 Server Core (Installation Option) (LTSB) 64 bit Windows Server 2019 Standard 64 bit Windows Server 2019 Datacenter 64 bit Windows Server 2019 Core 64 bit Windows Server 2022 Standard 64 bit Windows Server 2022 Datacenter 64 bit Windows Server 2022 Core 64 bit
Sistemi operativi. Linux	Debian GNU/Linux 12 (Bookworm) Debian GNU/Linux 11.x (Bullseye) 32 bit/64 bit Debian GNU/Linux 10.x (Buster) 32 bit / 64 bit Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bit Ubuntu Server 20.04 LTS (Focal Fossa) 32 bit/64 bit Ubuntu Server 18.04 LTS (Bionic Beaver) 32 bit/64 bit CentOS Stream 9 64 bit CentOS 7.x 64 bit Red Hat Enterprise Linux Server 9.x 64 bit Red Hat Enterprise Linux Server 8.x 64 bit Red Hat Enterprise Linux Server 7.x 64 bit Red Hat Enterprise Linux Server 6.x 32 bit/64 bit SUSE Linux Enterprise Server 12 (tutti i Service Pack) 64 bit SUSE Linux Enterprise Server 15 (tutti i Service Pack) 64 bit openSUSE 15 64 bit Oracle Linux 7 64 bit Oracle Linux 8 64 bit Oracle Linux 9 64 bit Linux Mint 20.x 64 bit
Sistemi operativi. macOS	macOS Big Sur (11.x) macOS Monterey (12.x) macOS Ventura (13.x)

Per Network Agent è supportata anche l'architettura Apple Silicon (M1), così come Intel.

Sono supportate le seguenti piattaforme di virtualizzazione:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0

- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 bit
- Microsoft Hyper-V Server 2012 R2 64 bit
- Microsoft Hyper-V Server 2016 64 bit
- Microsoft Hyper-V Server 2019 64 bit
- Microsoft Hyper-V Server 2022 64 bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Macchina virtuale basata su kernel (tutti i sistemi operativi Linux supportati da Network Agent)

In Microsoft Windows XP Network Agent non potrebbe eseguire correttamente alcune operazioni.

Sistemi operativi e piattaforme non supportati

Network Agent

I seguenti sistemi operativi non sono supportati:

- Microsoft Windows Embedded POSReady 7 32 bit/64 bit
- Microsoft Windows Embedded 8 Industry Pro 32 bit / 64 bit
- Microsoft Windows Embedded 8 Industry Enterprise 32 bit / 64 bit
- Microsoft Windows Embedded 8 Standard 32 bit/64 bit
- Microsoft Windows Embedded 8.1 Industry Enterprise 32 bit/64 bit
- Microsoft Windows Embedded 8.1 Industry Update 32 bit/64 bit
- Microsoft Windows 10 Home (Threshold 1, 1507) 32 bit/64 bit
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32 bit/64 bit

- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32 bit/64 bit
- Microsoft Windows 10 Education (Threshold 1, 1507) 32 bit/64 bit
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32 bit
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32 bit
- Microsoft Windows 10 Home Threshold 2 (aggiornamento novembre 2015, 1511) 32 bit/64 bit
- Microsoft Windows 10 Pro Threshold 2 (aggiornamento novembre 2015 Update, 1511) 32 bit/64 bit
- Microsoft Windows 10 Enterprise Threshold 2 (aggiornamento novembre 2015 Update, 1511) 32 bit/64 bit
- Microsoft Windows 10 Education Threshold 2 (aggiornamento novembre 2015, 1511) 32 bit/64 bit
- Microsoft Windows 10 Mobile Threshold 2 (aggiornamento novembre 2015, 1511) 32 bit
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (aggiornamento novembre 2015, 1511) 32 bit
- Microsoft Windows 10 Home RS1 (aggiornamento Anniversary, 1607) 32 bit/64 bit
- Microsoft Windows 10 Pro RS1 (aggiornamento Anniversary, 1607) 32 bit/64 bit
- Microsoft Windows 10 Enterprise RS1 (aggiornamento Anniversary, 1607) 32 bit/64 bit
- Microsoft Windows 10 Education RS1 (aggiornamento Anniversary, 1607) 32 bit/64 bit
- Microsoft Windows 10 Mobile RS1 (aggiornamento Anniversary, 1607) 32 bit
- Microsoft Windows 10 Mobile Enterprise RS1 (aggiornamento Anniversary, 1607) 32 bit
- Microsoft Windows 10 Home RS2 (aggiornamento Creators, 1703) 32 bit/64 bit
- Microsoft Windows 10 Pro RS2 (aggiornamento Creators, 1703) 32 bit/64 bit
- Microsoft Windows 10 Enterprise RS2 (aggiornamento Creators, 1703) 32 bit/64 bit
- Microsoft Windows 10 Education RS2 (aggiornamento Creators, 1703) 32 bit/64 bit
- Microsoft Windows 10 Mobile RS2 (aggiornamento Creators, 1703) 32 bit
- Microsoft Windows 10 Mobile Enterprise RS2 (aggiornamento Creators, 1703) 32 bit
- Microsoft Windows 10 Mobile RS3 32 bit
- Microsoft Windows 10 Mobile Enterprise RS3 32 bit
- Microsoft Windows 10 Mobile RS4 32 bit
- Microsoft Windows 10 Mobile Enterprise RS4 32 bit
- Microsoft Windows 10 Mobile RS5 32 bit
- Microsoft Windows 10 Mobile Enterprise RS5 32 bit

- Microsoft Windows 8 (Core) 32 bit/64 bit
- Microsoft Windows 7 Professional 32 bit/64 bit
- Microsoft Windows 7 Enterprise/Ultimate 32 bit/64 bit
- Microsoft Windows 7 Home Basic/Premium 32 bit/64 bit
- Microsoft Windows Vista Business con Service Pack 1 32 bit/64 bit
- Microsoft Windows Vista Enterprise con Service Pack 1 32 bit/64 bit
- Microsoft Windows Vista Ultimate con Service Pack 1 32 bit/64 bit
- Microsoft Windows Vista Business con Service Pack 2 e versioni successive 32 bit/64 bit
- Microsoft Windows Vista Enterprise con Service Pack 2 e versioni successive 32 bit/64 bit
- Microsoft Windows Vista Ultimate con Service Pack 2 e versioni successive 32 bit/64 bit
- Microsoft Windows XP Professional con Service Pack 2 32 bit/64 bit
- Microsoft Windows XP Home Service Pack 3 e versioni successive 32 bit
- Windows Essential Business Server 2008 Standard 64 bit
- Windows Essential Business Server 2008 Premium 64 bit
- Windows Small Business Server 2003 Standard con Service Pack 1 32 bit
- Windows Small Business Premium 2003 Standard con Service Pack 1 32 bit
- Windows Small Business Server 2008 Standard 64 bit
- Windows Small Business Server 2008 Premium 64 bit
- Windows Small Business Server 2011 Premium Add-on 64 bit
- Windows Small Business Server 2011 Standard 64 bit
- Windows Small Business Server 2011 Essentials 64 bit
- Windows Home Server 2011 64 bit
- Windows MultiPoint Server 2010 Standard 64 bit
- Windows MultiPoint Server 2010 Premium 64 bit
- Windows MultiPoint Server 2012 Standard/Premium 64 bit
- Microsoft Windows 2000 Server 32 bit
- Windows Server 2003 Enterprise con Service Pack 2 32 bit/64 bit
- Windows Server 2003 Standard con Service Pack 2 32 bit/64 bit

- Windows Server 2003 R2 Enterprise con Service Pack 2 32 bit/64 bit
- Windows Server 2003 R2 Standard con Service Pack 2 32 bit/64 bit
- Windows Server 2008 Datacenter Service Pack 1 32 bit/64 bit
- Windows Server 2008 Enterprise Service Pack 1 32 bit/64 bit
- Windows Server 2008 Service Pack 1 Server Core 32 bit/64 bit
- Windows Server 2008 Standard Service Pack 1 32 bit/64 bit
- Windows Server 2008 Standard 32 bit/64 bit
- Windows Server 2008 Enterprise 32 bit/64 bit
- Windows Server 2008 Datacenter 32 bit/64 bit
- Windows Server 2008 R2 Server Core 64 bit
- Windows Server 2008 R2 Datacenter 64 bit
- Windows Server 2008 R2 Enterprise 64 bit
- Windows Server 2008 R2 Foundation 64 bit
- Windows Server 2008 R2 Standard 64 bit
- Windows Server 2016 Nano (opzione installazione) (CBB)
- Windows Storage Server 2008 32 bit/64 bit
- Windows Storage Server 2008 Service Pack 2 64 bit
- Windows Storage Server 2008 R2 64 bit
- Windows Storage Server 2012 64 bit
- Windows Storage Server 2012 R2 64 bit
- Windows Storage Server 2016 64 bit
- Windows Storage Server 2019 64 bit
- Debian GNU / Linux 7.x (fino a 7.8) 32 bit / 64 bit
- Debian GNU / Linux 8.x (Jessie) 32 bit / 64 bit
- Debian GNU/Linux 9.x (Stretch) 32 bit / 64 bit
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32 bit / 64 bit
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32 bit / 64 bit
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32 bit / 64 bit

- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32 bit / 64 bit
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 bit
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 bit/64 bit
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 bit/64 bit
- CentOS 6.x (fino a 6.6) 64 bit
- CentOS 7.x ARM 64 bit
- CentOS 8.x 64 bit
- SUSE Linux Enterprise Desktop 12 (tutti i SP) 64 bit
- SUSE Linux Enterprise Desktop 15 (tutti i Service Pack) 64 bit
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 bit
- ALT Server 10 64 bit
- ALT Server 9.2 64 bit
- ALT Workstation 10 32 bit/64 bit
- ALT Workstation 9.2 32 bit/64 bit
- ALT 8 SP Server (LKNV.11100-01) 64 bit
- ALT 8 SP Server (LKNV.11100-02) 64 bit
- ALT 8 SP Server (LKNV.11100-03) 64 bit
- ALT 8 SP Workstation (LKNV.11100-01) 32 bit/64 bit
- ALT 8 SP Workstation (LKNV.11100-02) 32 bit/64 bit
- ALT 8 SP Workstation (LKNV.11100-03) 32 bit/64 bit
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 bit
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.7) 64 bit
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.6) 64 bit
- Astra Linux Common Edition (aggiornamento operativo 2.12) 64 bit
- Astra Linux Special Edition RUSB.10152-02 (aggiornamento operativo 4.7) ARM 64 bit
- Linux Mint 19.x 64-bit
- AlterOS 7.5 e versioni successive 64 bit

- Lotos (versione core Linux 4.19.50, DE: MATE) 64 bit
- Mageia 4 32 bit
- GosLinux IC6 64 bit
- RED OS 7.3 64 bit
- RED OS 7.3 Server 64 bit
- RED OS 7.3 Certified Edition 64 bit
- ROSA COBALT 7.9 64 bit
- ROSA CHROME 12 64 bit
- ROSA Enterprise Linux Server 7.3 64 bit
- ROSA Enterprise Linux Desktop 7.3 64 bit
- ROSA COBALT Workstation 7.3 64 bit
- ROSA COBALT Server 7.3 64 bit
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- macOS Sierra (10.12)
- macOS High Sierra (10.13)
- macOS Mojave (10.14)
- macOS Catalina (10.15)

Le seguenti piattaforme di virtualizzazione non sono supportate:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x

- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64 bit
- Microsoft Hyper-V Server 2008 R2 64 bit
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 e versioni successive 64 bit
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

Applicazioni e soluzioni Kaspersky compatibili

Le licenze per prodotti diversi garantiscono set diversi di applicazioni e soluzioni Kaspersky.

È possibile distribuire e gestire le seguenti applicazioni e soluzioni Kaspersky tramite Kaspersky Security Center Cloud Console:

- Kaspersky Security for Windows Server 11.0.1
- Kaspersky Endpoint Security 12.4 for Windows
- Kaspersky Endpoint Security 12.0 for Linux
- Kaspersky Endpoint Security 12.0 for Mac
- Kaspersky Embedded Systems Security 3.3 for Windows
- Kaspersky Embedded Systems Security 3.3 for Linux
- Kaspersky Endpoint Agent 3.16
- Kaspersky Endpoint Security for Android
- Kaspersky Security for iOS

È possibile integrare le seguenti soluzioni per visualizzare ed elaborare gli incidenti di sicurezza:

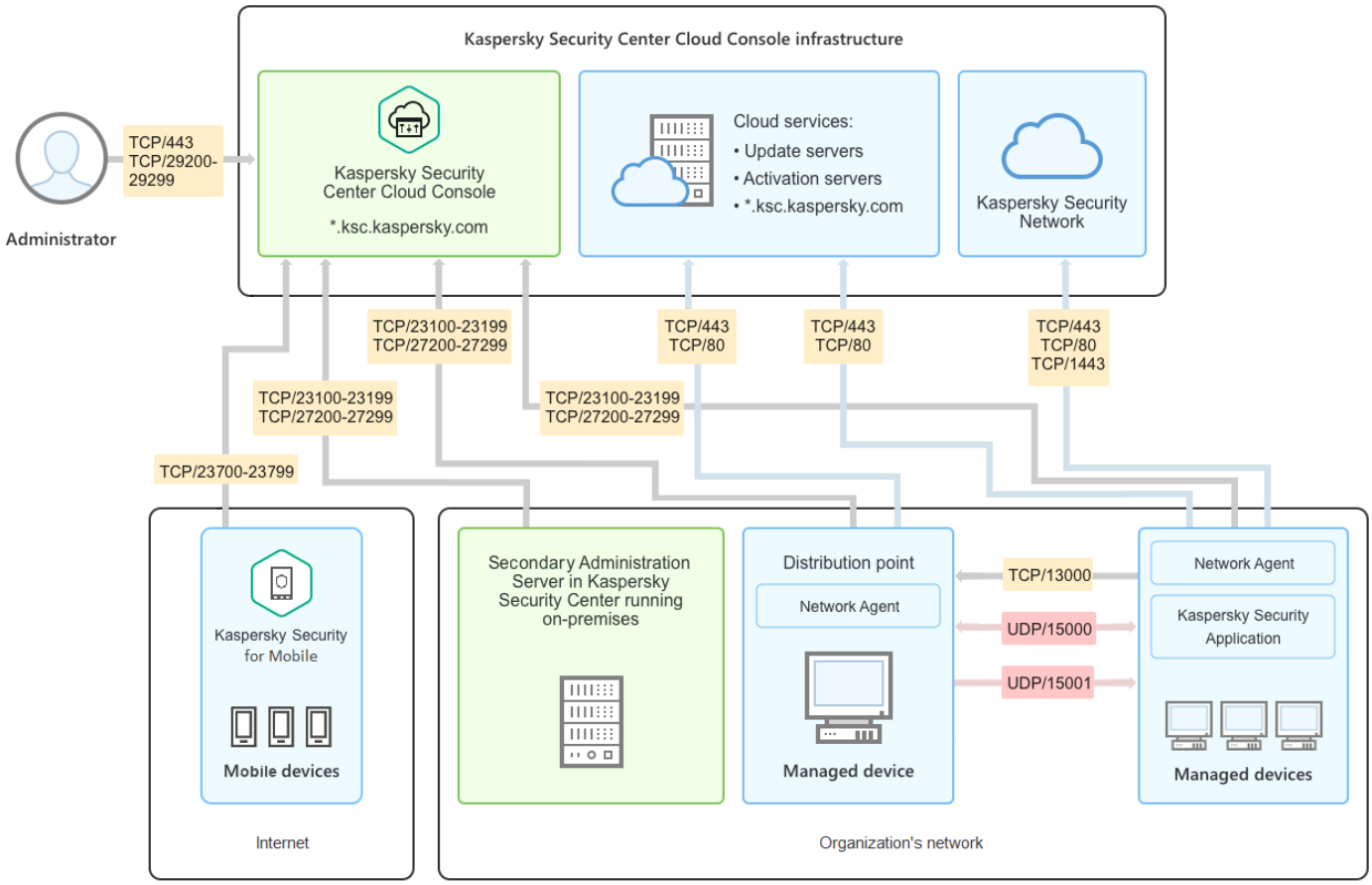
- Kaspersky Managed Detection and Response
- Kaspersky Endpoint Detection and Response Optimum 2.3

- Kaspersky Endpoint Detection and Response Expert

Se si installa una nuova versione dell'applicazione in un dispositivo gestito, ma si utilizza un criterio obsoleto per una nuova versione dell'applicazione anziché aggiornare il criterio, l'applicazione fornisce comunque i dati a Kaspersky Security Center Cloud Console, ma Kaspersky Security Center Cloud Console non è in grado di elaborare questi dati come descritto nella sezione Dati elaborati delle applicazioni gestite della documentazione. Per consentire a Kaspersky Security Center Cloud Console di elaborare questi dati, è necessario creare un nuovo criterio per la nuova versione dell'applicazione.

Architettura

Questa sezione fornisce una descrizione dei componenti di Kaspersky Security Center Cloud Console e la relativa interazione.



Architettura di Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console gestito tramite la console basata sul cloud include due componenti principali: l'infrastruttura di Kaspersky Security Center Cloud Console e l'infrastruttura del cliente.

L'infrastruttura di Kaspersky Security Center Cloud Console è composta da:

- **Administration Console basata sul cloud**. Offre un'interfaccia Web per la creazione e la manutenzione del sistema di protezione di una rete di un'organizzazione client gestita tramite Kaspersky Security Center Cloud Console.

- **Servizi cloud**. Include server di aggiornamento e server di attivazione.

- **Finestra Kaspersky Security Network (KSN)**. Server che contengono un database Kaspersky con informazioni sempre aggiornate sulla reputazione di file, risorse Web e software. Kaspersky Security Network assicura una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora l'efficacia di alcuni componenti della protezione e riduce la probabilità di falsi positivi.

L'infrastruttura del cliente può essere costituita da:

- **Punto di distribuzione**. Computer in cui è installato Network Agent e che viene utilizzato per la distribuzione di aggiornamenti, il polling della rete, l'installazione remota di applicazioni, il recupero di informazioni sui computer in un gruppo di amministrazione e/o la trasmissione in un dominio. L'amministratore seleziona i dispositivi appropriati e assegna manualmente i punti di distribuzione.

- **Dispositivi gestiti**. Computer della rete del cliente protetti tramite Kaspersky Security Center Cloud Console. Network Agent e un'applicazione di protezione Kaspersky devono essere installati in ciascun dispositivo gestito.

- **Administration Server secondario in esecuzione in locale** (facoltativo). È possibile utilizzare un Administration Server locale per creare una gerarchia di Administration Server.

Porte utilizzate da Kaspersky Security Center Cloud Console

Per utilizzare Kaspersky Security Center Cloud Console, che fa parte dell'infrastruttura Kaspersky, è necessario aprire le seguenti porte nei dispositivi client per consentire la connessione a Internet (vedere la seguente tabella):

Porte che devono essere aperte nei dispositivi client per consentire la connessione a Internet

Porta (o intervallo di porte)	Protocollo	Scopo della porta (o dell'intervallo di porte)
23100 -23199	TCP/TLS	Ricezione di connessioni da Network Agent e Administration Server secondari nell'Administration Server di Kaspersky Security Center Cloud Console all'indirizzo *.ksc.kaspersky.com. L'infrastruttura Kaspersky può utilizzare qualsiasi porta all'interno di questo intervallo e qualsiasi indirizzo Web all'interno di questa maschera. La porta e l'indirizzo Web possono cambiare di volta in volta.
23700 – 23799 (solo se si gestiscono dispositivi mobili)	TCP/TLS	Ricezione delle connessioni dai dispositivi mobili. Connessione all'Administration Server di Kaspersky Security Center Cloud Console all'indirizzo *.ksc.kaspersky.com. L'infrastruttura Kaspersky può utilizzare qualsiasi porta all'interno di questo intervallo e qualsiasi indirizzo Web all'interno di questa maschera. La porta e l'indirizzo Web possono cambiare di volta in volta.
27200 -27299	TCP/TLS	Ricezione delle connessioni per l'attivazione dell'applicazione dai dispositivi gestiti (ad eccezione dei dispositivi mobili). Connessione all'Administration Server di Kaspersky Security Center Cloud Console all'indirizzo *.ksc.kaspersky.com. L'infrastruttura Kaspersky può utilizzare qualsiasi porta all'interno di questo intervallo e qualsiasi indirizzo Web all'interno di questa maschera. La porta e l'indirizzo Web possono cambiare di volta in volta.
29200 – 29299	TCP/TLS	Tunneling delle connessioni ai dispositivi gestiti tramite l'utilità klsctunnel utilizzando l'Administration Server di Kaspersky Security Center Cloud Console all'indirizzo *.ksc.kaspersky.com.

		L'infrastruttura Kaspersky può utilizzare qualsiasi porta all'interno di questo intervallo e qualsiasi indirizzo Web all'interno di questa maschera. La porta e l'indirizzo Web possono cambiare di volta in volta.
443	HTTPS	Connessione al servizio di rilevamento di Kaspersky Security Center Cloud Console all'indirizzo *.ksc.kaspersky.com. Qualsiasi indirizzo Web all'interno di questa maschera può essere utilizzato dall'infrastruttura Kaspersky.
1443	TCP	Connessione a Kaspersky Security Network
80	TCP	La connessione viene utilizzata per verificare la validità dei certificati di Kaspersky Security Center su *.digicert.com. Qualsiasi indirizzo Web all'interno di questa maschera può essere utilizzato dall'infrastruttura Kaspersky.

La tabella seguente elenca le porte che devono essere aperte nei dispositivi client in cui è installato Network Agent.

Porte che devono essere aperte nei dispositivi client

Numero di porta	Protocollo	Ambito della porta	Ambito
15000	UDP	Ricezione di dati dai gateway di connessione (se in uso)	Gestione dei dispositivi client
15000	Trasmissione UDP	Acquisizione di dati su altri Network Agent all'interno dello stesso dominio di trasmissione	Distribuzione degli aggiornamenti e dei pacchetti di installazione
15001	UDP	Ricezione di richieste multicast da un punto di distribuzione (se in uso)	Ricezione di aggiornamenti e pacchetti di installazione da un punto di distribuzione

Si noti che il processo klnagent può anche richiedere porte libere dall'intervallo di porte dinamiche del sistema operativo di un endpoint. Queste porte vengono assegnate automaticamente al processo klnagent dal sistema operativo, quindi il processo klnagent può utilizzare alcune porte usate da un altro software. Se il processo klnagent influisce sulle operazioni del software, modificare le impostazioni delle porte in questo software o modificare l'intervallo di porte dinamiche predefinito nel sistema operativo per escludere la porta utilizzata dal software interessato.

Tenere inoltre presente che i suggerimenti sulla compatibilità di Kaspersky Security Center Cloud Console con il software di terze parti sono descritti solo come riferimento e potrebbero non essere applicabili alle nuove versioni del software di terze parti. I suggerimenti descritti per la configurazione delle porte si basano sull'esperienza dell'Assistenza tecnica e sulle nostre best practice.

La tabella seguente elenca le porte aggiuntive che devono essere aperte nei dispositivi client in cui è installato Network Agent come punto di distribuzione.

Porte utilizzate da Network Agent con il ruolo di punto di distribuzione

Numero di porta	Protocollo	Ambito della porta	Ambito
13000	TCP/TLS	Ricezione delle connessioni dai Network Agent	Gestione dei dispositivi client e distribuzione degli aggiornamenti e dei pacchetti di installazione
13111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	TCP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN

13295 (solo se si utilizza il punto di distribuzione come server push)	TCP/TLS	Invio di notifiche push ai dispositivi gestiti	Punto di distribuzione utilizzato come server push
15111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	UDP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN
17111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	HTTPS	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN

Se si dispone di uno o più Administration Server nella rete che vengono utilizzati come Administration Server secondari quando l'Administration Server primario si trova nell'infrastruttura Kaspersky, fare riferimento all'elenco delle porte utilizzate da Kaspersky Security Center in esecuzione in locale. Utilizzare queste porte per l'interazione tra l'Administration Server secondario (o gli Administration Server secondari) e i dispositivi client.

Interfaccia di Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console è gestito tramite l'interfaccia Web.

La finestra dell'applicazione contiene i seguenti elementi:

- Menu principale nella parte sinistra della finestra
- Area di lavoro nella parte destra della finestra

Menu principale

Il menu principale contiene le seguenti sezioni:

- **Presentazione e tutorial**. Contiene video su come configurare e utilizzare Kaspersky Security Center Cloud Console e le applicazioni di sicurezza.

  Nel browser Mozilla Firefox, se si riproduce un video nella sezione **Presentazione e tutorial** nella finestra pop-up, si apre il video nell'immagine in modalità immagine e quindi si chiude il video nella finestra pop-up, anche il video nell'immagine in modalità immagine viene chiuso.

- **Administration Server**. Mostra il nome dell'Administration Server a cui si è attualmente connessi. Fare clic sull'icona delle impostazioni () per aprire le proprietà di Administration Server.
- **Monitoraggio e generazione dei rapporti**. Offre una panoramica dell'infrastruttura, degli stati di protezione e delle statistiche.
- **Risorse (dispositivi)**. Contiene strumenti per la gestione dei dispositivi client, così come le attività e i criteri dell'applicazione Kaspersky.
- **Utenti e ruoli**. Consente di gestire utenti e ruoli, configurare i diritti degli utenti assegnando ruoli agli utenti e associare i profili dei criteri ai ruoli.

- **Operazioni**. Contiene una serie di operazioni, tra cui licensing dell'applicazione, gestione delle patch e gestione delle applicazioni di terzi. Fornisce anche accesso agli archivi delle applicazioni.
- **Individuazione e distribuzione**. Consente di eseguire il polling della rete per rilevare i dispositivi client e distribuire i dispositivi ai gruppi di amministrazione manualmente o automaticamente. Contiene anche l'avvio rapido guidato e la Distribuzione guidata della protezione.
- **Marketplace**. Contiene informazioni sull'intera gamma di soluzioni aziendali Kaspersky e consente di selezionare quelle necessarie, nonché di procedere all'acquisto di tali soluzioni sul sito Web di Kaspersky.
- **Impostazioni**. Contiene le impostazioni per integrare Kaspersky Security Center Cloud Console con altre applicazioni Kaspersky. Contiene anche le impostazioni personali relative all'aspetto dell'interfaccia, ad esempio la lingua o il tema dell'interfaccia.
- **Menu dell'account personale**. Contiene un collegamento alla Guida in linea e informazioni sul Servizio di assistenza tecnica di Kaspersky. Consente inoltre di eseguire la disconnessione da Kaspersky Security Center Cloud Console.

Area di lavoro

L'area di lavoro mostra le informazioni che si sceglie di visualizzare nelle sezioni della finestra dell'interfaccia Web dell'applicazione. Contiene inoltre elementi di controllo che è possibile utilizzare per configurare la modalità di visualizzazione delle informazioni.

Localizzazione di Kaspersky Security Center Cloud Console

L'interfaccia e la documentazione di Kaspersky Security Center Cloud Console sono disponibili nelle seguenti lingue:

- Inglese
- Francese
- Tedesco
- Italiano
- Giapponese
- Portoghese (Brasile)
- Russo
- Spagnolo
- Spagnolo (LATAM)

Confronto tra Kaspersky Security Center e Kaspersky Security Center Cloud Console

È possibile utilizzare Kaspersky Security Center nei seguenti modi:

- Come soluzione cloud

  Kaspersky Security Center viene automaticamente installato nell'ambiente cloud e Kaspersky offre l'accesso all'Administration Server come servizio. Il sistema di sicurezza di rete viene gestito tramite Administration Console basata su cloud, denominata Kaspersky Security Center Cloud Console. Questa console ha un'interfaccia simile all'interfaccia di Kaspersky Security Center Web Console.

- Come soluzione locale (basata su Windows o Linux)

  Kaspersky Security Center viene installato in un dispositivo locale e il sistema di sicurezza di rete viene gestito tramite Administration Console basata su Microsoft Management Console o Kaspersky Security Center Web Console.

  Oltre all'applicazione basata su Windows, è disponibile anche Kaspersky Security Center Linux. Kaspersky Security Center Linux è progettato per distribuire e gestire la protezione dei dispositivi Linux utilizzando Administration Server basato su Linux per soddisfare i requisiti degli ambienti Linux puri. Kaspersky Security Center basato su Windows e Kaspersky Security Center Linux prevedono diversi set di funzionalità.

La tabella seguente consente di confrontare le funzionalità principali di Kaspersky Security Center e Kaspersky Security Center Cloud Console.

Confronto delle funzionalità di Kaspersky Security Center in esecuzione in locale e come soluzione cloud

Funzionalità o proprietà	Kaspersky Security Center 14 in esecuzione in locale	Kaspersky Security Center Cloud Console
Posizione dell'Administration Server	In locale	Cloud
Posizione del DBMS (Database Management System)	In locale	Cloud
Administration Console basata sul Web	✓	✓
Manutenzione dell'Administration Server e del DBMS	Gestito dal cliente	Gestito da Kaspersky
Gerarchia di Administration Server	✓	✓ (L'Administration Server di Kaspersky Security Center Cloud Console può fungere solo da Administration Server primario nella gerarchia e può essere utilizzato solo per il monitoraggio di criteri e attività)
Gerarchia di gruppi di amministrazione	✓	✓
Migrazione dei dispositivi gestiti e degli oggetti correlati da Kaspersky Security Center in locale a Kaspersky Security Center Cloud Console	✓	✓
Polling della rete	✓	✓ (solo per punti di distribuzione)
Numero massimo di dispositivi gestiti	100.000	25.000
Protezione dei dispositivi gestiti Windows, Linux e macOS	✓	✓

Protezione dei dispositivi mobili	✓	✓ (sono supportati solo Kaspersky Endpoint Security for Android e Kaspersky Security for iOS)
Protezione dell'infrastruttura cloud pubblica	✓	✓
Gestione della sicurezza incentrata sul dispositivo	✓	✓
Criteri dell'applicazione	✓	✓
Attività per le applicazioni Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Server proxy KSN	✓	✓ (solo nei punti di distribuzione)
Kaspersky Private Security Network	✓	–
Distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky	✓	✓
Passaggio dei dispositivi gestiti a un altro Administration Server	✓	– (è necessario reinstallare i Network Agent nei dispositivi gestiti per il relativo passaggio a un altro Administration Server)
Supporto per Administration Server virtuali	✓	✓
Installazione di aggiornamenti software di terze parti e correzione delle vulnerabilità del software di terze parti	✓	✓ (per correggere le vulnerabilità del software di terze parti, è possibile installare solo le correzioni consigliate)
Notifiche sugli eventi che si sono verificati nei dispositivi gestiti	✓	✓
Creazione e gestione degli account utente	✓	✓
Numero massimo di eventi nel database	400.000 (può essere incrementato fino a 45.000.000)	400.000 (dipende dal numero di dispositivi gestiti)
Integrazione con i sistemi SIEM	✓	✓ (utilizzando solo il formato Syslog e il protocollo TLS su TCP)
Utilizzo di Administration Server come server WSUS	✓	–
Monitoraggio degli stati di criteri e attività	✓	✓
Supporto di cluster e array di server nei gruppi di amministrazione	✓	–

	(solo in Administration Console basata su MMC)	
Installazione remota di sistemi operativi	✓	–
Supporto SNMP	✓	–

Concetti di base

In questa sezione sono illustrati i concetti di base relativi a Kaspersky Security Center Cloud Console.

Network Agent

L'interazione tra l'Administration Server e i dispositivi viene eseguita dal componente *Network Agent* di Kaspersky Security Center Cloud Console. Network Agent deve essere installato in tutti i dispositivi in cui viene utilizzato Kaspersky Security Center Cloud Console per gestire applicazioni Kaspersky.

Network Agent viene installato nei dispositivi come un servizio con il seguente set di attributi:

- Con il nome "Kaspersky Security Center Network Agent"
- Impostato per l'avvio automatico all'avvio del sistema operativo
- Utilizzo dell'account LocalSystem

Un dispositivo con Network Agent installato è denominato *dispositivo gestito* o *dispositivo*. È possibile installare Network Agent in un dispositivo Windows, Linux o Mac.

Il nome del processo avviato da Network Agent è *klnagent.exe*.

Network Agent sincronizza il dispositivo gestito con Administration Server. Kaspersky Security Center Cloud Console sincronizza automaticamente Administration Server con i dispositivi gestiti diverse volte all'ora. Administration Server imposta l'intervallo di sincronizzazione (denominato anche *heartbeat*) a seconda del numero di dispositivi gestiti.

Gruppi di amministrazione

Un *gruppo di amministrazione* (di seguito denominato anche *gruppo*) è un set logico di dispositivi gestiti combinati in base a una specifica caratteristica allo scopo di gestire i dispositivi raggruppati come una singola unità in Kaspersky Security Center Cloud Console.

Tutti i dispositivi gestiti all'interno di un gruppo di amministrazione sono configurati in modo da eseguire quanto segue:

- Utilizzare le stesse impostazioni dell'applicazione (che possono essere specificate nei criteri di gruppo).
- Utilizzare una modalità operativa comune per tutte le applicazioni grazie alla creazione di attività di gruppo con impostazioni specificate. Tramite le attività di gruppo è ad esempio possibile creare e installare un pacchetto di installazione comune, aggiornare i database e i moduli dell'applicazione, eseguire la scansione del dispositivo su richiesta e abilitare la protezione in tempo reale.

Un dispositivo gestito può appartenere a un solo gruppo di amministrazione.

È possibile creare gerarchie con qualsiasi livello di nidificazione per gli Administration Server e i gruppi. Un singolo livello della gerarchia può comprendere Administration Server secondari e virtuali, gruppi e dispositivi gestiti. È possibile spostare i dispositivi da un gruppo all'altro senza spostarli fisicamente. Ad esempio, se la posizione di un dipendente all'interno dell'azienda cambia da addetto alla contabilità a sviluppatore, è possibile spostare il computer del dipendente dal gruppo di amministrazione Contabilità al gruppo di amministrazione Sviluppatori. Il computer riceverà automaticamente le impostazioni dell'applicazione necessarie per gli sviluppatori.

Gerarchia di Administration Server

Gli Administration Server possono essere organizzati in una gerarchia "primari/secondari". Ogni Administration Server può disporre di diversi Administration Server secondari a diversi livelli di nidificazione della gerarchia. Non vi sono limiti per il livello di nidificazione degli Administration Server secondario. I gruppi di amministrazione dell'Administration Server primario includeranno i dispositivi client di tutti gli Administration Server secondari.

L'Administration Server di Kaspersky Security Center Cloud Console può fungere solo da Administration Server primario e può avere come server secondari solo Administration Server in esecuzione in locale.

Durante la migrazione dall'Administration Server che viene eseguito in locale all'Administration Server di Kaspersky Security Center Cloud Console, è possibile disporre gli Administration Server in una gerarchia. Quindi, per mitigare la migrazione, è possibile predisporre il passaggio solo di una parte dei dispositivi gestiti alla gestione dell'Administration Server di Kaspersky Security Center Cloud Console. Il resto dei dispositivi gestiti rimane sotto la gestione dell'Administration Server in locale. Ciò consente di testare le funzionalità di gestione di Kaspersky Security Center Cloud Console su un numero limitato di dispositivi gestiti. Al tempo stesso, è possibile configurare criteri, attività, rapporti e altri oggetti per testare la gestione e il monitoraggio dell'intera rete. Ciò consente di tornare agli oggetti configurati nell'Administration Server in locale, se necessario.

Ogni dispositivo incluso nella gerarchia dei gruppi di amministrazione può essere connesso a un unico Administration Server. È necessario monitorare in modo indipendente la connessione dei dispositivi agli Administration Server. Utilizzare la funzionalità per la ricerca di dispositivi nei gruppi di amministrazione di differenti Administration Server in base agli attributi di rete.

Administration Server virtuale

Un Administration Server virtuale (denominato anche *server virtuale*) è un componente di Kaspersky Security Center Cloud Console progettato per la gestione della protezione anti-virus della rete di un'organizzazione client. Ciascun Administration Server virtuale può avere la propria struttura di gruppi di amministrazione e i propri mezzi di gestione e monitoraggio, come criteri, attività, rapporti ed eventi. L'ambito funzionale degli Administration Server virtuali può essere utilizzato da organizzazioni con flussi di lavoro complessi.

L'Administration Server virtuale presenta le seguenti restrizioni:

- Gli Administration Server virtuali sono supportati solo nella modalità commerciale di Kaspersky Security Center Cloud Console.
- L'Administration Server virtuale non supporta la creazione di Administration Server secondari (inclusi server virtuali).
- Non è possibile eseguire la migrazione di Administration Server virtuali da Kaspersky Security Center a Kaspersky Security Center Cloud Console.

- Gli Administration Server virtuali non possono essere gestiti da amministratori dedicati. Per impostazione predefinita, l'amministratore che gestisce l'Administration Server primario gestisce anche tutti gli Administration Server virtuali.
- Agli utenti creati in un server virtuale non può essere assegnato un ruolo in Administration Server.
- Nella finestra delle proprietà di Administration Server virtuale il numero delle sezioni è limitato.

Punto di distribuzione

Per *punto di distribuzione* si intende un dispositivo in cui è installato Network Agent, utilizzato per la distribuzione degli aggiornamenti, l'installazione remota delle applicazioni e il recupero di informazioni sui dispositivi della rete. Un punto di distribuzione può eseguire le seguenti funzioni:

- Distribuire gli aggiornamenti e i pacchetti di installazione ai dispositivi client nel gruppo (con distribuzione mediante il multicasting tramite UDP). Gli aggiornamenti possono essere ricevuti dai server di aggiornamento Kaspersky tramite un'attività di aggiornamento creata per il punto di distribuzione.

  I dispositivi dei punti di distribuzione che eseguono macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky.

  > Se uno o più dispositivi che eseguono macOS rientrano nell'ambito dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'attività viene completata con lo stato *Non riuscito*, anche se è stata completata correttamente in tutti i dispositivi Windows.

- Distribuire criteri e attività di gruppo attraverso il multicasting tramite UDP.
- Operare come gateway per la connessione all'Administration Server per i dispositivi di un gruppo di amministrazione.

  Se è impossibile stabilire una connessione diretta tra i dispositivi gestiti nel gruppo e Administration Server, il punto di distribuzione può essere utilizzato come gateway di connessione ad Administration Server per il gruppo. In questo caso, i dispositivi gestiti sono connessi al gateway di connessione, che a sua volta è connesso ad Administration Server.

  La presenza di un punto di distribuzione che opera come gateway di connessione non esclude la possibilità di una connessione diretta tra i dispositivi gestiti e Administration Server. Se il gateway di connessione non è disponibile, ma è tecnicamente possibile la connessione diretta ad Administration Server, i dispositivi gestiti vengono connessi direttamente ad Administration Server.

- Eseguire il polling della rete per rilevare nuovi dispositivi e aggiornare le informazioni sui dispositivi esistenti.
- Eseguire l'installazione remota di software di terze parti e di applicazioni Kaspersky tramite gli strumenti di Microsoft Windows, inclusa l'installazione nei dispositivi client senza Network Agent.

  Questa funzionalità consente di trasferire in remoto i pacchetti di installazione di Network Agent ai dispositivi client disponibili nelle reti a cui Administration Server non ha accesso diretto.

- Operare come server proxy che partecipa a Kaspersky Security Network.

  > Questa funzionalità non è supportata dai dispositivi dei punti di distribuzione che eseguono Linux o macOS.

È possibile abilitare il proxy KSN da parte del punto di distribuzione per fare in modo che il dispositivo abbia il ruolo di Proxy KSN. In questo caso il servizio proxy KSN (ksnproxy) viene eseguito nel dispositivo.

I file vengono trasmessi da Administration Server a un punto di distribuzione tramite HTTP o, se la connessione SSL è abilitata, HTTPS. L'utilizzo di HTTP o HTTPS garantisce un livello di prestazioni superiore rispetto a SOAP, grazie alla riduzione del traffico.

Ai dispositivi in cui è installato Network Agent devono essere assegnati manualmente i punti di distribuzione in base ai gruppi di amministrazione. L'elenco completo dei punti di distribuzione per i gruppi di amministrazione specificati è visualizzato nel rapporto sull'elenco dei punti di distribuzione.

L'ambito di un punto di distribuzione è il gruppo di amministrazione a cui è stato assegnato dall'amministratore, nonché i relativi sottogruppi a tutti i livelli. Tuttavia, il dispositivo che opera come punto di distribuzione può non essere incluso nel gruppo di amministrazione a cui è stato assegnato. Se sono stati assegnati più punti di distribuzione nella gerarchia dei gruppi di amministrazione, Network Agent nel dispositivo gestito si connette al punto di distribuzione più vicino nella gerarchia.

L'ambito dei punti di distribuzione può anche essere un percorso di rete. Il percorso di rete viene utilizzato per la creazione manuale di un set di dispositivi in cui il punto di distribuzione distribuirà gli aggiornamenti. È possibile determinare il percorso di rete solo per i dispositivi con sistema operativo Windows.

Kaspersky Security Center Cloud Console assegna a ciascun Network Agent un indirizzo IP multicast univoco diverso da tutti gli altri indirizzi. Questo consente di evitare il sovraccarico della rete che potrebbe verificarsi a causa di sovrapposizioni IP.

Se due o più punti di distribuzione vengono assegnati in un'unica area di rete o in un singolo gruppo di amministrazione, uno di loro diventa il punto di distribuzione attivo, mentre gli altri diventano punti di distribuzione standby. Il punto di distribuzione attivo scarica gli aggiornamenti e i pacchetti di installazione direttamente da Administration Server, mentre i punti di distribuzione standby ricevono gli aggiornamenti solo dal punto di distribuzione attivo. In questo caso, i file vengono scaricati una sola volta da Administration Server e in seguito distribuiti tra i punti di distribuzione. Se il punto di distribuzione attivo diventa non disponibile per qualsiasi motivo, uno dei punti di distribuzione standby diventa attivo. Administration Server assegna automaticamente a un punto di distribuzione il ruolo di standby.

Lo stato di un punto di distribuzione (*Attivo* / Standby) è visualizzato con una casella di controllo nel rapporto di klnagchk.

Un punto di distribuzione richiede almeno 4 GB di spazio disponibile sul disco. Se lo spazio disponibile sul disco del punto di distribuzione è inferiore a 2 GB, Kaspersky Security Center Cloud Console crea un problema di sicurezza con il livello di importanza *Avviso*. Il problema di sicurezza sarà pubblicato nelle proprietà del dispositivo, nella sezione **Problemi di sicurezza**.

L'esecuzione delle attività di installazione remota in un dispositivo assegnato come punto di distribuzione richiede ulteriore spazio libero su disco. Il volume di spazio disponibile sul disco deve essere superiore alle dimensioni totali di tutti i pacchetti di installazione da installare.

L'esecuzione di attività di aggiornamento (installazione delle patch) e di correzione vulnerabilità in un dispositivo con il ruolo di punto di distribuzione richiede ulteriore spazio libero su disco. Il volume di spazio disponibile sul disco deve essere almeno il doppio rispetto alle dimensioni totali di tutte le patch da installare.

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Plug-in Web di gestione

Un componente speciale (il *plug-in Web di gestione*) viene utilizzato per l'amministrazione remota del software Kaspersky tramite Kaspersky Security Center Cloud Console. Da questo momento il plug-in Web di gestione verrà denominato anche *plug-in di gestione*. Il plug-in di gestione è un'interfaccia tra Kaspersky Security Center Cloud Console e un'applicazione Kaspersky specifica. Con un plug-in di gestione è possibile configurare le attività e i criteri per l'applicazione.

Il plug-in di gestione offre i seguenti elementi:

- Interfaccia per la creazione e la modifica di impostazioni e attività delle applicazioni
- Interfaccia per la creazione e la modifica di criteri e profili criterio per la configurazione centralizzata e remota dei dispositivi e delle applicazioni Kaspersky
- Trasmissione di eventi generati dall'applicazione
- Kaspersky Security Center Cloud Console consente di visualizzare eventi e dati relativi al funzionamento dell'applicazione e le statistiche trasmesse dai dispositivi client

Criteri

Un *criterio* è un set di impostazioni dell'applicazione Kaspersky che vengono applicate a un gruppo di amministrazione e ai relativi sottogruppi. È possibile installare diverse applicazioni Kaspersky nei dispositivi di un gruppo di amministrazione. Kaspersky Security Center Cloud Console fornisce un singolo criterio per ogni applicazione Kaspersky in un gruppo di amministrazione. Un criterio ha uno dei seguenti stati (vedere la seguente tabella):

Lo stato del criterio

Stato	Descrizione
Attivo	Il criterio corrente applicato al dispositivo. Può essere attivo un solo criterio per un'applicazione Kaspersky in ogni gruppo di amministrazione. I dispositivi applicano i valori delle impostazioni di un criterio attivo per un'applicazione Kaspersky.
Inattivo	Un criterio che non è attualmente applicato a un dispositivo.
Fuori sede	Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.

I criteri funzionano secondo le seguenti regole:

- È possibile configurare diversi criteri con differenti impostazioni per una singola applicazione.
- Un solo criterio può essere attivo per l'applicazione corrente.
- È possibile attivare un criterio inattivo quando si verifica un evento specifico. È ad esempio possibile applicare impostazioni di protezione anti-virus più rigide durante le epidemie di virus.
- Un criterio può avere criteri figlio.

In generale è possibile utilizzare i criteri in preparazione a situazioni di emergenza, come un attacco virus. Ad esempio in caso di attacco tramite unità flash, è possibile attivare un criterio che blocca l'accesso alle unità flash. In questo caso il criterio attivo corrente diventa automaticamente inattivo.

Per evitare di dover gestire più criteri, ad esempio quando diverse occasioni presuppongono solo la modifica di più impostazioni, è possibile utilizzare i profili criterio.

Un *profilo criterio* è un sottoinsieme denominato di valori delle impostazioni dei criteri che sostituisce i valori delle impostazioni di un criterio. Un profilo criterio influisce sulla creazione delle impostazioni ottimizzate in un dispositivo gestito. Per *impostazioni effettive* si intende un insieme di impostazioni dei criteri, impostazioni dei profili criterio e impostazioni delle applicazioni locali attualmente applicate nel dispositivo.

I profili criterio funzionano secondo le seguenti regole:

- Un profilo criterio assume validità quando si verifica una condizione di attivazione specifica.
- I profili criterio contengono valori delle impostazioni che differiscono dalle impostazioni dei criteri.
- L'attivazione di un profilo criterio modifica le impostazioni effettive del dispositivo gestito.
- Un criterio può includere al massimo 100 profili criterio.

Profili criterio

Talvolta può essere necessario creare più istanze di un singolo criterio per diversi gruppi di amministrazione; è inoltre possibile modificare le impostazioni di questi criteri in modo centralizzato. Le istanze potrebbero avere solo una o due impostazioni differenti. Ad esempio, a tutti gli addetti alla contabilità di un'azienda viene applicato lo stesso criterio, ma quelli di livello senior possono utilizzare unità flash, a differenza degli altri. In questo caso, l'applicazione dei criteri ai dispositivi solo tramite la gerarchia dei gruppi di amministrazione può essere poco pratica.

Per evitare di creare più istanze di un singolo criterio, Kaspersky Security Center Cloud Console consente di creare *profili criterio*. I profili criterio sono necessari per consentire l'esecuzione dei dispositivi all'interno di un unico gruppo di amministrazione con diverse impostazioni del criterio.

Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo nel dispositivo gestito. L'attivazione di un profilo modifica le impostazioni del criterio "di base" che erano inizialmente attive nel dispositivo. Le impostazioni modificate assumono i valori specificati nel profilo.

Relazioni tra impostazioni locali delle applicazioni e criteri

È possibile utilizzare i criteri per impostare valori identici delle impostazioni delle applicazioni per tutti i dispositivi nel gruppo.

I valori delle impostazioni specificati da un criterio possono essere ridefiniti per singoli dispositivi in un gruppo utilizzando le impostazioni locali delle applicazioni. È possibile impostare soltanto i valori delle impostazioni che il criterio consente di modificare, ovvero le impostazioni sbloccate.

Il valore di un'impostazione utilizzata da un'applicazione in un dispositivo client è determinato dalla posizione del lucchetto (🔒) per l'impostazione nel criterio:

- Se la modifica di un'impostazione è bloccata, viene utilizzato lo stesso valore definito nel criterio in tutti i dispositivi client.

- Se la modifica di un'impostazione è "sbloccata", l'applicazione utilizza in ogni dispositivo client il valore dell'impostazione locale invece di quello specificato nel criterio. Il valore del parametro può quindi essere modificato nelle impostazioni locali dell'applicazione.

In questo modo, quando l'attività viene eseguita in un dispositivo client, l'applicazione utilizza impostazioni definite in due modi diversi:

- tramite le impostazioni delle attività e le impostazioni locali delle applicazioni, se la modifica dell'impostazione nel criterio non è bloccata.

- tramite il criterio di gruppo, se la modifica dell'impostazione è bloccata.

Le impostazioni locali delle applicazioni vengono modificate dopo la prima applicazione del criterio in base alle relative impostazioni.

Licensing dell'applicazione

In questa sezione vengono fornite informazioni relative al licensing dell'applicazione.

Licensing di Kaspersky Security Center Cloud Console: scenario

Seguendo questo scenario, è possibile iniziare a utilizzare Kaspersky Security Center Cloud Console e le applicazioni di protezione gestite con una licenza.

Kaspersky Security Center Cloud Console consente la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi client, il monitoraggio del relativo utilizzo e il rinnovo delle licenze.

Se si sta già utilizzando Kaspersky Security Center Cloud Console, è possibile visitare Kaspersky Marketplace per visualizzare l'intera gamma di soluzioni aziendali Kaspersky, selezionare quelle desiderate e procedere all'acquisto sul sito Web di Kaspersky.

Verifica delle funzionalità di Kaspersky Security Center Cloud Console in modalità di prova prima dell'acquisto di una licenza

Prima dell'acquisto è possibile provare gratuitamente Kaspersky Security Center Cloud Console. A tale scopo, creare un'area di lavoro di prova che terminerà dopo 30 giorni. Se si desidera un'area di lavoro commerciale da utilizzare senza limiti di tempo, sarà necessario acquistare una licenza.

La modalità di prova non consente di passare successivamente alla modalità commerciale. Qualsiasi area di lavoro di prova verrà automaticamente eliminata con tutti i relativi contenuti allo scadere del periodo di 30 giorni.

Passaggi

Lo scenario procede per fasi:

1. **Acquisizione di un codice di attivazione per il licensing di Kaspersky Security Center Cloud Console in modalità commerciale. Acquisto di una licenza (o più licenze)**

   Licenze diverse garantiscono l'utilizzo di applicazioni e servizi Kaspersky diversi, pertanto è consigliabile acquistare più di una licenza.

   Di seguito viene illustrato quali licenze è possibile acquistare e il numero minimo di dispositivi per ogni licenza.

   Kaspersky Security Center Cloud Console fa parte di diverse soluzioni Kaspersky. Scegliere la soluzione che si desidera utilizzare e acquistare una licenza. Se si desidera acquistare una licenza in grado di coprire 10.000 o più dispositivi, sarà necessario contattare Kaspersky o uno dei partner Kaspersky con una richiesta speciale.

   Utilizzare la tabella per verificare quali funzionalità di Vulnerability e patch management sono disponibili con le diverse licenze.

   Se si desidera utilizzare Kaspersky Security Center Cloud Console in un ambiente cloud come Microsoft Azure, leggere le opzioni di licensing per gli ambienti cloud.

   Gli MSP possono consultare le informazioni sul licensing di Kaspersky Security Center Cloud Console per MSP.

2. **Attivazione di Kaspersky Security Center Cloud Console durante la creazione dell'area di lavoro**

È necessario specificare la chiave di licenza per attivare Kaspersky Security Center Cloud Console durante la creazione di un'area di lavoro.

Se si dispone di più chiavi di licenza, specificarne una. In seguito sarà necessario aggiungere altre chiavi di licenza in Kaspersky Security Center Cloud Console per attivare le applicazioni Kaspersky gestite.

3. **Aggiunta di chiavi di licenza per le applicazioni gestite all'archivio dell'Administration Server**

   Prima della distribuzione delle chiavi di licenza, è necessario aggiungere queste chiavi di licenza all'archivio dell'Administration Server.

   La chiave di licenza specificata durante la creazione dell'area di lavoro viene aggiunta automaticamente all'archivio dell'Administration Server.

   Se si dispone di più chiavi di licenza, aggiungere la chiave (o le chiavi) di licenza una alla volta all'archivio dell'Administration Server di Kaspersky Security Center Cloud Console.

4. **Distribuzione delle chiavi di licenza per applicazioni gestite**

   Scegliere un metodo di distribuzione della chiave di licenza (o delle chiavi di licenza) a tutti i dispositivi che si desidera proteggere:

   - Distribuzione automatica

     > Se si utilizzano diverse applicazioni gestite ed è necessario distribuire un codice di attivazione specifico per le applicazioni, scegliere un'altra modalità di distribuzione del codice di attivazione.

     Kaspersky Security Center consente di distribuire automaticamente le chiavi di licenza disponibili per le applicazioni gestite. Ad esempio, nell'archivio dell'Administration Server sono presenti tre chiavi di licenza. È stata abilitata l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti** per tutte e tre le chiavi di licenza. Un'applicazione di protezione Kaspersky, ad esempio Kaspersky Endpoint Security for Windows, è installata nei dispositivi dell'organizzazione. Viene rilevata una nuova applicazione gestita in un dispositivo a cui deve essere distribuita una chiave di licenza. Ad esempio, due delle chiavi di licenza dell'archivio possono essere distribuite per l'applicazione gestita nel dispositivo: la chiave di licenza denominata *Key_1* e la chiave di licenza denominata *Key_2*. Una di queste chiavi di licenza viene distribuita per l'applicazione gestita. In questo caso non è possibile prevedere quale delle due chiavi di licenza verrà distribuita poiché la distribuzione automatica delle chiavi di licenza non offre nessuna attività di amministrazione.

     Quando una chiave di licenza viene distribuita, il numero di installazioni viene ricalcolato per questa chiave di licenza. È necessario accertarsi che il numero di applicazioni per cui è stata distribuita la chiave di licenza non superi la limitazione licenza. Se il numero di installazioni supera la limitazione licenza, a tutti i dispositivi non coperti dalla licenza verrà assegnato lo stato *Critico*.

     Istruzioni dettagliate:

     - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
     - Distribuzione automatica di una chiave di licenza

   - Distribuzione tramite l'attività di aggiunta della chiave di licenza per un'applicazione gestita

     Se si sceglie di utilizzare l'attività Aggiungi chiave di licenza per un'applicazione gestita, è possibile selezionare la chiave di licenza che deve essere distribuita nei dispositivi e selezionare i dispositivi nella modalità più opportuna, ad esempio selezionando un gruppo di amministrazione o una selezione dispositivi.

     Istruzioni dettagliate:

     - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
     - Distribuzione di una chiave di licenza ai dispositivi client

- Aggiunta manuale di un codice di attivazione o di un file chiave ai dispositivi

  È possibile attivare l'applicazione Kaspersky installata in locale utilizzando gli strumenti disponibili nell'interfaccia dell'applicazione. Fare riferimento alla documentazione dell'applicazione installata.

5. **Verifica dell'attivazione delle applicazioni Kaspersky gestite nei diversi dispositivi**

   Per assicurarsi che le chiavi di licenza siano distribuite correttamente, visualizzare l'elenco delle chiavi di licenza utilizzate per un'applicazione.

6. **Configurazione degli eventi relativi alla scadenza della licenza**

   Configurare gli eventi in modo da ricevere una notifica quando le chiavi di licenza sono finite o in scadenza:

   - Eventi critici di Administration Server
   - Eventi di errore funzionale di Administration Server
   - Eventi di avviso di Administration Server
   - Eventi informativi di Administration Server

Informazioni sulla modalità di prova di Kaspersky Security Center Cloud Console

La *modalità di prova* è una modalità di Kaspersky Security Center Cloud Console appositamente pensata per far conoscere all'utente le funzionalità di Kaspersky Security Center Cloud Console. In questa modalità è possibile eseguire attività all'interno di un'area di lavoro il cui periodo di validità è limitato a 30 giorni. La modalità di prova viene attivata automaticamente non appena si crea un'area di lavoro di prova. Il set di funzionalità disponibili in modalità di prova è identico all'ambito della licenza standard di Kaspersky Endpoint Security for Business Advanced.

In Kaspersky Security Center Cloud Console non è necessario concedere in licenza l'Administration Server, poiché le funzionalità che richiedono una licenza speciale non sono supportate. Se si desidera utilizzare Kaspersky Security Center Cloud Console in modalità di prova, si ottiene automaticamente una licenza di prova quando si crea la prima area di lavoro.

La modalità di prova non consente di passare successivamente alla modalità commerciale. Qualsiasi area di lavoro di prova verrà automaticamente eliminata con tutti i relativi contenuti allo scadere del periodo di 30 giorni.

Vengono imposte le seguenti restrizioni sull'utilizzo delle funzionalità di Kaspersky Security Center Cloud Console in modalità di prova:

- Non è possibile creare una gerarchia di Administration Server. Non è possibile creare Administration Server virtuali.
- La sezione **Licensing** è disponibile in sola lettura. Tutte le operazioni sono vietate in questa sezione, inclusa l'aggiunta e la rimozione delle chiavi di licenza.
- Non è possibile creare pacchetti di installazione personalizzati.
- Non è possibile creare ruoli personalizzati per gli utenti.

- La funzionalità Epidemia di virus non è disponibile. Gli eventi Epidemia di virus non vengono memorizzati e non vengono inviate notifiche.
- L'archivio **Oggetti eliminati** non è disponibile.
- Non è possibile abilitare l'aggiunta di eventi in batch (pubblicati in grandi quantità) nel database.
- La migrazione degli Administration Server dalla modalità In locale alla modalità Cloud Console non è supportata.
- Le informazioni statistiche KSN provenienti dai componenti di Administration Server, come Administration Server o Network Agent, non vengono inviate a Kaspersky.

Alcuni limiti sono imposti anche relativamente alla creazione di alcuni oggetti dell'applicazione (vedere la tabella di seguito). Se uno di questi limiti viene superato quando si tenta di creare un oggetto di questo tipo, la creazione dell'oggetto verrà bloccata e verrà visualizzato un messaggio di errore relativo al limite.

Limitazioni relative alla creazione di oggetti Kaspersky Security Center Cloud Console in modalità di prova

Tipo di limitazione	Valore
Criteri	8
Attività	17
Chiavi di licenza	1
Pacchetti di installazione	5
Selezioni dispositivi (istanze preimpostate non incluse)	5
Selezioni eventi (istanze preimpostate non incluse)	5
Regole di spostamento dei dispositivi	3
Modelli di rapporto dello stesso tipo	10
Gruppi di protezione interni	20
Dispositivi gestiti	20

Utilizzo di Kaspersky Marketplace per scegliere le soluzioni aziendali Kaspersky

Marketplace è una sezione del menu principale che consente di visualizzare l'intera gamma di soluzioni aziendali Kaspersky, selezionare quelle desiderate e procedere all'acquisto nel sito Web di Kaspersky. È possibile utilizzare i filtri per visualizzare solo le soluzioni che si adattano alla propria organizzazione e ai requisiti del proprio sistema di sicurezza delle informazioni. Quando si seleziona una soluzione, Kaspersky Security Center Cloud Console reindirizza alla relativa pagina Web nel sito Web di Kaspersky per ulteriori informazioni sulla soluzione. Ogni pagina Web consente di procedere all'acquisto o contiene istruzioni sulla procedura di acquisto.

Nella sezione **Marketplace** è possibile filtrare le soluzioni Kaspersky utilizzando i seguenti criteri:

- Numero di dispositivi (endpoint, server e altri tipi di asset) che si desidera proteggere:
  - 50–250
  - 250–1000

- Più di 1000

- Livello di maturità del team di sicurezza delle informazioni dell'organizzazione:

  - **Foundations**

    Questo livello è tipico delle aziende che dispongono solo di un team IT. Il numero massimo di minacce possibili viene bloccato automaticamente.

  - **Optimum**

    Questo livello è tipico delle aziende che hanno una funzione di sicurezza IT specifica all'interno del team IT. A questo livello, le aziende richiedono soluzioni che consentano loro di contrastare le minacce commodity e le minacce che eludono i meccanismi di prevenzione esistenti.

  - **Expert**

    Questo livello è tipico delle aziende con ambienti IT complessi e distribuiti. Il team di sicurezza IT ha un livello di maturità ottimale o l'azienda dispone di un team SOC (Security Operations Center). Le soluzioni richieste consentono alle aziende di contrastare minacce complesse e attacchi mirati.

- Tipi di asset da proteggere:

  - **Endpoint**: workstation dei dipendenti, macchine fisiche e virtuali, sistemi integrati

  - **Server**: server fisici e virtuali

  - **Cloud**: ambienti cloud pubblici, privati o ibridi; servizi cloud

  - **Rete**: LAN, infrastruttura IT

  - **Servizio**: servizi relativi alla sicurezza forniti da Kaspersky

Per trovare e acquistare una soluzione aziendale Kaspersky:

1. Nel menu principale accedere a **Marketplace**.

   Per impostazione predefinita, la sezione mostra tutte le soluzioni aziendali Kaspersky disponibili.

2. Per visualizzare solo le soluzioni adatte alla propria organizzazione, selezionare i valori desiderati nei filtri.

3. Fare clic sulla soluzione che si desidera acquistare o per cui si desidera ottenere maggiori informazioni.

Si verrà reindirizzati alla pagina Web della soluzione. È possibile seguire le istruzioni visualizzate per procedere all'acquisto.

Licenze e numero minimo di dispositivi per ogni licenza

Se si desidera utilizzare Kaspersky Security Center Cloud Console in modalità commerciale, è necessario acquistare una licenza prima di creare la prima area di lavoro. Nella tabella seguente sono elencate le licenze che è possibile acquistare, con il numero minimo di dispositivi per ogni licenza (applicabile anche nel caso in cui il numero dei dispositivi da proteggere sia inferiore):

Licenze per l'utilizzo di Kaspersky Security Center Cloud Console

Licenza	Numero minimo di dispositivi (applicabile anche se si desidera proteggere un numero inferiore di dispositivi)

Kaspersky Endpoint Security for Business Select	Per le licenze commerciali: 300 Per licenze commerciali (in abbonamento): 100
Kaspersky Endpoint Security for Business Advanced	Per le licenze commerciali: 300 Per licenze commerciali (in abbonamento): 100
Kaspersky Total Security for Business	300
Kaspersky Endpoint Detection and Response Optimum	Per le licenze commerciali: 300 Per licenze commerciali (in abbonamento): 100
Kaspersky Endpoint Detection and Response Expert	50
Kaspersky Hybrid Cloud Security, Desktop	Per le licenze commerciali: 300 Per licenze commerciali (in abbonamento): 100
Kaspersky Hybrid Cloud Security, Server	50
Kaspersky Hybrid Cloud Security, Core	20
Kaspersky Hybrid Cloud Security, CPU	20
Kaspersky Hybrid Cloud Security Enterprise, Desktop	Per le licenze commerciali: 300 Per licenze commerciali (in abbonamento): 100
Kaspersky Hybrid Cloud Security Enterprise, Server	50
Kaspersky Hybrid Cloud Security Enterprise, CPU	20
Kaspersky Embedded Systems Security	300
Kaspersky Embedded Systems Security Compliance Edition	300
Kaspersky Symphony (attualmente disponibile solo in Russia)	300
Kaspersky Next EDR Foundations	300 utenti (ogni licenza utente può essere applicata a 1 dispositivo PC/Mac e 2 dispositivi mobili)
Kaspersky Next EDR Optimum	300 utenti (ogni licenza utente può essere applicata a 1 dispositivo PC/Mac e 2 dispositivi mobili)
Kaspersky Next XDR Expert	250 utenti (ogni licenza utente può essere applicata a 1 dispositivo PC/Mac e 2 dispositivi mobili)

Il numero massimo di dispositivi per ogni area di lavoro è 25.000. Se si desidera proteggere più di 10.000 dispositivi, è necessario creare un'area di lavoro separata. A tale scopo, inviare una richiesta al Servizio di assistenza tecnica Kaspersky. Tale richiesta deve contenere le seguenti informazioni:

- **Indirizzo e-mail utente**: l'indirizzo e-mail dell'utente registrato a Kaspersky Security Center Cloud Console. A tale utente vengono concessi i diritti di amministratore per l'area di lavoro creata.

  Dopo aver creato un account in Kaspersky Security Center Cloud Console, non è necessario registrare un'azienda e creare la relativa area di lavoro. Specificare le informazioni sull'azienda e sull'area di lavoro nella richiesta.

- **Nome dell'azienda**: il nome dell'azienda in cui si desidera utilizzare Kaspersky Security Center Cloud Console.
- **Paese dell'azienda**: il paese in cui è situata l'azienda.
- **Nome dell'area di lavoro**: il nome dell'area di lavoro da creare per l'azienda.
- **Numero di endpoint stimati**: il numero totale di dispositivi client (inclusi i dispositivi mobili) che si desidera proteggere nella nuova area di lavoro.
- **Paese dell'area di lavoro**: il paese in cui si desidera collocare la nuova area di lavoro. Questo parametro influisce sulla selezione del datacenter per l'archiviazione dell'area di lavoro.

  Se si desidera collocare l'area di lavoro negli Stati Uniti o in Canada, specificare lo stato o la provincia per determinare la regione del datacenter.

  I parametri **Paese dell'azienda** e **Paese dell'area di lavoro** possono essere gli stessi.
- **Codice di attivazione**: il codice di attivazione ricevuto dopo l'acquisto di Kaspersky Security Center Cloud Console. Assicurarsi che la licenza che si desidera acquistare copra tutti i dispositivi client da proteggere.

Dopo aver inviato la richiesta, gli specialisti di Kaspersky registrano l'azienda specificata e creano la relativa area di lavoro. Al termine della creazione dell'area di lavoro, si riceverà un messaggio e-mail di notifica. È possibile accedere al proprio account in Kaspersky Security Center Cloud Console per visualizzare il risultato.

Eventi di superamento del limite di licenze

Kaspersky Security Center Cloud Console consente di ottenere informazioni sugli eventi che si verificano in caso di superamento dei limiti di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client.

Il livello di importanza degli eventi quando avviene il superamento di una limitazione di licenza è definito in base alle regole seguenti:

- Se le unità attualmente in uso coperte da una singola licenza costituiscono tra il 90% e il 100% del numero totale di unità coperte dalla licenza, l'evento è pubblicato con il livello di importanza **Informazioni**.
- Se le unità attualmente in uso coperte da una singola licenza costituiscono tra il 100% e il 110% del numero totale di unità coperte dalla licenza, l'evento è pubblicato con il livello di importanza **Avviso**.
- Se il numero di unità attualmente in uso coperte da una singola licenza è superiore al 110% del numero totale di unità coperte dalla licenza, l'evento è pubblicato con il livello di importanza **Evento critico**.

Metodi di distribuzione dei codici di attivazione ai dispositivi gestiti

Le applicazioni Kaspersky installate nei dispositivi gestiti devono essere concesse in licenza applicando un codice di attivazione a ognuna delle applicazioni. Non è possibile utilizzare file chiave per il licensing delle applicazioni gestite; sono accettati solo i codici di attivazione. È possibile distribuire un codice di attivazione nei seguenti modi:

- Distribuzione automatica
- Attività di aggiunta della chiave di licenza per un'applicazione gestita
- Attivazione manuale di un'applicazione gestita

Le applicazioni Kaspersky possono utilizzare più di una chiave di licenza contemporaneamente. Kaspersky Endpoint Security for Windows può ad esempio utilizzare due chiavi di licenza: una per Kaspersky Endpoint Security for Windows e una per l'attivazione delle funzioni integrate di Kaspersky Endpoint Detection and Response.

Inoltre, le applicazioni Kaspersky possono avere non solo una chiave di licenza attiva, ma anche una chiave di licenza aggiuntiva. Un'applicazione Kaspersky utilizza una chiave attiva al momento e memorizza una chiave aggiuntiva da applicare dopo la scadenza della chiave attiva. È possibile aggiungere una nuova chiave di licenza attiva o aggiuntiva con uno dei metodi sopra elencati. L'applicazione per la quale si aggiunge una chiave di licenza definisce se la chiave è attiva o aggiuntiva. La definizione della chiave non dipende dal metodo utilizzato per aggiungere una nuova chiave di licenza.

Aggiunta di una chiave di licenza all'archivio dell'Administration Server

Quando si aggiunge una chiave di licenza utilizzando Kaspersky Security Center Cloud Console, le impostazioni della chiave di licenza vengono salvate nell'Administration Server. In base a queste informazioni, l'applicazione genera un rapporto sull'utilizzo delle chiavi di licenza e segnala all'amministratore la scadenza delle licenze e la violazione delle limitazioni di licenza specificate nelle proprietà delle chiavi di licenza. È possibile configurare le notifiche dell'utilizzo delle chiavi di licenza nelle impostazioni di Administration Server.

Per aggiungere una chiave di licenza all'archivio dell'Administration Server:

1. Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.
2. Fare clic sul pulsante **Aggiungi**.
3. Specificare il codice di attivazione nel campo di testo e fare clic sul pulsante **Invia**.
4. Fare clic sul pulsante **Chiudi**.

Una o più chiavi di licenza verranno aggiunte all'archivio dell'Administration Server.

Distribuzione di una chiave di licenza ai dispositivi client

Kaspersky Security Center Web Console consente la distribuzione di una chiave di licenza ai dispositivi client automaticamente o tramite l'attività di aggiunta della chiave.

Prima della distribuzione, aggiungere una chiave di licenza all'archivio dell'Administration Server.

Per distribuire una chiave di licenza ai dispositivi client tramite l'attività di aggiunta della chiave:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nell'elenco a discesa **Applicazione**, selezionare l'applicazione per la quale si desidera aggiungere una chiave di licenza.

4. Nell'elenco **Tipo di attività**, selezionare e aggiungere l'attività di **aggiunta della chiave**.
5. Nel campo **Nome attività**, specificare il nome della nuova attività.
6. Selezionare i dispositivi a cui verrà assegnata l'attività.
7. Nel passaggio **Selezione di una chiave di licenza** della procedura guidata, fare clic sul collegamento **Aggiungi chiave** per aggiungere la chiave di licenza.
8. Nel riquadro di aggiunta della chiave, aggiungere la chiave di licenza utilizzando una delle seguenti opzioni:

   È necessario aggiungere la chiave di licenza solo se non è stata aggiunta all'archivio dell'Administration Server prima di creare l'attività di aggiunta della chiave.

   - Selezionare l'opzione **Immettere il codice di attivazione** per immettere un codice di attivazione, quindi effettuare le seguenti operazioni:

     a. Specificare il codice di attivazione, quindi fare clic sul pulsante **Invia**.

     Le informazioni sulla chiave di licenza vengono visualizzate nel riquadro di aggiunta della chiave.

     b. Fare clic sul pulsante **Salva**.

     Se si desidera distribuire automaticamente la chiave di licenza ai dispositivi gestiti, abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

     Il riquadro di aggiunta delle chiavi viene chiuso.

   - Selezionare l'opzione **Aggiungere un file chiave** per aggiungere un file chiave, quindi effettuare le seguenti operazioni:

     a. Fare clic sul pulsante **Seleziona file chiave**.

     b. Nella finestra visualizzata, selezionare un file chiave, quindi fare clic sul pulsante **Apri**.

     Le informazioni sulla chiave di licenza vengono visualizzate nel riquadro di aggiunta della chiave di licenza.

     c. Fare clic sul pulsante **Salva**.

     Se si desidera distribuire automaticamente la chiave di licenza ai dispositivi gestiti, abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

     Il riquadro di aggiunta delle chiavi viene chiuso.

9. Selezionare la chiave di licenza nella tabella delle chiavi.
10. Nel passaggio **Informazioni sulla licenza** della procedura guidata, abilitare l'opzione **Usa come chiave di riserva** se si desidera utilizzare questa chiave come chiave di riserva.

    In questo caso, viene applicata una chiave di riserva alla scadenza della chiave attiva.
11. Nel passaggio **Completa creazione attività** della procedura guidata, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** per modificare le impostazioni predefinite dell'attività.

Se non si abilita questa opzione, l'attività verrà creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in un secondo momento.

12. Fare clic sul pulsante **Fine**.

    La procedura guidata crea l'attività: Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata automaticamente la finestra delle proprietà dell'attività. In questa finestra, è possibile specificare le impostazioni generali dell'attività e, se necessario, modificare le impostazioni specificate durante la creazione dell'attività.

    > È inoltre possibile aprire la finestra delle proprietà dell'attività facendo clic sul nome dell'attività creata nell'elenco delle attività.

    L'attività verrà creata, configurata e visualizzata nell'elenco delle attività.

13. Per eseguire l'attività, selezionarla nell'elenco delle attività, quindi fare clic sul pulsante **Avvia**.

    È inoltre possibile impostare una pianificazione per l'avvio dell'attività nella scheda **Pianificazione** della finestra delle proprietà dell'attività.

    Per una descrizione dettagliata delle impostazioni di avvio pianificato, fare riferimento alle impostazioni generali dell'attività.

Una volta completata l'attività, la chiave di licenza viene distribuita nei dispositivi selezionati.

Distribuzione automatica di una chiave di licenza

Kaspersky Security Center Cloud Console consente la distribuzione automatica delle chiavi di licenza ai dispositivi gestiti, se sono presenti nell'archivio delle chiavi di licenza in Administration Server.

Per distribuire automaticamente una chiave di licenza ai dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.
2. Fare clic sul nome della chiave di licenza da distribuire automaticamente ai dispositivi.
3. Nella finestra delle proprietà della chiave di licenza visualizzata spostare l'interruttore su **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.
4. Fare clic sul pulsante **Salva**.

La chiave di licenza verrà automaticamente distribuita a tutti i dispositivi compatibili.

La distribuzione della chiave di licenza viene eseguita tramite Network Agent. Non vengono create attività di distribuzione della chiave di licenza per l'applicazione.

Durante la distribuzione automatica di una chiave di licenza, viene tenuto in considerazione il limite di licenze relativo al numero di dispositivi. Il limite di licenze è impostato nelle proprietà della chiave di licenza. Se viene raggiunto il limite di licenze, la distribuzione della chiave di licenza nei dispositivi si interrompe automaticamente.

Se si specifica l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti** per una chiave di licenza in abbonamento per l'attivazione di un'applicazione in un dispositivo gestito e allo stesso tempo si dispone di una chiave di licenza di prova attiva, la chiave di licenza di prova verrà automaticamente sostituita dalla chiave di licenza in abbonamento otto giorni prima della data di scadenza.

Visualizzazione delle informazioni sulle chiavi di licenza in uso nell'archivio dell'Administration Server

Per visualizzare l'elenco delle chiavi di licenza aggiunte all'archivio dell'Administration Server,

Nel menu principale accedere a **Operazioni → Licensing → Licenze di Kaspersky**.

L'elenco visualizzato contiene i codici di attivazione aggiunti all'archivio dell'Administration Server.

Per visualizzare informazioni dettagliate su una chiave di licenza:

1. Nel menu principale accedere a **Operazioni → Licensing → Licenze di Kaspersky**.
2. Fare clic sul nome della chiave di licenza desiderata.

Nella finestra delle proprietà della chiave di licenza visualizzata è possibile visualizzare:

- Nella scheda **Generale**: le informazioni principali sulla chiave di licenza
- Nella scheda **Dispositivi**: l'elenco dei dispositivi client in cui è stata utilizzata la chiave di licenza per l'attivazione dell'applicazione Kaspersky installata

Visualizzazione delle informazioni sulle chiavi di licenza utilizzate per un'applicazione Kaspersky specifica

Per sapere quali chiavi di licenza sono in uso per un'applicazione Kaspersky:

1. Nel menu principale accedere a **Risorse (dispositivi) → Dispositivi gestiti**.

   Se il dispositivo appartiene al gruppo Dispositivi non assegnati, passare invece a **Individuazione e distribuzione → Dispositivi non assegnati**.
2. Fare clic sul nome del dispositivo desiderato.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la sezione **Applicazioni**.
4. Nell'elenco delle applicazioni visualizzato selezionare l'applicazione di cui si desidera visualizzare le chiavi di licenza.
5. Nella finestra delle proprietà dell'applicazione visualizzata, nella scheda **Generale**, selezionare la sezione **Chiavi di licenza**.

   Le informazioni vengono visualizzate nell'area di lavoro di questa sezione.

Eliminazione di una chiave di licenza dall'archivio

È possibile eliminare una chiave di licenza dall'archivio dell'Administration Server. Kaspersky Security Center Cloud Console elimina automaticamente l'area di lavoro dopo 90 giorni nei seguenti casi:

- È stata eliminata l'ultima chiave di licenza (attiva, aggiuntiva o non in uso) aggiunta manualmente nell'archivio.
- L'ultima chiave di licenza è in scadenza.

Se l'area di lavoro viene eliminata, non è possibile gestire la protezione della rete tramite Kaspersky Security Center Cloud Console. Inoltre, si perdono definitivamente i dati da Kaspersky Security Center Cloud Console. Se necessario, è possibile eliminare manualmente l'area di lavoro. In caso contrario, è consigliabile conservare almeno una chiave di licenza nell'archivio dell'Administration Server.

Se si elimina una chiave di licenza e precedentemente è stata aggiunta una chiave di licenza aggiuntiva, questa diventa automaticamente la chiave di licenza attiva allo scadere o all'eliminazione della precedente chiave di licenza attiva.

Quando si elimina la chiave di licenza attiva distribuita in un dispositivo gestito, l'applicazione continuerà a funzionare nel dispositivo gestito.

Per eliminare una chiave di licenza dall'archivio dell'Administration Server:

1. Verificare che Administration Server non utilizzi una chiave di licenza che si desidera eliminare. In questo caso, non è possibile eliminare la chiave. Per eseguire il controllo:

   a. Nel menu principale, fare clic sull'icona delle impostazioni () accanto ad Administration Server.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

   b. Nella scheda **Generale** selezionare la sezione **Chiavi di licenza**.

   c. Se la chiave di licenza desiderata viene visualizzata nella sezione aperta, fare clic sul pulsante **Rimuovi chiave di licenza attiva**, quindi confermare l'operazione. Successivamente, Administration Server non utilizza la chiave di licenza eliminata, ma la chiave rimane nell'archivio dell'Administration Server. Se la chiave di licenza desiderata non viene visualizzata, Administration Server non la utilizza.

2. Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.

3. Selezionare la chiave di licenza richiesta, quindi fare clic sul pulsante **Elimina**.

4. Nella finestra visualizzata selezionare la casella di controllo **Comprendo il rischio e desidero eliminare la chiave di licenza**. Ciò significa che eliminando l'ultima chiave di licenza, si è consapevoli della successiva eliminazione dell'area di lavoro e della perdita del controllo sui dispositivi gestiti. Fare clic sul pulsante **Elimina**.

Di conseguenza, la chiave di licenza selezionata viene eliminata dall'archivio.

È possibile aggiungere nuovamente una chiave di licenza eliminata o aggiungerne una nuova. Se è stata eliminata l'ultima chiave di licenza, è anche possibile aggiungere una chiave di licenza purché l'area di lavoro non venga eliminata. Kaspersky Security Center Cloud Console invia una notifica agli amministratori dell'area di lavoro 30 giorni, 7 giorni e 1 giorno prima dell'eliminazione.

Visualizzazione dell'elenco dei dispositivi in cui un'applicazione Kaspersky non è attivata

È possibile visualizzare l'elenco di tutti i dispositivi in cui è installata un'applicazione Kaspersky ma non è attivata (ad esempio una licenza non disponibile o scaduta).

Per visualizzare i dispositivi in cui un'applicazione Kaspersky non è attivata:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

   Verrà visualizzato l'elenco delle attività.

2. Fare clic sul nome dell'attività di aggiornamento correlata all'applicazione Kaspersky in questione.

   Verrà visualizzata la finestra delle proprietà dell'attività con diverse schede denominate.

3. Nella finestra delle proprietà dell'attività selezionare la sezione **Risultati**.

   Nella colonna **Dispositivo** sono visualizzati i dispositivi in cui l'attività è andata a buon fine.

4. Ordinare la colonna **Dispositivo**.

   Nella colonna **Dispositivo** sono visualizzati i dispositivi in cui l'attività è andata a buon fine. I dispositivi in cui l'attività non è andata a buon fine a causa di una licenza non disponibile sono dispositivi in cui l'applicazione non è attivata.

Revoca del consenso a un Contratto di licenza con l'utente finale

Se si decide di interrompere la protezione di alcuni dispositivi client, è possibile revocare il Contratto di licenza con l'utente finale (EULA) per qualsiasi applicazione Kaspersky gestita. È necessario disinstallare l'applicazione selezionata e i relativi pacchetti di installazione prima di revocarne il Contratto di licenza con l'utente finale. I pacchetti di installazione devono essere eliminati da Administration Server e dai relativi Administration Server virtuali.

I Contratti di licenza con l'utente finale accettati in un Administration Server virtuale possono essere revocati nell'Administration Server virtuale o nell'Administration Server primario. I Contratti di licenza con l'utente finale accettati in un Administration Server primario possono essere revocati solo nell'Administration Server primario.

Per revocare un EULA per le applicazioni Kaspersky gestite:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** della finestra delle proprietà di Administration Server selezionare la sezione **Contratti di licenza con l'utente finale**.

   Verrà visualizzato un elenco dei Contratti di licenza con l'utente finale accettati al momento della creazione dei pacchetti di installazione o dell'installazione immediata degli aggiornamenti.

3. Nell'elenco selezionare il Contratto di licenza con l'utente finale che si desidera revocare.

   È possibile visualizzare le seguenti proprietà degli EULA:

   - Data di accettazione del Contratto di licenza con l'utente finale
   - Nome dell'utente che ha accettato il Contratto di licenza con l'utente finale
   - Se il Contratto di licenza con l'utente finale può essere revocato o meno

4. Fare clic sulla data di accettazione di qualsiasi Contratto di licenza con l'utente finale per aprirne la finestra delle proprietà in cui sono visualizzati i seguenti dati:

   - Nome dell'utente che ha accettato il Contratto di licenza con l'utente finale

- Data di accettazione del Contratto di licenza con l'utente finale
- Identificatore univoco (UID) del Contratto di licenza con l'utente finale
- Testo completo del Contratto di licenza con l'utente finale
- Elenco di oggetti (pacchetti di installazione, aggiornamenti immediati) collegati al Contratto di licenza con l'utente finale e relativi nomi e tipi

5. Nella parte inferiore della finestra delle proprietà del Contratto di licenza con l'utente finale fare clic sul pulsante **Revoca Contratto di licenza**.

   Se il Contratto di licenza con l'utente finale selezionato può essere revocato solo disinstallando l'applicazione o se questo Contratto di licenza con l'utente finale può essere revocato solo nell'Administration Server primario, verrà visualizzata una notifica su questa restrizione anziché il pulsante **Revoca Contratto di licenza**.

   > Se esistono oggetti (pacchetti di installazione e rispettive attività) che impediscono la revoca del Contratto di licenza con l'utente finale, viene visualizzata la notifica corrispondente. Non è possibile procedere con la revoca fino a quando non si eliminano questi oggetti.

   Nella finestra visualizzata l'utente viene informato della necessità di disinstallare prima l'applicazione Kaspersky corrispondente al Contratto di licenza con l'utente finale.

6. Fare clic sul pulsante per confermare la revoca.

L'EULA è revocato. Non viene più visualizzato nell'elenco dei Contratti di licenza nella sezione **Contratti di licenza con l'utente finale**. La finestra delle proprietà del Contratto di licenza con l'utente finale viene chiusa; l'applicazione non è più installata.

Rinnovo delle licenze per le applicazioni Kaspersky

È possibile rinnovare una licenza dell'applicazione Kaspersky scaduta o in scadenza (fra meno di 30 giorni).

> Se l'ultima chiave di licenza è scaduta, Kaspersky Security Center Cloud Console elimina automaticamente l'area di lavoro dopo 90 giorni. Di conseguenza, non è possibile gestire la protezione della rete tramite Kaspersky Security Center Cloud Console. Inoltre, si perdono definitivamente i dati da Kaspersky Security Center Cloud Console. È consigliabile rinnovare le chiavi di licenza obsolete o aggiungerne di nuove nell'archivio dell'Administration Server per mantenere l'area di lavoro.

Per visualizzare una notifica su una licenza scaduta o una licenza che sta per scadere:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.
   - Nel menu principale, accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**, quindi fare clic sul collegamento **Visualizza licenze in scadenza** accanto a una notifica.

   Verrà visualizzata la finestra **Licenze di Kaspersky** in cui è possibile visualizzare e rinnovare le licenze scadute e in scadenza.

2. Se si desidera rinnovare una licenza, fare clic sul collegamento **Rinnova licenza** accanto alla licenza desiderata.

   Facendo clic su un collegamento per il rinnovo della licenza, si accetta di trasferire i seguenti dati a Kaspersky: ID software, versione software, localizzazione software, ID licenza e un attributo che indica se la licenza è stata fornita da un'azienda partner. I dati sono necessari per stabilire i termini di rinnovo della licenza.

3. Nella finestra del servizio di rinnovo della licenza visualizzata seguire le istruzioni per rinnovare una licenza.

   La licenza in scadenza viene rinnovata.

In Kaspersky Security Center Cloud Console le notifiche vengono visualizzate quando una licenza sta per scadere, in base alla seguente pianificazione:

- 30 giorni prima della scadenza
- 7 giorni prima della scadenza
- 3 giorni prima della scadenza
- 24 ore prima della scadenza
- Quando una licenza è scaduta

Utilizzo di Kaspersky Security Center Cloud Console dopo la scadenza della licenza

Dopo la scadenza della licenza, Kaspersky potrebbe concedere l'utilizzo di Kaspersky Security Center Cloud Console per un massimo di 90 giorni senza limitazioni. Durante questo periodo, le interfacce Web di Administration Server, Network Agent e Kaspersky Security Center Cloud Console funzionano senza limiti. Kaspersky Security Center Cloud Console invia anche le statistiche KSN a Kaspersky in base alle impostazioni di accesso KSN correnti. Le applicazioni gestite funzionano solo con funzionalità limitate (per i dettagli, consultare la documentazione per queste applicazioni).

Quando la licenza è scaduta da 90 giorni, Kaspersky Security Center Cloud Console elimina automaticamente l'area di lavoro. Se si desidera mantenere l'area di lavoro, rinnovare almeno una chiave di licenza scaduta o aggiungerne una nuova all'archivio.

Finestra Kaspersky Security Network (KSN)

In questa sezione viene descritto come utilizzare un'infrastruttura di servizi online denominata Kaspersky Security Network (KSN). Vengono fornite informazioni dettagliate su KSN e istruzioni su come abilitare KSN, configurare l'accesso a KSN e visualizzare le statistiche di utilizzo del server proxy KSN.

Informazioni su KSN

Kaspersky Security Network (KSN) è un'infrastruttura di servizi online che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora l'efficacia di alcuni componenti della protezione e riduce il rischio di falsi positivi. KSN consente di utilizzare i database di reputazione di Kaspersky per recuperare informazioni sulle applicazioni installate nei dispositivi client.

Se si partecipa a KSN, si autorizza l'invio automatico a Kaspersky di informazioni sul funzionamento delle applicazioni Kaspersky installate nei dispositivi client gestiti tramite Kaspersky Security Center Cloud Console. Le informazioni vengono trasferite in base alle impostazioni di accesso a KSN correnti. Gli analisti di Kaspersky analizzano inoltre le informazioni ricevute e le includono nei database statistici e di reputazione di Kaspersky Security Network.

All'utente verrà richiesto di partecipare a KSN durante l'esecuzione dell'Avvio rapido guidato. È possibile iniziare o smettere di utilizzare KSN in qualsiasi momento durante l'utilizzo dell'applicazione.

È necessario utilizzare KSN in conformità con l'Informativa KSN letta e accettata durante l'attivazione di KSN. Se l'Informativa KSN viene aggiornata, viene visualizzata quando si esegue l'aggiornamento o l'upgrade di Administration Server. È possibile accettare o rifiutare l'Informativa KSN aggiornata. In caso di rifiuto, si continuerà a utilizzare KSN in conformità con la versione precedente dell'Informativa KSN già accettata.

Quando KSN è abilitato, Kaspersky Security Center Cloud Console verifica se i server KSN sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. Ciò è necessario per garantire il mantenimento del livello di sicurezza per i dispositivi gestiti.

I dispositivi client gestiti da Administration Server interagiscono con KSN attraverso il server proxy KSN. Il server proxy KSN fornisce le seguenti funzionalità:

- I dispositivi client possono inviare richieste a KSN e trasferire informazioni a KSN anche se non hanno accesso diretto a Internet.
- Il server proxy KSN memorizza nella cache i dati elaborati, riducendo in tal modo il carico sul canale in uscita e il tempo di attesa per ottenere le informazioni richieste da un dispositivo client.

È possibile abilitare il proxy KSN da parte del punto di distribuzione per fare in modo che il dispositivo abbia il ruolo di Proxy KSN. In questo caso il servizio proxy KSN (ksnproxy) viene eseguito nel dispositivo.

Abilitazione e disabilitazione di KSN

Per abilitare KSN:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni KSN**.

3. Impostare l'interruttore sulla posizione **Usa Kaspersky Security Network Abilitato**.

   KSN è abilitato.

   Se l'interruttore è abilitato, i dispositivi client invieranno i risultati dell'installazione delle patch a Kaspersky. Quando si abilita questo interruttore, è necessario leggere e accettare i termini dell'informativa KSN.

4. Fare clic sul pulsante **Salva**.

Per disabilitare KSN:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni KSN**.

3. Impostare l'interruttore sulla posizione **Usa Kaspersky Security Network Disabilitato**.

   KSN è disabilitato.

   Se questo interruttore è disabilitato, i dispositivi client non invieranno i risultati dell'installazione delle patch a Kaspersky.

4. Fare clic sul pulsante **Salva**.

Visualizzazione dell'Informativa KSN accettata

Quando si abilita Kaspersky Security Network (KSN), è necessario leggere e accettare l'Informativa KSN. È possibile visualizzare l'Informativa KSN accettata in qualsiasi momento.

Per visualizzare l'Informativa KSN accettata:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome di Administration Server.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni KSN**.

3. Fare clic sul collegamento **Visualizza l'Informativa di Kaspersky Security Network**.

Nella finestra visualizzata è possibile visualizzare il testo dell'Informativa KSN accettata.

Accettazione di un'Informativa KSN aggiornata

È necessario utilizzare KSN in conformità con l'Informativa KSN letta e accettata durante l'attivazione di KSN. Se l'Informativa KSN viene aggiornata, viene visualizzata automaticamente all'apertura di Kaspersky Security Center Cloud Console. È possibile accettare o rifiutare l'Informativa KSN aggiornata. In caso di rifiuto, si continuerà a utilizzare KSN in conformità con la versione dell'Informativa KSN accettata precedentemente. È possibile visualizzare e accettare l'Informativa KSN aggiornata in un secondo momento.

Per visualizzare e successivamente accettare o rifiutare un'Informativa KSN aggiornata:

1. Fare clic sul collegamento **Visualizza notifiche** nell'angolo superiore destro della finestra principale dell'applicazione.

   Verrà visualizzata la finestra **Notifiche**.

2. Fare clic sul collegamento **Visualizza l'Informativa KSN aggiornata**.

   Verrà visualizzata la finestra **Aggiornamento dell'Informativa di Kaspersky Security Network**.

3. Leggere l'Informativa KSN, quindi prendere una decisione facendo clic su uno dei seguenti pulsanti:

   - **Accetto l'Informativa KSN aggiornata**

- **Usa KSN con l'Informativa precedente**

A seconda della scelta, KSN continuerà a funzionare in conformità con i termini dell'Informativa KSN corrente o aggiornata. È possibile visualizzare il testo dell'Informativa KSN accettata nelle proprietà di Administration Server in qualsiasi momento.

Verifica per stabilire se il punto di distribuzione funziona come server proxy KSN

In un dispositivo gestito a cui è assegnato il ruolo di punto di distribuzione è possibile abilitare il server proxy KSN. Un dispositivo gestito funziona come server proxy KSN quando il servizio ksnproxy è in esecuzione nel dispositivo. È possibile controllare, attivare o disattivare questo servizio nel dispositivo in locale.

È possibile assegnare un dispositivo basato su Windows o Linux come punto di distribuzione. Il metodo di controllo del punto di distribuzione dipende dal sistema operativo di questo punto di distribuzione.

Per verificare se il punto di distribuzione basato su Windows funziona come server proxy KSN:

1. Nel dispositivo del punto di distribuzione, in Windows, aprire **Servizi** (**Tutti i programmi** → **Strumenti di amministrazione** → **Servizi**).

2. Nell'elenco dei servizi verificare se il servizio ksnproxy è in esecuzione.

   Se il servizio ksnproxy è in esecuzione, Network Agent nel dispositivo partecipa a Kaspersky Security Network e funziona come server proxy KSN per i dispositivi gestiti inclusi nell'ambito del punto di distribuzione.

Se si desidera, è possibile disattivare il servizio ksnproxy. In questo caso Network Agent nel punto di distribuzione interrompe la partecipazione a Kaspersky Security Network. Sono necessari i diritti di amministratore locale.

Per verificare se il punto di distribuzione basato su Linux funziona come server proxy KSN:

1. Nel dispositivo del punto di distribuzione, visualizzare l'elenco dei processi in esecuzione.

2. Nell'elenco dei processi in esecuzione, controllare se il processo `/opt/kaspersky/ksc64/sbin/ksnproxy` è in esecuzione.

Se il processo `/opt/kaspersky/ksc64/sbin/ksnproxy` è in esecuzione, Network Agent nel dispositivo partecipa a Kaspersky Security Network e funziona come server proxy KSN per i dispositivi gestiti inclusi nell'ambito del punto di distribuzione.

Definizioni relative al licensing

Questa sezione contiene le definizioni per i concetti relativi al licensing delle applicazioni Kaspersky gestite tramite Kaspersky Security Center Cloud Console.

Informazioni sulla licenza

Una *licenza* concede per un determinato periodo di tempo il diritto di utilizzare Kaspersky Security Center Cloud Console, in conformità con i termini del Contratto di licenza (Contratto di licenza con l'utente finale).

L'ambito dei servizi forniti e il periodo di validità per l'utilizzo dell'applicazione dipendono dalla licenza utilizzata per attivare l'applicazione.

Sono disponibili i seguenti tipi di licenza:

- *Di prova*

  Una licenza gratuita che consente di valutare l'applicazione. Una licenza di prova ha in genere un periodo limitato.

  Alla scadenza della licenza di prova, tutte le funzionalità di Kaspersky Security Center Cloud Console 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.

  Alla scadenza di una licenza commerciale, le funzionalità chiave dell'applicazione vengono disattivate. Per continuare a utilizzare Kaspersky Security Center Cloud Console, è necessario rinnovare la licenza commerciale. Dopo la scadenza di una licenza commerciale, non è possibile continuare a utilizzare l'applicazione ed è necessario rimuoverla dal dispositivo.

  È consigliabile rinnovare la licenza prima della scadenza per assicurare la protezione costante da tutti i tipi di minacce.

Informazioni sul certificato di licenza

Un *certificato di licenza* è un documento ricevuto 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 di ordine
- Informazioni sull'utente a cui è stata concessa la licenza
- Informazioni sull'applicazione che può essere attivata con la licenza fornita
- Limite del numero di unità di licensing (ad esempio dispositivi in cui può essere utilizzata l'applicazione con la licenza fornita)
- Data di inizio del periodo di validità della licenza
- Data di scadenza della licenza o periodo licenza
- Tipo di licenza

Informazioni sulla chiave di licenza

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

È possibile aggiungere una chiave di licenza all'applicazione inserendo un *codice di attivazione*. La chiave di licenza viene visualizzata nell'interfaccia dell'applicazione come sequenza alfanumerica univoca dopo essere stata aggiunta all'applicazione.

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

Una chiave di licenza può essere attiva o aggiuntiva (o di riserva).

Una *chiave di licenza attiva* è una chiave di licenza attualmente utilizzata dall'applicazione. È possibile aggiungere una chiave di licenza attiva per una licenza di prova o commerciale. L'applicazione non può avere più di una chiave di licenza attiva.

Una *chiave di licenza aggiuntiva (o di riserva)* è una chiave di licenza che concede all'utente il diritto di utilizzare l'applicazione, pur non essendo attualmente in uso. La chiave di licenza di riserva diventa automaticamente attiva alla scadenza della licenza associata alla chiave di licenza attiva corrente. Una chiave di licenza di riserva può essere aggiunta solo se è stata già aggiunta una chiave di licenza attiva.

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

Informazioni sul codice di attivazione

Codice di attivazione è una sequenza univoca di 20 caratteri alfanumerici. Il codice di attivazione viene inserito per aggiungere una chiave di licenza che consente di attivare Kaspersky Security Center Cloud Console. Il codice di attivazione viene ricevuto all'indirizzo e-mail specificato, in seguito all'acquisto di Kaspersky Security Center Cloud Console o all'ordine della versione di prova di Kaspersky Security Center Cloud Console.

Per attivare l'applicazione utilizzando un codice di attivazione, è necessario l'accesso a Internet per stabilire la connessione con i server di attivazione Kaspersky. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici.

Se l'applicazione è stata attivata con un codice di attivazione, l'applicazione in alcuni casi invia richieste ricorrenti ai server di attivazione di Kaspersky per verificare lo stato corrente della chiave di licenza. È necessario concedere all'applicazione l'accesso a Internet per consentire l'invio delle richieste.

Se è stato smarrito il codice di attivazione dopo l'installazione dell'applicazione, contattare il partner Kaspersky da cui è stata acquistata la licenza.

Non è possibile utilizzare file chiave per l'attivazione di applicazioni gestite; sono accettati solo i codici di attivazione.

Informazioni sull'abbonamento

L'*abbonamento a Kaspersky Security Center Cloud Console* è un ordine per l'utilizzo dell'applicazione con le impostazioni selezionate (data di scadenza dell'abbonamento, numero di dispositivi protetti). È possibile registrare l'abbonamento a Kaspersky Security Center Cloud Console presso il provider di servizi (ad esempio il provider Internet). L'abbonamento può essere rinnovato manualmente o in modalità automatica; è possibile anche annullarlo.

Un abbonamento può essere limitato (ad esempio un anno) o illimitato (senza data di scadenza). Per continuare a utilizzare Kaspersky Security Center Cloud Console dopo la scadenza di un abbonamento limitato, è necessario rinnovarlo. L'abbonamento illimitato viene rinnovato automaticamente se il pagamento al provider di servizi è stato effettuato anticipatamente entro i termini.

Quando un abbonamento limitato scade, è possibile usufruire di un periodo di tolleranza per il rinnovo durante il quale l'applicazione continua a funzionare. La disponibilità e la durata del periodo di tolleranza sono definite dal provider di servizi.

Per utilizzare Kaspersky Security Center Cloud Console con abbonamento, è necessario applicare il codice di attivazione ricevuto dal provider di servizi.

È possibile applicare un codice di attivazione diverso per Kaspersky Security Center Cloud Console solo dopo la scadenza dell'abbonamento scade o in seguito all'annullamento.

A seconda del provider di servizi, il set di azioni possibili per la gestione dell'abbonamento può variare. Il provider di servizi potrebbe non fornire alcun periodo di tolleranza per il rinnovo dell'abbonamento, pertanto l'applicazione perde le funzionalità.

I codici di attivazione acquistati con l'abbonamento non possono essere utilizzati per attivare versioni precedenti di Kaspersky Security Center Cloud Console.

Quando si utilizza l'applicazione con abbonamento, Kaspersky Security Center Cloud Console tenta automaticamente di accedere al server di attivazione a intervalli di tempo specificati fino alla scadenza dell'abbonamento. Se non è possibile accedere al server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. È possibile rinnovare l'abbonamento nel sito Web del provider di servizi.

Trasmissione dei dati

Kaspersky Security Center Cloud Console consente all'Utente di identificare e controllare i dispositivi (e i proprietari dei dispositivi) connessi a Kaspersky Security Center Cloud Console mediante le funzionalità delle applicazioni gestite.

Metodi di trasmissione dei dati:

1. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.
2. Network Agent riceve i dati dal dispositivo e li trasferisce all'Administration Server.
3. Network Agent riceve i dati recuperati dall'applicazione Kaspersky gestita e li trasferisce ad Administration Server. L'elenco dei dati elaborati dalle applicazioni gestite di Kaspersky è disponibile nella Guida delle applicazioni corrispondenti.
4. I dati vengono trasferiti da Administration Server secondari in esecuzione in locale.

Kaspersky Security Center Cloud Console elimina automaticamente le aree di lavoro 30 giorni dopo la scadenza del periodo della licenza di prova, 90 giorni dopo la scadenza del periodo della licenza commerciale.

Dopo la scadenza del periodo licenza, Kaspersky salva i dati dell'utente relativi ad avvisi e incidenti nelle aree di lavoro dell'utente per 30 giorni.

In base alla licenza corrente, il periodo di archiviazione per avvisi e incidenti è di 360 giorni. Dopo tale periodo, gli avvisi e gli incidenti meno recenti vengono automaticamente eliminati.

L'eliminazione definitiva dei dati elencati in questa sezione può richiedere fino a 24 ore.

Dati inviati ai server Kaspersky

Dati inviati durante l'attivazione

Quando si utilizza il Codice di attivazione per attivare il Software, al fine di verificare la legittimità dell'utilizzo del software, l'Utente accetta di fornire periodicamente a Kaspersky le seguenti informazioni:

- Codice di attivazione
- Identificatore di attivazione univoco per la licenza corrente

Kaspersky può inoltre utilizzare queste informazioni per generare informazioni statistiche sulla distribuzione e sull'utilizzo del software Kaspersky.

Dati inviati durante l'aggiornamento

Alla ricezione degli Aggiornamenti dai server di aggiornamento del Titolare dei diritti, al fine di migliorare la qualità del meccanismo di aggiornamento, l'Utente accetta di fornire periodicamente le seguenti informazioni a Kaspersky:

- ID software ricevuto con la licenza
- Versione completa del software

- ID licenza software
- ID installazione software (PCID)
- ID avvio dell'aggiornamento software

Kaspersky può inoltre utilizzare queste informazioni per generare informazioni statistiche sulla distribuzione e sull'utilizzo del software Kaspersky.

Dati che consentono di garantire un'operatività costante e un funzionamento efficiente, nonché di verificare l'utilizzo legittimo di Kaspersky Security Center Cloud Console

Le seguenti informazioni possono essere utilizzate per lo scopo specificato:

- Nomi e versioni delle applicazioni di protezione Kaspersky connesse all'area di lavoro e il numero di dispositivi in cui sono installate queste applicazioni di protezione.
- Numero di dispositivi in cui sono installate applicazioni di protezione Kaspersky connessi a tutte le aree di lavoro e distribuzione di tali dispositivi connessi per tipo.
- Identificatore dell'area di lavoro, identificatore dell'azienda, paese e area geografica dell'area di lavoro e data di creazione dell'area di lavoro.
- Numero di utenti nell'area di lavoro, data dell'ultima autenticazione nell'area di lavoro.
- Dettagli della licenza attualmente in uso (il tipo di licenza, la limitazione licenza relativa al numero di dispositivi, il numero di dispositivi connessi e la data di scadenza della licenza precedentemente utilizzata).

Dati trasferiti quando si seguono i collegamenti nell'interfaccia di Kaspersky Security Center Cloud Console

Seguendo i collegamenti in Administration Console o Kaspersky Security Center Cloud Console, l'Utente accetta di trasferire automaticamente i seguenti dati:

- Localizzazione di Kaspersky Security Center Cloud Console
- ID licenza
- Se la licenza è stata acquistata tramite un partner

L'elenco dei dati forniti tramite ciascun collegamento dipende dalla finalità e dalla posizione del collegamento.

Dati necessari per il funzionamento dell'area di lavoro

Kaspersky Security Center Cloud Console elabora i seguenti dati:

1. Dettagli dei dispositivi rilevati nella rete dell'organizzazione

   Network Agent riceve i dati elencati di seguito dai dispositivi collegati alla rete e li trasferisce all'Administration Server:

   a. Specifiche tecniche del dispositivo rilevato e dei relativi componenti, necessarie per la loro identificazione e ricevute tramite polling di rete:

- Polling di Active Directory:

  Dispositivi Active Directory: nome distinto del dispositivo; nome del dominio Windows ricevuto dal controller di dominio; nome del dispositivo nell'ambiente Windows; nome di dominio NetBIOS; dominio DNS e nome DNS del dispositivo; account SAM (Security Account Manager) (nome di accesso al sistema utilizzato per consentire a client e server di supportare versioni precedenti del sistema operativo, come Windows NT 4.0, Windows 95, Windows 98 e LAN Manager); nome distinto del dominio; nomi distinti dei gruppi a cui appartiene il dispositivo; nome distinto dell'utente che gestisce il dispositivo; GUID e GUID principale del dispositivo.

  Quando viene eseguito il polling della rete Active Directory, vengono sottoposti a trattamento anche i seguenti tipi di dati al fine di visualizzare informazioni sull'infrastruttura gestita e sull'uso di tali informazioni da parte dell'utente, ad esempio durante la distribuzione della protezione:

- Unità organizzative di Active Directory: nome distinto dell'unità organizzativa; nome distinto del dominio; GUID e GUID principale dell'unità organizzativa.

- Domini Active Directory: nome del dominio Windows ricevuto dal controller di dominio; dominio DNS; GUID del dominio.

- Utenti di Active Directory: nome visualizzato dell'utente; nome distinto dell'utente; nome distinto del dominio; nome dell'organizzazione dell'utente; nome del reparto dove lavora l'utente; nome distinto dell'utente che agisce in qualità di manager dell'utente; nome completo dell'utente; account SAM; indirizzo e-mail; indirizzo e-mail alternativo; numero di telefono principale; numero di telefono alternativo; numero di cellulare; nome della posizione dell'utente; nomi distinti dei gruppi a cui appartiene l'utente; GUID dell'utente; SID dell'utente (SID) (valore binario univoco utilizzato per identificare l'utente come entità di sicurezza); e nome dell'entità utente (UPN): nome di accesso di tipo Internet per un utente, basato sullo standard Internet RFC 822. L'UPN è più breve del nome distinto e più semplice da ricordare. Per convenzione, l'UPN è mappato al nome di posta elettronica dell'utente.

- Gruppi Active Directory: nome distinto del gruppo; indirizzo e-mail; nome distinto del dominio; account SAM; nomi distinti di altri gruppi a cui appartiene il gruppo; gruppo di SID e GUID del gruppo.

b. Polling del dominio Samba:

   Dispositivi Samba: nome distinto del dispositivo; nome di dominio ricevuto dal controller di dominio; nome del dispositivo NetBIOS; nome di dominio NetBIOS; dominio DNS e nome DNS del dispositivo; account SAM (Security Account Manager); nome distinto del dominio; nomi distinti dei gruppi a cui appartiene il dispositivo; nome distinto dell'utente che gestisce il dispositivo; identificatore univoco globale (GUID) e GUID principale del dispositivo.

   - Unità organizzative di Samba: nome distinto dell'unità organizzativa; nome distinto del dominio; GUID e GUID principale dell'unità organizzativa.

   - Dominio Samba: nome del dominio ricevuto dal controller di dominio; dominio DNS; GUID del dominio.

   - Utenti di Samba: nome visualizzato dell'utente; nome distinto dell'utente; nome dell'organizzazione dell'utente; nome del reparto dove lavora l'utente; nome distinto dell'utente che agisce in qualità di manager dell'utente; nome completo dell'utente; account SAM; indirizzo e-mail; indirizzo e-mail alternativo; numero di telefono principale; numero di telefono alternativo; numero di cellulare; nome della posizione dell'utente; nomi distinti dei gruppi a cui appartiene l'utente; GUID dell'utente; SID dell'utente (SID) (valore binario univoco utilizzato per identificare l'utente come entità di sicurezza); nome dell'entità utente (UPN): nome di accesso di tipo Internet per un utente, basato sullo standard Internet RFC 822. L'UPN è più breve del nome distinto e più semplice da ricordare. Per convenzione, l'UPN è mappato al nome di posta elettronica dell'utente.

   - Gruppi Samba: nome distinto del gruppo; indirizzo e-mail; nome distinto del dominio; account SAM; nomi distinti di altri gruppi a cui appartiene il gruppo; SID dell'utente e GUID del gruppo.

c. Polling del dominio Windows:

- Nome del gruppo di lavoro o del dominio Windows
- Nome NetBIOS del dispositivo
- Dominio DNS e nome DNS del dispositivo
- Nome e descrizione del dispositivo
- Visibilità dispositivi nella rete
- Indirizzo IP dispositivo
- Tipo di dispositivo (workstation, server, SQL Server, controller di dominio e così via)
- Tipo di sistema operativo nel dispositivo
- Versione del sistema operativo del dispositivo
- Ora dell'ultimo aggiornamento delle informazioni sul dispositivo
- Ora dell'ultima volta in cui il dispositivo è stato visibile nella rete

d. Polling dell'intervallo IP:

- Indirizzo IP dispositivo
- Nome DNS o nome NetBIOS del dispositivo
- Nome e descrizione del dispositivo
- Indirizzo MAC del dispositivo
- Ora dell'ultima volta in cui il dispositivo è stato visibile nella rete

2. Dettagli dei dispositivi gestiti.

Network Agent trasferisce i dati elencati di seguito dal dispositivo ad Administration Server. L'utente inserisce il nome visualizzato e la descrizione del dispositivo nell'interfaccia di Kaspersky Security Center Cloud Console:

a. Le specifiche tecniche del dispositivo gestito e i relativi componenti necessari per l'identificazione, tra cui:

- Nome visualizzato (generato in base al nome NetBIOS, può essere modificato manualmente) e descrizione del dispositivo (immessa manualmente)
- Nome e tipo del dominio Windows (dominio Windows NT/gruppo di lavoro Windows)
- Nome del dispositivo nell'ambiente Windows
- Dominio DNS e nome DNS del dispositivo
- Indirizzo IP dispositivo
- Subnet mask del dispositivo
- Percorso di rete del dispositivo
- Indirizzo MAC del dispositivo

- Tipo di sistema operativo nel dispositivo
- Se il dispositivo è una macchina virtuale e il tipo di hypervisor
- Se il dispositivo è una macchina virtuale dinamica nell'ambito dell'infrastruttura VDI (Virtual Desktop Infrastructure)
- GUID del dispositivo
- ID istanza di Network Agent
- ID di installazione di Network Agent
- ID permanente di Network Agent

b. Altre specifiche dei dispositivi gestiti e dei relativi componenti richieste per il controllo dei dispositivi gestiti e per le decisioni sull'applicabilità di patch e aggiornamenti specifici:

- Stato di Windows Update Agent
- Architettura del sistema operativo
- Fornitore del sistema operativo
- Numero di build del sistema operativo
- ID di rilascio del sistema operativo
- Cartella della posizione del sistema operativo
- Se il dispositivo è una macchina virtuale, il tipo di macchina virtuale
- Tempo di attesa della risposta del dispositivo
- Se Network Agent è eseguito in modalità autonoma

c. Informazioni dettagliate sull'attività nei dispositivi gestiti:

- Data e ora dell'ultimo aggiornamento
- Data e ora dell'ultima volta in cui il dispositivo è stato visibile nella rete
- Stato in attesa di riavvio ("È necessario il riavvio.")
- Ora di accensione del dispositivo

d. Dettagli degli account utente del dispositivo e delle relative sessioni di lavoro

e. Statistiche relative alle operazioni del punto di distribuzione, se il dispositivo è un punto di distribuzione:

- Data e ora di creazione del punto di distribuzione
- Nome della cartella di lavoro
- Dimensione cartella di lavoro

- Numero di sincronizzazioni con l'Administration Server
- Data e ora dell'ultima sincronizzazione del dispositivo con l'Administration Server
- Numero e dimensioni totali dei file trasferiti
- Numero e dimensioni totali dei file scaricati dai client
- Volume dei dati scaricati dai client tramite TCP (Transmission Control Protocol)
- Volume di dati inviati ai client tramite multicasting
- Volume di dati scaricati dai client tramite multicasting
- Numero di distribuzioni multicast
- Volume totale della distribuzione multicast
- Numero di sincronizzazioni con i client dopo l'ultima sincronizzazione con l'Administration Server

f. Nome dell'Administration Server virtuale che gestisce il dispositivo

g. Dettagli dei dispositivi cloud:

- Regioni cloud
- Virtual Private Cloud (VPC)
- Zona di disponibilità cloud
- Sottorete cloud
- Gruppo di collocazione Cloud

h. Dettagli dei dispositivi mobili. L'applicazione gestita trasferisce questi dati dal dispositivo mobile ad Administration Server. L'elenco completo dei dati è disponibile nella documentazione dell'applicazione gestita.

3. Dettagli delle applicazioni Kaspersky installate nel dispositivo.

L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent:

a. Applicazioni gestite Kaspersky e componenti di Kaspersky Security Center Cloud Console installati nel dispositivo

b. Impostazioni delle applicazioni Kaspersky installate nel dispositivo gestito:

- Nome e versione dell'applicazione Kaspersky
- Stato
- Stato protezione in tempo reale
- Data e ora dell'ultima scansione del dispositivo
- Numero di minacce rilevate

- Numero di oggetti che non è stato possibile disinfettare
- Attività per l'applicazione di protezione Kaspersky
- Disponibilità e stato dei componenti dell'applicazione
- Ora dell'ultimo aggiornamento e versione dei database anti-virus
- Dettagli delle impostazioni dell'applicazione Kaspersky
- Informazioni sulle chiavi di licenza attive
- Informazioni sulle chiavi di licenza aggiuntive
- Data di installazione dell'applicazione
- ID di installazione dell'applicazione

c. Statistiche sull'esecuzione dell'applicazione: eventi relativi alle modifiche dello stato dei componenti dell'applicazione Kaspersky nel dispositivo gestito e alle prestazioni delle attività avviate dai componenti dell'applicazione

d. Stato del dispositivo definito dall'applicazione Kaspersky

e. Tag assegnati dall'applicazione Kaspersky

f. Set di aggiornamenti installati e applicabili per l'applicazione Kaspersky:

- Nome visualizzato, versione e lingua dell'applicazione
- Nome interno dell'applicazione
- Nome e versione dell'applicazione dalla chiave del Registro di sistema
- Cartella di installazione dell'applicazione
- Versione della patch
- Elenco delle patch automatiche dell'applicazione installate
- Se l'applicazione è supportata da Kaspersky Security Center Cloud Console
- Se l'applicazione è installata in un cluster

g. Dettagli degli errori di criptaggio dei dati nei dispositivi: ID errore, ora dell'occorrenza, tipo di operazione (criptaggio/decriptaggio), descrizione dell'errore, percorso del file, descrizione della regola di criptaggio, ID del dispositivo e nome utente

4. Eventi dei componenti Kaspersky Security Center Cloud Console e delle applicazioni Kaspersky gestite.

   Network Agent trasferisce i dati dal dispositivo ad Administration Server.

   La descrizione di un evento può contenere i dati seguenti:

   a. Nome dispositivo

   b. Nome utente del dispositivo

c. Nome dell'amministratore che ha collegato il dispositivo da remoto

d. Nome, versione e fornitore dell'applicazione installata sul dispositivo

e. Percorso della cartella di installazione dell'applicazione sul dispositivo

f. Percorso del file sul dispositivo e nome del file

g. Nome dell'applicazione e parametri della riga di comando utilizzata per eseguire l'applicazione

h. Nome della patch, nome del file di patch, ID della patch, livello della vulnerabilità corretta dalla patch, descrizione dell'errore di installazione della patch

i. Indirizzo IP dispositivo

j. Indirizzo MAC del dispositivo

k. Stato di riavvio del dispositivo

l. Nome dell'attività che ha pubblicato l'evento

m. Se il dispositivo è passato in modalità autonoma e perché

n. Informazioni sul problema di protezione nel dispositivo: tipo di problema di protezione, nome del problema di protezione, livello di criticità, descrizione del problema di protezione, dettagli sul problema di protezione trasmessi dall'applicazione Kaspersky

o. Quantità di spazio libero su disco nel dispositivo

p. Se l'applicazione Kaspersky viene eseguita in modalità con funzionalità limitate, gli ID degli ambiti funzionali

q. Vecchio e nuovo valore dell'impostazione dell'applicazione Kaspersky

r. Descrizione dell'errore che si è verificato quando l'applicazione Kaspersky o uno qualsiasi dei suoi componenti ha eseguito l'operazione

5. Impostazioni dei componenti di Kaspersky Security Center Cloud Console e delle applicazioni Kaspersky gestite indicate nei criteri e nei profili criterio.

   L'utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.

6. Impostazioni delle attività dei componenti Kaspersky Security Center Cloud Console e delle applicazioni Kaspersky gestite

   L'utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.

7. Dati elaborati dalla funzionalità Vulnerability e patch management.

   Network Agent trasferisce i dati elencati di seguito dal dispositivo ad Administration Server:

   a. Dettagli delle applicazioni e patch installate nei dispositivi gestiti (registro delle applicazioni). Le applicazioni possono essere identificate sulla base delle informazioni sui file eseguibili rilevati nei dispositivi gestiti dalla funzionalità Controllo Applicazioni:

      - ID dell'applicazione/patch
      - ID applicazione principale (per una patch)

- Nome e versione dell'applicazione/patch
- Se l'applicazione/patch è un file MSI di Windows Installer
- Fornitore dell'applicazione/patch
- ID della lingua di localizzazione
- Data di installazione applicazione/patch
- Percorso di installazione dell'applicazione
- Sito Web del Servizio di assistenza tecnica del fornitore dell'applicazione/patch
- Numero telefonico del Servizio di assistenza tecnica
- ID dell'istanza dell'applicazione installata
- Commento
- Chiave di disinstallazione
- Chiave di installazione in modalità automatica
- Classificazione patch
- Indirizzo Web per maggiori informazioni sulla patch
- Chiave del Registro di sistema dell'applicazione
- Numero di build dell'applicazione
- SID dell'utente
- Tipo di sistema operativo (Windows, Unix)

b. Informazioni relative all'hardware rilevato sui dispositivi gestiti (registro hardware):

- ID dispositivo
- Tipo di dispositivo (scheda madre, CPU, RAM, dispositivo di archiviazione di massa, scheda video, scheda audio, Network Interface Controller, monitor, dispositivo disco ottico)
- Nome dispositivo
- Descrizione
- Fornitore
- Numero di serie
- Revisione
- Informazioni sul driver: sviluppatore, versione, descrizione e data di rilascio
- Informazioni sul BIOS: sviluppatore, versione, numero di serie e data di rilascio

- Chipset
- Frequenza di clock
- Numero di core della CPU
- Numero di thread per CPU
- Piattaforma CPU
- Velocità di rotazione del dispositivo di archiviazione
- RAM: tipo, codice
- Memoria video
- Codec della scheda audio

c. Dettagli delle vulnerabilità del software di terzi rilevate nei dispositivi gestiti:

- Identificatore vulnerabilità
- Livello di criticità della vulnerabilità (Avviso, Alto, Critico)
- Tipo di vulnerabilità (Microsoft, di terze parti)
- Indirizzo Web della pagina contenente la descrizione della vulnerabilità
- Ora di creazione della voce vulnerabilità
- Nome fornitore
- Nome del fornitore dell'applicazione
- ID del fornitore
- Nome applicazione
- Nome localizzato dell'applicazione
- Codice di installazione dell'applicazione
- Versione applicazione
- Lingua di localizzazione dell'applicazione
- Elenco degli identificatori CVE basato sulla descrizione delle vulnerabilità
- Tecnologie di protezione Kaspersky che bloccano la vulnerabilità (Protezione minacce file, Rilevamento del Comportamento, Protezione minacce Web, Protezione minacce di posta, Prevenzione Intrusioni Host, ZETA Shield)
- Percorso del file oggetto in cui è stata rilevata la vulnerabilità
- Orario di rilevamento della vulnerabilità

- ID degli articoli della Knowledge Base basati sulla descrizione della vulnerabilità
- ID dei bollettini sulla sicurezza basati sulla descrizione della vulnerabilità
- Elenco di aggiornamenti per la vulnerabilità
- Se esiste o meno un exploit per la vulnerabilità
- Se esiste o meno un malware per la vulnerabilità

d. Dettagli degli aggiornamenti disponibili per applicazioni di terzi installate sui dispositivi gestiti:

- Nome e versione dell'applicazione
- Fornitore
- Lingua di localizzazione dell'applicazione
- Sistema operativo
- Elenco di patch in base alla sequenza di installazione
- Versione originale dell'applicazione a cui è applicata la patch
- Versione dell'applicazione dopo l'applicazione della patch
- ID della patch
- Numero build
- Flag di installazione
- Contratto di licenza per la patch
- Se la patch è un prerequisito per l'installazione di altre patch
- Elenco delle applicazioni richieste installate e dei relativi aggiornamenti
- Fonti di informazioni sulla patch
- Ulteriori informazioni sulla patch (indirizzi delle pagine Web)
- Indirizzo Web per il download della patch, nome del file, versione, revisione e SHA-256

e. Dettagli degli aggiornamenti Microsoft rilevati dalla funzionalità WSUS:

- Numero di revisione dell'aggiornamento
- Tipo di aggiornamento Microsoft (Driver, Software, Categoria, Detectoid)
- Livello di importanza dell'aggiornamento secondo il bollettino Microsoft Security Response Center (MSRC) (Basso, Medio, Alto, Critico)
- ID dei bollettini MSRC correlati all'aggiornamento
- ID degli articoli della MSRC Knowledge Base

- Nome aggiornamento (intestazione)
- Descrizione dell'aggiornamento
- Se il programma di installazione degli aggiornamenti è interattivo
- Flag di installazione
- Classificazione degli aggiornamenti (Aggiornamenti critici, Aggiornamenti definizione, Driver, Feature Pack, Aggiornamenti della protezione, Service Pack, Strumenti, Aggiornamenti cumulativi, Aggiornamenti, Upgrade)
- Informazioni sull'applicazione di cui viene eseguito l'aggiornamento
- ID del Contratto di licenza con l'utente finale (EULA)
- Testo dell'EULA
- Se l'EULA deve essere accettato per eseguire l'aggiornamento dell'applicazione
- Informazioni sugli aggiornamenti associati (ID e numero di revisione)
- ID dell'aggiornamento (identificativo dell'aggiornamento Microsoft Windows globale)
- ID degli aggiornamenti sostituiti
- Se l'aggiornamento è nascosto
- Se l'aggiornamento è obbligatorio
- Stato dell'installazione dell'aggiornamento (Non applicabile, Non assegnato per l'installazione, Assegnato, Installazione in corso, Installato, Non riuscito, È necessario il riavvio, Non assegnato per l'installazione (nuova versione))
- ID CVE per l'aggiornamento
- Azienda che ha rilasciato l'aggiornamento oppure il valore "Azienda mancante"

f. Elenco degli aggiornamenti Microsoft rilevati dalla funzionalità WSUS che devono essere installati nel dispositivo.

8. Informazioni sui file eseguibili rilevati sui dispositivi gestiti dalla funzionalità Controllo Applicazioni (possono essere associate a informazioni del registro delle applicazioni). Un elenco completo dei dati è fornito nella sezione che descrive i dati relativi ai dispositivi gestiti mediante la relativa applicazione.

   L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent.

9. Informazioni sui file presenti in Backup. Un elenco completo dei dati è fornito nella sezione che descrive i dati relativi ai dispositivi gestiti mediante la relativa applicazione.

   L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent.

10. Informazioni sui file richiesti dagli specialisti Kaspersky per l'analisi dettagliata. Un elenco completo dei dati è fornito nella sezione che descrive i dati relativi ai dispositivi gestiti mediante la relativa applicazione.

    L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent.

11. Informazioni sullo stato e sull'attivazione delle regole di Controllo adattivo delle anomalie. Un elenco completo dei dati è fornito nella sezione che descrive i dati relativi ai dispositivi gestiti mediante la relativa applicazione.

L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent.

12. Informazioni sui dispositivi (unità di memoria, strumenti per il trasferimento di informazioni, strumenti per la copia cartacea di informazioni e bus di connessione) installati o connessi al dispositivo gestito e rilevati dalla funzionalità Controllo Dispositivi. Un elenco completo dei dati è fornito nella sezione che descrive i dati relativi ai dispositivi gestiti mediante la relativa applicazione.

    L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent.

13. Dati sugli avvisi:

    - Data e ora del primo evento di telemetria nell'avviso
    - Data e ora dell'ultimo evento di telemetria nell'avviso
    - Nome della regola attivata (inserito dall'utente nell'interfaccia di Kaspersky Security Center Cloud Console)
    - Stato dell'avviso
    - Risoluzione (falso positivo, vero positivo, priorità bassa)
    - ID e nome dell'utente assegnato per l'avviso
    - ID univoco nel database di Kaspersky Security Center Cloud Console e nome del dispositivo correlato agli eventi che generano avvisi
    - SID e nome dell'utente del dispositivo correlato agli eventi che generano avvisi
    - Elementi osservabili, cioè dati osservabili correlati agli eventi che generano avvisi:
        - Indirizzo IP
        - Hashsum MD5 del file e percorso del file
        - Indirizzo Web
        - Dominio
    - Dettagli aggiuntivi dell'oggetto correlato all'avviso (ricevuti dall'applicazione)
    - Commenti relativi all'avviso:
        - Data e ora in cui è stato aggiunto il commento
        - Utente che ha aggiunto il commento
        - Testo del commento
    - Registro modifiche relative agli avvisi:
        - Data e ora della modifica
        - Utente che ha eseguito la modifica
        - Descrizione della modifica

14. Dati sui problemi di sicurezza:

- Data e ora del primo evento nel problema di sicurezza
- Data e ora dell'ultimo evento nel problema di sicurezza
- Nome del problema di sicurezza (inserito dall'utente nell'interfaccia di Kaspersky Security Center Cloud Console)
- Breve descrizione del problema di sicurezza
- Priorità del problema di sicurezza
- Stato del problema di sicurezza
- ID e nome dell'utente assegnato per il problema di sicurezza
- Risoluzione (falso positivo, vero positivo, priorità bassa, unito)
- Commento al problema di sicurezza:
  - Data e ora in cui è stato aggiunto il commento
  - Utente che ha aggiunto il commento
  - Testo del commento
- Registro delle modifiche del problema di sicurezza:
  - Data e ora della modifica
  - Utente che ha eseguito la modifica
  - Descrizione della modifica

15. Dati elaborati dalla funzionalità di criptaggio dei dati delle applicazioni Kaspersky.

    L'applicazione gestita trasferisce i dati elencati di seguito dal dispositivo ad Administration Server tramite Network Agent. L'utente inserisce la descrizione dell'unità nell'interfaccia di Kaspersky Security Center Cloud Console:

    a. Elenco delle unità nei dispositivi:
       - Nome dell'unità
       - Stato criptaggio
       - Tipo di unità (unità di avvio, unità disco)
       - Numero di serie dell'unità
       - Descrizione

    b. Dettagli degli errori di criptaggio dei dati nei dispositivi:
       - Data e ora in cui si è verificato l'errore
       - Tipo di operazione (criptaggio, decriptaggio)

- Descrizione errore
- Percorso del file
- Descrizione della regola
- ID dispositivo
- Nome utente
- ID errore

c. Impostazioni di criptaggio dei dati dell'applicazione Kaspersky.

Un elenco completo dei dati è fornito nella sezione che descrive i dati relativi ai dispositivi gestiti mediante la relativa applicazione.

16. Dettagli dei codici di attivazione inseriti.

L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.

17. Account utente.

L'Utente inserisce i dati elencati di seguito nell'interfaccia di Kaspersky Security Center Cloud Console:

a. Nome

b. Descrizione

c. Nome completo

d. Indirizzo e-mail

e. Numero di telefono principale

f. Password

18. Dati necessari per l'autenticazione dell'utente tramite Active Directory:

a. Impostazioni di Active Directory Federation Services (ADFS):

- URL principale del provider del servizio di autenticazione
- Certificati radice attendibili per ADFS
- ID cliente generato in ADFS
- Chiave segreta per la protezione dell'accesso ad ADFS
- Ambito dei token
- Dominio Active Directory con cui viene eseguita l'integrazione
- Nome del campo token contenente il SID dell'utente
- Nome del campo token contenente l'array di SID dei gruppi dell'utente

L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.

b. Dati che Kaspersky Security Center Cloud Console riceve automaticamente dal server ADFS:

- Emittente (emittente)
- Endpoint di autorizzazione dell'utente (authorization_endpoint)
- Endpoint di token (token_endpoint)
- URI di JSON Web Key Set (JWKS) (jwks_uri)
- Emittente del token di accesso (access_token_issuer)
- Endpoint delle informazioni sull'utente (userinfo_endpoint)
- Endpoint di fine sessione (end_session_endpoint)
- Certificati per la firma di token

19. Cronologia delle revisioni degli oggetti di gestione: Administration Server, Gruppo di amministrazione, Criterio, Attività, Utente/gruppo di protezione, Pacchetto di installazione.

    L'Utente inserisce i dati elencati di seguito nell'interfaccia di Kaspersky Security Center Cloud Console:

    a. Administration Server

    b. Gruppo di amministrazione

    c. Criterio

    d. Attività

    e. Utente/gruppo di protezione

    f. Pacchetto di installazione

20. Registro degli oggetti di gestione dettagliati.

    L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.

21. Pacchetti di installazione creati dal file, nonché impostazioni di installazione.

    L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.

22. Dati necessari per la visualizzazione degli annunci di Kaspersky in Kaspersky Security Center Cloud Console:

    a. Informazioni sulle applicazioni Kaspersky gestite utilizzate dall'Utente: ID applicazione, numero di versione completo.

    b. La localizzazione dell'Utente dell'interfaccia di Kaspersky Security Center Cloud Console.

    c. Informazioni sull'attivazione del Software nel Dispositivo: ID licenza Software; periodo licenza del Software; data e ora di scadenza della licenza Software; tipo di licenza Software utilizzata; tipo di abbonamento Software; data e ora di scadenza dell'abbonamento Software; stato corrente dell'abbonamento Software; motivo dello stato corrente/in fase di modifica dell'abbonamento Software; ID dell'elemento del listino da cui è stata acquistata la licenza Software.

    d. Informazioni sul contratto legale accettato dall'Utente durante l'utilizzo del Software: tipo di contratto legale; versione del contratto legale; contrassegno indicante se l'utente ha accettato i termini del contratto legale.

e. Informazioni sugli annunci ricevuti dal Titolare dei diritti: ID annuncio; ora di ricezione dell'annuncio; stato di ricezione dell'annuncio.

L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.

23. Impostazioni utente di Kaspersky Security Center Cloud Console.

    L'Utente inserisce i dati elencati di seguito nell'interfaccia di Kaspersky Security Center Cloud Console:

    a. Lingua di localizzazione dell'interfaccia utente

    b. Tema dell'interfaccia utente

    c. Impostazioni di visualizzazione del riquadro di monitoraggio

    d. Informazioni sullo stato delle notifiche: Già letta/Non ancora letta

    e. Stato delle colonne nei fogli di calcolo: Mostra/Nascondi

    f. Stato di avanzamento del tutorial

24. Dati ricevuti durante l'utilizzo della funzionalità di diagnostica remota su un dispositivo gestito: file di traccia, informazioni di sistema, dettagli delle applicazioni Kaspersky installate nel dispositivo, file di dump, file di registro, risultati dell'esecuzione di script diagnostici ricevuti dall'Assistenza tecnica Kaspersky.

25. Dati che l'utente inserisce nell'interfaccia di Kaspersky Security Center Cloud Console:

    a. Nome del gruppo di amministrazione quando si crea una gerarchia di gruppi di amministrazione

    b. Indirizzo e-mail quando si configurano le notifiche tramite e-mail

    c. Tag per i dispositivi e regole per l'assegnazione di tag

    d. Tag per le applicazioni

    e. Categorie utente di applicazioni

    f. Nome del ruolo quando si assegna un ruolo a un utente

    g. Informazioni sulle subnet: nome della subnet, descrizione, indirizzo e mask

    h. Impostazioni di rapporti e selezioni

    i. Qualsiasi altro dato inserito dall'Utente

26. Dati ricevuti da un Administration Server secondario distribuito in locale.

    I dati elaborati da Kaspersky Security Center Administration Server sono descritti nella Guida in linea di Kaspersky Security Center.

    Quando si connette un Kaspersky Security Center Administration Server distribuito in locale come secondario nell'ambito della soluzione Kaspersky Security Center Cloud Console, Kaspersky Security Center Cloud Console esegue il trattamento dei seguenti tipi di dati provenienti dall'Administration Server secondario:

    a. Informazioni sui dispositivi nella rete dell'organizzazione ricevute in seguito alla device discovery nella rete di Active Directory o nella rete Windows oppure tramite la scansione degli intervalli IP

b. Informazioni relative a unità organizzative di Active Directory, domini, utenti e gruppi ricevute in seguito al polling della rete Active Directory

c. Informazioni relative ai dispositivi gestiti, relative specifiche tecniche, tra qui quelle necessarie per l'identificazione dei dispositivi, account degli utenti dei dispositivi e relative sessioni di lavoro

d. Informazioni sui dispositivi mobili trasferite mediante il protocollo Exchange ActiveSync

e. Informazioni sui dispositivi mobili trasferite mediante il protocollo MDM iOS

f. Dettagli delle applicazioni Kaspersky installate sul dispositivo: impostazioni, statistiche delle operazioni, stato del dispositivo definito dall'applicazione, aggiornamenti installati e applicabili, tag

g. Informazioni trasferite con le impostazioni dell'evento dai componenti di Kaspersky Security Center e dalle applicazioni Kaspersky gestite

h. Impostazioni dei componenti Kaspersky Security Center e delle applicazioni Kaspersky gestite presenti nei criteri e nei profili criterio

i. Impostazioni delle attività dei componenti Kaspersky Security Center e delle applicazioni Kaspersky gestite

j. Dati elaborati dalla funzionalità Vulnerability e patch management: dettagli relativi ad applicazioni e patch; informazioni sull'hardware; dettagli delle vulnerabilità del software di terzi rilevate nei dispositivi gestiti; dettagli degli aggiornamenti disponibili per applicazioni di terzi; dettagli degli aggiornamenti Microsoft rilevati dalla funzionalità WSUS

k. Categorie utente di applicazioni

l. Dettagli dei file eseguibili rilevati sui dispositivi gestiti dalla funzionalità Controllo Applicazioni

m. Dettagli dei file collocati in Backup

n. Dettagli dei file collocati in Quarantena

o. Dettagli dei richiesti dagli esperti Kaspersky per eseguire analisi dettagliate

p. Informazioni sullo stato e sull'attivazione delle regole di Controllo adattivo delle anomalie

q. Dettagli dei dispositivi (unità di memoria, strumenti per il trasferimento di informazioni, strumenti per la copia cartacea di informazioni e bus di connessione) installati o connessi al dispositivo gestito e rilevati dalla funzionalità Controllo Applicazioni

r. Impostazioni di criptaggio dell'applicazione Kaspersky: archivio delle chiavi di criptaggio, stato di criptaggio del dispositivo

s. Informazioni sugli errori relativi al criptaggio eseguito sui dispositivi mediante la funzionalità Criptaggio dei dati delle applicazioni Kaspersky

t. Elenco dei PLC (Programmable Logic Controller) gestiti

u. Dettagli dei codici di attivazione immessi

v. Account utente

w. Cronologia delle revisioni degli oggetti di gestione

x. Registro degli oggetti di gestione eliminati

y. Pacchetti di installazione creati dal file, nonché impostazioni di installazione

z. Impostazioni utente di Kaspersky Security Center Web Console

aa. Tutti i dati che l'utente immette in Administration Console o nell'interfaccia di Kaspersky Security Center Cloud Console

ab. Certificato di connessione sicura dei dispositivi gestiti ai componenti di Kaspersky Security Center

27. Informazioni caricate dal dispositivo gestito utilizzando la funzionalità Diagnostica remota: file di diagnostica (file di dump, file di log, file di traccia, ecc.) e dati contenuti in tali file.

28. Dati necessari per l'integrazione di Kaspersky Security Center Cloud Console con un sistema SIEM per l'esportazione degli eventi:

- Dati necessari per la connessione e l'autenticazione:
  - Porta e indirizzo di connessione del sistema SIEM
  - Certificato di autenticazione del server SIEM
  - Certificato attendibile e chiave privata per l'autenticazione del client di Kaspersky Security Center Cloud Console nel sistema SIEM

  L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.
- Dati che Kaspersky Security Center Cloud Console riceve dal sistema SIEM: chiave pubblica del certificato del server SIEM per l'autenticazione del server SIEM

29. Dati necessari per l'interazione di Kaspersky Security Center Cloud Console con l'ambiente cloud:

a. Amazon Web Services (AWS):

- ID chiave di accesso dell'account utente IAM
- Chiave segreta dell'account utente IAM

b. Microsoft Azure:

- ID applicazione Azure
- ID sottoscrizione Azure
- Password dell'applicazione Azure
- Nome account per il repository Azure
- Chiave di accesso all'account per il repository Azure

c. Google Cloud:

- E-mail client Google
- ID progetto
- Chiave privata

L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Cloud Console.

30. Dati trasferiti da un'applicazione Kaspersky non supportata

    Quando si installa Network Agent in un dispositivo in cui è installata un'applicazione Kaspersky che non è supportata da Kaspersky Security Center Cloud Console, questa applicazione Kaspersky trasferirà comunque i dati a Kaspersky Security Center Cloud Console. (L'elenco dei dati è disponibile nella sezione "Informazioni sulla trasmissione dei dati" della Guida dell'applicazione.) Tuttavia, Kaspersky Security Center Cloud Console non sarà in grado di elaborare i dati trasferiti dall'applicazione non supportata nel modo descritto per il processo per la funzionalità principale di Kaspersky Security Center Cloud Console.

    L'elenco delle applicazioni Kaspersky supportate è disponibile nella Guida in linea di Kaspersky Security Center Cloud Console.

Dati necessari per il funzionamento delle applicazioni gestite

Le seguenti applicazioni gestite trasferiscono i dati dal dispositivo ad Administration Server tramite Network Agent:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Security for Windows Server
- Kaspersky Security for Mobile
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Embedded Systems Security for Linux

L'elenco dei dati elaborati è pubblicato alla pagina https://ksc.kaspersky.com/home/legaldocuments?locale=it, nell'Accordo di elaborazione dei dati di Kaspersky Security Center Cloud Console. Nella pagina Web dei documenti legali individuare la sezione di testo denominata Contratto di Kaspersky Security Center Cloud Console, quindi scorrere verso il basso fino alla sezione che descrive i dati relativi ai dispositivi gestiti mediante la relativa applicazione. In alternativa, è anche possibile utilizzare la funzionalità di ricerca predefinita del browser in uso.

Dati degli utenti elaborati in locale

L'unico componente di Kaspersky Security Center che può essere distribuito in locale in Kaspersky Security Center Cloud Console è Network Agent.

Elenco dei dati degli utenti elaborati in locale:

- Tutti i dati elencati nella sezione Dati utente elaborati nell'ambito e nell'infrastruttura di Kaspersky, ad eccezione dei dati immessi dall'amministratore tramite l'interfaccia di Kaspersky Security Center Cloud Console
- Registro eventi Kaspersky di Network Agent

- Tracce di Network Agent
- Registri, inclusi i registri creati dal programma di installazione di Network Agent, le utilità di Kaspersky Security Center

I file di dump, di registro e di traccia di Network Agent contengono dati casuali e possono contenere dati personali. I file vengono archiviati non criptati nel dispositivo in cui è installato Network Agent. I file non vengono trasferiti automaticamente a Kaspersky. L'utente può trasferire questi dati a Kaspersky manualmente su richiesta del Servizio di assistenza tecnica per risolvere problemi nel funzionamento di Kaspersky Security Center.

Processori aggiuntivi di dati personali

Oltre a Kaspersky, i processori di dati personali relativi all'area di lavoro per Kaspersky Security Center Cloud Console sono elencati di seguito:

Nome e indirizzo dell'organizzazione:
Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park, Leopardstown
Dublino 18 D18 P521

Servizio:
Microsoft Azure (hosting di dati)

I paesi in cui vengono elaborati i dati sono elencati nella sezione "Selezione dei datacenter utilizzati per l'archiviazione delle informazioni di Kaspersky Security Center Cloud Console".

Informazioni sui documenti legali di Kaspersky Security Center Cloud Console

Per utilizzare Kaspersky Security Center Cloud Console, è necessario leggere e accettare i termini e le condizioni dei documenti legali specificati nel sito Web di Kaspersky Security Center Cloud Console. È possibile visualizzare i termini e le condizioni dell'Informativa sulla privacy per i siti Web di AO Kaspersky Lab quando si accede a Kaspersky Security Center Cloud Console per gestire un'area di lavoro. È possibile leggere il Contratto di Kaspersky Security Center Cloud Console e l'Accordo di elaborazione dei dati di Kaspersky Security Center Cloud Console quando si crea un'area di lavoro aziendale.

Leggere attentamente i testi di tutti i documenti legali prima di iniziare a utilizzare Kaspersky Security Center Cloud Console.

Contratto di licenza con l'utente finale per le applicazioni Kaspersky

Il Contratto di licenza con l'utente finale (di seguito denominato Contratto di licenza o EULA) è un accordo vincolante tra l'utente e AO Kaspersky Lab, in cui sono definite le condizioni di utilizzo delle applicazioni Kaspersky.

È possibile visualizzare le condizioni del Contratto di licenza con l'utente finale utilizzando i seguenti metodi:

- Nella finestra visualizzata durante la creazione del pacchetto di installazione dell'applicazione Kaspersky.
- Nel file license.txt nella cartella di installazione dell'applicazione Kaspersky, nel dispositivo gestito.

È possibile revocare l'accettazione del Contratto di licenza con l'utente finale in qualsiasi momento.

Se non si accettano le condizioni del Contratto di licenza per un'applicazione Kaspersky, non è possibile utilizzare l'applicazione.

Guida di protezione avanzata

Kaspersky Security Center Cloud Console è un'applicazione ospitata e gestita da Kaspersky. Non è necessario installare Kaspersky Security Center Cloud Console nel computer o nel server. Kaspersky Security Center Cloud Console consente all'amministratore di installare le applicazioni di protezione Kaspersky nei dispositivi in una rete aziendale, eseguire in remoto attività di scansione e aggiornamento e gestire i criteri di sicurezza delle applicazioni gestite.

Kaspersky Security Center Cloud Console è progettato per l'esecuzione centralizzata delle attività di base di amministrazione e manutenzione nella rete di un'organizzazione. L'applicazione fornisce all'amministratore l'accesso a informazioni dettagliate sul livello di sicurezza della rete dell'organizzazione. Kaspersky Security Center Cloud Console consente di configurare tutti i componenti della protezione creati utilizzando le applicazioni Kaspersky.

Kaspersky Security Center Cloud Console ha accesso completo alla gestione della protezione dei dispositivi client ed è il componente più importante del sistema di sicurezza dell'organizzazione. Pertanto, sono necessari metodi di protezione avanzati per Kaspersky Security Center Cloud Console.

Nella Guida di protezione avanzata, sono descritti i suggerimenti e le caratteristiche della configurazione di Kaspersky Security Center Cloud Console e dei suoi componenti, intesi a ridurre i rischi di compromissione.

La Guida di protezione avanzata contiene le seguenti informazioni:

- Configurazione degli account per accedere a Kaspersky Security Center Cloud Console
- Gestione della protezione dei dispositivi client
- Configurazione della protezione per le applicazioni gestite
- Trasferimento di informazioni ad applicazioni di terzi

Prima di iniziare a utilizzare Kaspersky Security Center Cloud Console, verrà richiesto di leggere la versione breve della Guida di protezione avanzata.

Si noti che non è possibile utilizzare Kaspersky Security Center Cloud Console finché non si conferma di aver letto la Guida di protezione avanzata.

Per leggere la Guida di protezione avanzata:

1. Aprire Kaspersky Security Center Cloud Console e accedere. Kaspersky Security Center Cloud Console controlla se l'utente ha confermato di aver letto la versione corrente della Guida di protezione avanzata.

   Se la Guida di protezione avanzata non è ancora stata letta, si apre una finestra che ne mostra una versione breve.

2. Eseguire una delle seguenti operazioni:

   - Se si desidera visualizzare la versione breve della Guida di protezione avanzata come documento di testo, fare clic sul collegamento **Apri in una nuova finestra**.
   - Se si desidera visualizzare la versione completa della Guida di protezione avanzata, fare clic sul collegamento **Apri Guida di protezione avanzata nella Guida in linea**.

3. Dopo aver letto la Guida di protezione avanzata, selezionare la casella di controllo **Confermo di aver letto e compreso integralmente la Guida di protezione avanzata**, quindi fare clic sul pulsante **Accetta**.

A questo punto, è possibile utilizzare Kaspersky Security Center Cloud Console.

Quando viene visualizzata una nuova versione della Guida di protezione avanzata, Kaspersky Security Center Cloud Console richiederà di leggerla.

Architettura di Kaspersky Security Center Cloud Console

In generale, la scelta di un'architettura di gestione centralizzata dipende dalla posizione dei dispositivi protetti, dall'accesso da reti adiacenti, dagli schemi di distribuzione degli aggiornamenti del database e così via.

Nella fase iniziale dello sviluppo dell'architettura, si consiglia di familiarizzare con i componenti di Kaspersky Security Center Cloud Console e con le modalità di interazione tra essi, così come con gli schemi per il traffico dati e l'utilizzo delle porte.

Sulla base di queste informazioni, è possibile formare un'architettura che specifichi:

- Organizzazione delle aree di lavoro dell'amministratore e modalità di connessione a Kaspersky Security Center Cloud Console
- I metodi di distribuzione per Network Agent e il software di protezione
- L'utilizzo dei punti di distribuzione
- L'utilizzo di Administration Server virtuali
- L'utilizzo di una gerarchia di Administration Server
- Lo schema di aggiornamento del database anti-virus
- Altri flussi informativi

Account e autenticazione

Utilizzo della verifica in due passaggi con Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console fornisce la verifica in due passaggi per gli utenti.

La verifica in due passaggi può contribuire a potenziare la sicurezza dell'account in Kaspersky Security Center Cloud Console. Quando questa funzionalità è abilitata, ogni volta che si accede a Kaspersky Security Center Cloud Console con l'indirizzo e-mail e la password si inserisce un codice di sicurezza monouso aggiuntivo. È possibile ricevere un codice di sicurezza monouso tramite SMS o generando questo codice nell'applicazione di autenticazione (a seconda del metodo di verifica in due passaggi impostato).

Si sconsiglia vivamente di installare l'applicazione di autenticazione nello stesso dispositivo da cui viene stabilita la connessione con Kaspersky Security Center Cloud Console. È possibile installare un'applicazione di autenticazione nel dispositivo mobile.

Divieto di salvare la password amministratore

Se si utilizza Kaspersky Security Center Cloud Console, **si sconsiglia vivamente** di salvare la password amministratore nel browser installato nel dispositivo dell'utente.

Se il browser è compromesso, un intruso può ottenere l'accesso alle password salvate. Inoltre, se un dispositivo utente con password salvate viene smarrito o sottratto, un intruso può ottenere l'accesso ai dati protetti.

Limitazione dell'appartenenza al ruolo di amministratore principale

Si consiglia di limitare l'appartenenza al ruolo di amministratore principale.

Per impostazione predefinita, dopo che un utente ha creato un'area di lavoro, a questo utente viene assegnato il ruolo di amministratore principale. È utile per la gestione, ma è fondamentale dal punto di vista della sicurezza, poiché il ruolo di amministratore principale ha una vasta gamma di privilegi. L'assegnazione di questo ruolo agli utenti deve essere rigorosamente regolamentata.

È possibile utilizzare i ruoli utente predefiniti con un set di diritti preconfigurato per amministrare Kaspersky Security Center Cloud Console.

Configurazione dei diritti di accesso alle funzionalità dell'applicazione

Si consiglia di utilizzare una configurazione flessibile dei diritti di accesso alle funzionalità di Kaspersky Security Center Cloud Console per ciascun utente o gruppo di utenti.

Il controllo degli accessi in base al ruolo consente la creazione di ruoli utente standard con un set di diritti predefinito e l'assegnazione di tali ruoli agli utenti sulla base dell'ambito delle relative mansioni lavorative.

Principali vantaggi del modello di controllo degli accessi in base al ruolo:

- Amministrazione semplificata
- Gerarchia dei ruoli
- Approccio con privilegio minimo
- Separazione dei compiti

È possibile assegnare ruoli predefiniti a determinati dipendenti in base alle loro posizioni o creare ruoli completamente nuovi.

Durante la configurazione dei ruoli, prestare attenzione ai privilegi associati alla modifica dello stato di protezione del dispositivo Administration Server e all'installazione remota di software di terzi:

- Gestione dei gruppi di amministrazione.
- Operazioni con Administration Server.
- Installazione remota.
- Modifica dei parametri per l'archiviazione di eventi e l'invio delle notifiche.

  Questo privilegio consente di impostare notifiche che eseguono uno script o un modulo eseguibile nel dispositivo Administration Server quando si verifica un evento.

Account separato per l'installazione remota delle applicazioni

Oltre alla differenziazione di base dei diritti di accesso, si consiglia di limitare l'installazione remota delle applicazioni per tutti gli account (ad eccezione dell'amministratore principale o di un altro account specializzato).

Si consiglia di utilizzare un account separato per l'installazione remota delle applicazioni. È possibile assegnare un ruolo o autorizzazioni all'account separato.

Gestione della protezione dei dispositivi client

Regole automatiche per lo spostamento dei dispositivi tra i gruppi di amministrazione

Si consiglia di limitare l'uso delle regole automatiche per lo spostamento dei dispositivi tra i gruppi di amministrazione.

Se si utilizzano regole automatiche per lo spostamento dei dispositivi, ciò potrebbe comportare la propagazione di criteri che forniscono più privilegi al dispositivo spostato rispetto a quelli di cui disponeva prima del riposizionamento.

Inoltre, lo spostamento di un dispositivo client in un altro gruppo di amministrazione può comportare la propagazione delle impostazioni dei criteri. Queste impostazioni dei criteri potrebbero non essere appropriate per la distribuzione a dispositivi guest e non attendibili.

Questo suggerimento non si applica all'allocazione iniziale una tantum dei dispositivi ai gruppi di amministrazione.

Requisiti di sicurezza per i punti di distribuzione e i gateway di connessione

I dispositivi con Network Agent installato possono fungere da punto di distribuzione ed eseguire le seguenti funzioni:

- Distribuire gli aggiornamenti e i pacchetti di installazione ricevuti da Administration Server ai dispositivi client all'interno del gruppo.
- Eseguire l'installazione remota di software di terzi e applicazioni Kaspersky nei dispositivi client.
- Eseguire il polling della rete per rilevare nuovi dispositivi e aggiornare le informazioni sui dispositivi esistenti.
- Fungere da server proxy KSN per i dispositivi client.

Tenendo conto delle capacità disponibili, si consiglia di proteggere i dispositivi che fungono da punti di distribuzione da qualsiasi tipo di accesso non autorizzato (anche fisico).

Configurazione della protezione per le applicazioni gestite

Configurazione della protezione di rete

Assicurarsi di aver completato lo scenario di configurazione iniziale di Kaspersky Security Center Cloud Console. Questo scenario include anche l'esecuzione dei passaggi dell'avvio rapido guidato.

Quando l'avvio rapido guidato è in esecuzione, vengono creati criteri e attività con parametri predefiniti. Questi parametri potrebbero non essere ottimali o addirittura essere vietati nell'organizzazione. Pertanto, si consiglia di configurare i criteri e le attività creati e creare ulteriori criteri e attività, se necessario, per la rete dell'organizzazione.

Indicazione della password per disabilitare la protezione e disinstallare l'applicazione

Per impedire agli intrusi di disabilitare le applicazioni di sicurezza Kaspersky, si consiglia vivamente di abilitare la protezione tramite password per disabilitare la protezione e disinstallare le applicazioni di sicurezza Kaspersky. È possibile impostare la password, ad esempio, per Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Server, Network Agent e altre applicazioni Kaspersky. Dopo aver abilitato la protezione tramite password, si consiglia di bloccare queste impostazioni chiudendo il "lucchetto".

Specificazione della password per la connessione manuale di un dispositivo client ad Administration Server (utilità klmover)

L'utilità klmover consente di connettere manualmente un dispositivo client ad Administration Server. Quando si installa Network Agent su un dispositivo client, l'utilità viene automaticamente copiata nella cartella di installazione di Network Agent.

Per impedire agli intrusi di spostare i dispositivi fuori dal controllo di Administration Server, si consiglia di abilitare la protezione tramite password per l'esecuzione dell'utilità klmover. Per abilitare la protezione con password, selezionare l'opzione **Usa password di disinstallazione** nelle impostazioni dei criteri di Network Agent.

L'abilitazione di **Usa password di disinstallazione** abilita anche la protezione con password per lo Strumento di rimozione per Kaspersky Security Center Web Console (cleaner.exe).

Utilizzo di Kaspersky Security Network

In tutti i criteri delle applicazioni gestite e nelle proprietà di Kaspersky Security Center Cloud Console, si consiglia di abilitare l'uso di Kaspersky Security Network (KSN) e di accettare l'Informativa KSN. Quando si aggiorna o si effettua l'upgrade di Kaspersky Security Center Cloud Console, è possibile accettare l'Informativa KSN aggiornata.

Individuazione di nuovi dispositivi

Si consiglia di configurare correttamente le impostazioni di rilevamento dei dispositivi: impostare l'integrazione con Active Directory e specificare gli intervalli di indirizzi IP per il rilevamento di nuovi dispositivi.

Per motivi di sicurezza, è possibile utilizzare il gruppo di amministrazione predefinito che include tutti i nuovi dispositivi e i criteri predefiniti che interessano questo gruppo.

Trasferimento di eventi a sistemi di terzi

Monitoraggio e generazione di rapporti

Per una risposta tempestiva ai problemi di sicurezza, si consiglia di configurare le funzionalità di monitoraggio e generazione dei rapporti.

Esportazione di eventi nei sistemi SIEM

Per il rilevamento rapido dei problemi di sicurezza prima che si verifichino danni significativi, si consiglia di utilizzare l'esportazione degli eventi in un sistema SIEM.

Notifiche e-mail degli eventi di controllo

Per una risposta tempestiva alle emergenze, si consiglia di configurare Kaspersky Security Center Cloud Console in modo che invii notifiche sugli eventi di controllo, gli eventi critici, gli eventi di errore e gli avvisi pubblicati.

Poiché questi eventi sono eventi interni al sistema, è prevedibile che se ne verifichino pochi; si tratta di una situazione abbastanza normale per la posta.

Configurazione iniziale di Kaspersky Security Center Cloud Console

Questa sezione illustra lo scenario principale per la distribuzione di Kaspersky Security Center Cloud Console, dalla creazione di un'area di lavoro al monitoraggio dello stato di protezione della rete.

Per informazioni sulla distribuzione di Kaspersky Security Center in esecuzione in locale, consultare la Guida in linea di Kaspersky Security Center.

È consigliabile assegnare almeno un giorno lavorativo per il completamento di questo scenario.

Lo scenario guida l'utente nei seguenti passaggi:

- Avvio dell'utilizzo di un'area di lavoro aziendale come amministratore
- Rilevamento dei dispositivi nella rete (se necessario, l'utente assegnerà i punti di distribuzione e vi installerà manualmente i pacchetti di distribuzione)
- Distribuzione delle applicazioni Kaspersky gestite nei dispositivi client, configurazione di strumenti per la protezione della rete, il monitoraggio e gli aggiornamenti periodici di database, moduli software e applicazioni Kaspersky

Dopo aver completato questo scenario, verrà configurata la protezione della rete basata sulle applicazioni Kaspersky. Sarà possibile procedere al monitoraggio dello stato di protezione della rete.

Prerequisiti

Prima di iniziare:

- Visualizzare l'architettura di Kaspersky Security Center Cloud Console per comprendere l'interazione tra i principali componenti dell'applicazione.
- Leggere le informazioni sul licensing di Kaspersky Security Center Cloud Console e sulle applicazioni gestite.
- Assicurarsi di disporre di un codice di attivazione valido per Kaspersky Security Center Cloud Console (se si sta creando un'area di lavoro commerciale).

Passaggi

La configurazione di Kaspersky Security Center Cloud Console comprende le seguenti fasi:

1. **Configurazione delle porte**

   Assicurarsi che tutte le porte necessarie siano aperte per l'interazione tra la rete e l'infrastruttura Kaspersky. Inoltre, se si prevede di utilizzare la gerarchia di Administration Server, assicurarsi che tutte le porte necessarie siano aperte per l'interazione tra l'Administration Server secondario (o gli Administration Server secondari) e i dispositivi client.

2. **Creazione dell'area di lavoro per l'azienda**

   Creare un account, quindi creare un'area di lavoro per l'azienda.

3. **Esecuzione dell'avvio rapido guidato**

   Aprire e accedere a Kaspersky Security Center Cloud Console. Al primo accesso viene automaticamente richiesto di eseguire l'avvio rapido guidato. È anche possibile avviare manualmente l'avvio rapido guidato in qualsiasi momento.

Al termine dell'avvio rapido guidato, saranno disponibili i pacchetti di installazione di Network Agent e delle applicazioni di protezione. Questi pacchetti di installazione sono necessari per la successiva distribuzione di Kaspersky Security Center Cloud Console.

4. **Distribuzione delle applicazioni Kaspersky**

   Eseguire lo scenario di distribuzione iniziale delle applicazioni Kaspersky. Uno dei passaggi dello scenario fa riferimento all'operazione di polling della rete. Questa operazione è necessaria per rilevare i dispositivi client della rete. Il polling della rete e le relative impostazioni sono descritti nello scenario di rilevamento dei dispositivi della rete.

   Se si intende distribuire Kaspersky Security for Windows Server, assicurarsi che i database per questa applicazione siano aggiornati.

5. **Gestione delle licenze delle applicazioni di protezione Kaspersky**

   Quando le applicazioni di protezione Kaspersky vengono distribuite nei dispositivi gestiti, le applicazioni devono essere concesse in licenza applicando un codice di attivazione a ciascuna delle applicazioni. Distribuire i codici di attivazione nelle applicazioni Kaspersky installate nei dispositivi gestiti. Sono disponibili diverse opzioni per concedere in licenza le applicazioni di protezione Kaspersky.

6. **Configurazione della protezione di rete**

   Eseguire la configurazione della protezione di rete per ottimizzare i criteri e le attività creati tramite l'avvio rapido guidato.

7. **Aggiornamento periodico dei database, dei moduli software e delle applicazioni Kaspersky**

   Per proteggere la rete da virus e altre minacce, è necessario configurare aggiornamenti regolari di database, moduli software e applicazioni Kaspersky.

8. **Aggiornamento del software di terze parti e correzione delle vulnerabilità del software di terze parti (facoltativo)**

   Kaspersky Security Center Cloud Console consente di gestire gli aggiornamenti delle applicazioni Microsoft installate nei dispositivi client. È inoltre possibile correggere le vulnerabilità nelle applicazioni Microsoft tramite l'installazione degli aggiornamenti richiesti.

9. **Configurazione di strumenti per il monitoraggio dello stato di protezione della rete**

   Selezionare e configurare widget, rapporti e altri strumenti che consentono di monitorare lo stato di protezione della rete.

Quando Kaspersky Security Center Cloud Console viene distribuito e configurato, è possibile procedere al monitoraggio dello stato di protezione della rete.

Gestione delle aree di lavoro

Questa sezione descrive come utilizzare account e aree di lavoro in Kaspersky Security Center Cloud Console.

Informazioni sulla gestione dell'area di lavoro in Kaspersky Security Center Cloud Console

Utilizzando Kaspersky Security Center Cloud Console, è possibile eseguire le seguenti operazioni:

- Creare un account.
- Modificare un account.
- Registrare un'azienda e creare un'area di lavoro.
- Modificare le informazioni sull'azienda e sulle aree di lavoro.
- Eliminare un'area di lavoro e un'azienda.
- Eliminare un account.

Introduzione a Kaspersky Security Center Cloud Console

Questa sezione descrive come registrarsi e iniziare a utilizzare Kaspersky Security Center Cloud Console.

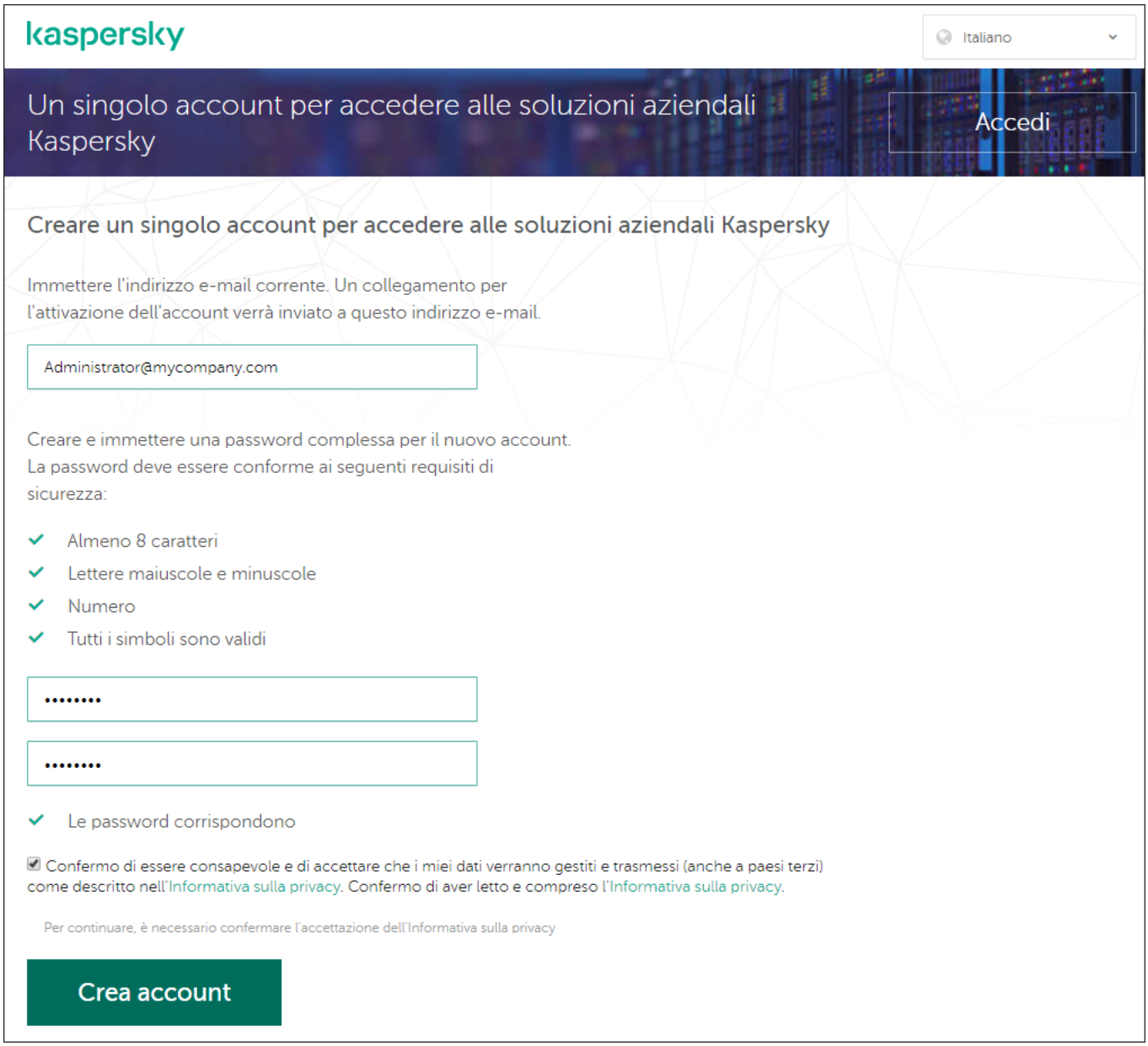
La registrazione a Kaspersky Security Center Cloud Console prevede i seguenti passaggi:

1. Creazione e conferma di un account.
2. Registrazione di un'azienda e creazione di un'area di lavoro.

Creazione di un account

Per creare un account in Kaspersky Security Center Cloud Console:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.
2. Fare clic sul pulsante **Crea un account** nella pagina di avvio di Kaspersky Security Center Cloud Console.
3. Nella pagina **Creare un singolo account per accedere alle soluzioni aziendali Kaspersky** immettere l'indirizzo e-mail, la password e la conferma della password per l'account (vedere la figura di seguito).



Creazione di un account in Kaspersky Security Center Cloud Console

4. Fare clic sul collegamento dell'**Informativa sulla privacy** e leggere attentamente il testo dell'Informativa sulla privacy.

5. Se si accetta che i dati verranno gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy e si conferma di aver letto e compreso l'Informativa sulla privacy, selezionare la casella di controllo accanto al testo del consenso all'elaborazione dei dati in conformità all'Informativa sulla privacy, quindi fare clic sul pulsante **Crea account**.

   Se non si accetta l'Informativa sulla privacy, non utilizzare Kaspersky Security Center Cloud Console.

   Il pulsante diventa disponibile solo dopo aver selezionato la casella di controllo.

   Verrà visualizzata una pagina con la richiesta di controllare l'e-mail. Un messaggio proveniente da Kaspersky viene inviato all'indirizzo e-mail specificato. Il messaggio contiene un collegamento per completare la procedura di creazione dell'account.

6. Chiudere la pagina e aprire il messaggio e-mail nella casella di posta.

7. Fare clic sul collegamento contenuto nel messaggio inviato da Kaspersky per passare alla pagina dell'account.

8. Nella pagina **Attivazione account utente** fare clic sul pulsante **Continua** per completare l'attivazione dell'account.

La creazione dell'account in Kaspersky Security Center Cloud Console è stata completata.

Registrazione di un'azienda e creazione di un'area di lavoro

Subito dopo la creazione dell'account, è possibile registrare un'azienda e creare un'area di lavoro.

> Se si desidera proteggere più di 10.000 dispositivi, non si deve registrare un'azienda e creare un'area di lavoro in Kaspersky Security Center Cloud Console come descritto di seguito. È invece necessario inviare una richiesta al Servizio di assistenza tecnica Kaspersky. Nella richiesta specificare le informazioni sull'azienda e sull'area di lavoro che si desidera creare.

Al momento è possibile registrare una sola azienda e creare una sola area di lavoro. Nelle versioni future di Kaspersky Security Center Cloud Console, sarà possibile creare aree di lavoro aggiuntive per l'azienda. Questo consentirà di mappare la struttura dell'azienda in aree di lavoro, creando un'area di lavoro distinta per ogni sezione dell'azienda.

Prima di iniziare, accertarsi di conoscere le seguenti informazioni:

- Il nome dell'azienda in cui si intende utilizzare la soluzione software.
- Il paese in cui è situata l'azienda. Se l'azienda si trova negli Stati Uniti o in Canada, è necessario conoscere anche lo stato o la provincia.
- Numero totale di dispositivi mobili e computer aziendali che si desidera proteggere.

Per registrare un'azienda e creare un'area di lavoro in Kaspersky Security Center Cloud Console:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.

2. Fare clic sul pulsante **Accedi** nella pagina di avvio di Kaspersky Security Center Cloud Console.

3. Immettere l'indirizzo e-mail e la password specificati durante la creazione dell'account, quindi fare clic sul pulsante **Accedi**.

   Verrà avviata la procedura guidata per la creazione di un'area di lavoro. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Nella pagina **Passaggio 01: Condizioni per l'utilizzo di Kaspersky Security Center Cloud Console** della procedura guidata procedere nel modo seguente:

   a. Leggere attentamente il Contratto, l'Informativa sulla privacy e l'Accordo elaborazione dati per la soluzione software.

   b. Se si accettano i termini e le condizioni del Contratto e dell'Accordo di elaborazione dei dati, si accetta che i dati verranno gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy e si conferma di avere letto e compreso l'Informativa sulla privacy, selezionare le caselle di controllo accanto ai tre documenti elencati e fare clic sul pulsante **Accetta**.

Se non si accettano i termini e le condizioni, non utilizzare Kaspersky Security Center Cloud Console.

Se si fa clic sul pulsante **Rifiuta**, il processo di creazione dell'area di lavoro verrà terminato.

5. Nella pagina **Passaggio 02: Informazioni sull'azienda** della procedura guidata specificare i dettagli principali dell'azienda.

   Compilare i seguenti campi:

   - **Nome dell'azienda** (obbligatorio)

     Specificare il nome dell'azienda in cui si desidera utilizzare la soluzione software. È possibile immettere una stringa con un massimo di 255 caratteri. La stringa può contenere caratteri maiuscoli e minuscoli, numeri, spazi, punti, virgole, trattini e trattini bassi. Il nome dell'azienda specificato verrà visualizzato in Kaspersky Security Center Cloud Console.

   - Campo **Descrizione aggiuntiva dell'azienda** (facoltativo)

     È possibile specificare ulteriori informazioni sull'azienda registrata. È possibile immettere una stringa con un massimo di 255 caratteri. La stringa può contenere caratteri maiuscoli e minuscoli, numeri, spazi, punti, virgole, trattini e trattini bassi.

6. Nella pagina **Passaggio 03: Informazioni sull'area di lavoro** della procedura guidata specificare le informazioni sull'area di lavoro che si desidera creare per la propria azienda.

   Compilare i seguenti campi obbligatori:

   - **Nome dell'area di lavoro**. Specificare il nome dell'area di lavoro in cui si desidera utilizzare la soluzione software. È possibile immettere una stringa con un massimo di 255 caratteri. La stringa può contenere caratteri maiuscoli e minuscoli, numeri, spazi, punti, virgole, trattini e trattini bassi. Il nome dell'area di lavoro specificato verrà visualizzato in Kaspersky Security Center Cloud Console.

   - **Paese**. Nell'elenco a discesa selezionare il paese in cui si trova l'area di lavoro. Se si selezionano gli Stati Uniti o il Canada, specificare anche lo stato o la provincia nell'elenco a discesa **Provincia** visualizzato sotto questo campo.

   - **Numero di dispositivi**. Immettere il numero totale dei dispositivi mobili e dei computer che si desidera proteggere nell'area di lavoro.

     Nel campo di immissione è possibile immettere un numero da 300 a 10.000.

7. Nella pagina **Passaggio 04: Licenza per una nuova area di lavoro** della procedura guidata eseguire una delle seguenti operazioni:

   - Se si desidera provare Kaspersky Security Center Cloud Console, fare clic sul collegamento **Desidero richiedere un'area di lavoro di prova**.

     È consigliabile collegare i propri dispositivi all'area di lavoro di prova e testare eventuali modifiche alle impostazioni, registrando i risultati.

     Non sarà possibile eseguire il passaggio di un'area di lavoro di prova alla modalità commerciale inserendo un codice di attivazione. Per passare alla modalità commerciale è necessario eliminare l'area di lavoro e crearla di nuovo.

   - Se si desidera utilizzare Kaspersky Security Center Cloud Console in modalità commerciale, immettere il codice di attivazione e fare clic sul pulsante **Verifica**.

La registrazione di un'azienda e la creazione di un'area di lavoro in Kaspersky Security Center Cloud Console sono state completate.

Dopo aver preparato l'area di lavoro, si riceve un messaggio e-mail con il collegamento per accedere all'area di lavoro.

Apertura dell'area di lavoro Kaspersky Security Center Cloud Console

Subito dopo aver creato un'area di lavoro per Kaspersky Security Center Cloud Console, l'area di lavoro si apre automaticamente. Successivamente è possibile aprire l'area di lavoro come descritto in questa sezione.

L'amministratore di un Administration Server virtuale ha accesso solo all'Administration Server virtuale. Dopo aver eseguito l'accesso e aver aperto l'area di lavoro, Kaspersky Security Center Cloud Console offre l'interfaccia dell'Administration Server virtuale. Non è possibile passare all'Administration Server primario o ad altri Administration Server secondari.

Un amministratore di un Administration Server virtuale deve avere accesso a un unico Administration Server virtuale. Se non si dispone dei diritti di accesso nel server primario e di diritti di accesso in più server virtuali, non è possibile accedere a Kaspersky Security Center Cloud Console.

Per aprire l'area di lavoro Kaspersky Security Center Cloud Console:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.
2. Accedere all'account in Kaspersky Security Center Cloud Console specificando il nome utente e la password.
3. Se si configura la verifica in due passaggi, immettere il codice di sicurezza monouso inviato tramite SMS o generato nell'app di autenticazione (a seconda del metodo di verifica in due passaggi configurato).

   La pagina del portale visualizza l'azienda di cui l'utente è un amministratore e l'elenco delle relative aree di lavoro.
4. Fare clic sul nome dell'area di lavoro desiderata o sul collegamento **Accedere all'area di lavoro** per passare all'area di lavoro.

   Occasionalmente l'area di lavoro può non essere disponibile per interventi di manutenzione. In tal caso, l'utente non sarà in grado di procedere all'area di lavoro Kaspersky Security Center Cloud Console.

   Non è possibile aprire un'area di lavoro contrassegnata per l'eliminazione.
5. Se uno dei documenti legali di Kaspersky Security Center Cloud Console è stato modificato dopo l'accettazione dei termini e delle condizioni, nella pagina del portale vengono visualizzati i documenti modificati.

   Procedere come segue:

   a. Leggere attentamente i documenti visualizzati.

   b. Se si accettano i termini e le condizioni dei documenti visualizzati, selezionare le caselle di controllo accanto ai documenti elencati, quindi fare clic sul pulsante **Accetto le condizioni**.

      Se non si accettano i termini e le condizioni, non utilizzare più la soluzione software Kaspersky selezionata.

Se si fa clic sul pulsante **Rifiuto**, l'operazione verrà terminata.

Si aprirà l'area di lavoro Kaspersky Security Center Cloud Console.

Disconnessione da Kaspersky Security Center Cloud Console

Al termine del lavoro, chiudere in modo sicuro la sessione corrente eseguendo la disconnessione da Kaspersky Security Center Cloud Console.

Per eseguire la disconnessione da Kaspersky Security Center Cloud Console:

Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Esci**.

Kaspersky Security Center Cloud Console verrà chiuso e sarà visualizzata la pagina dell'account. È possibile chiudere questa pagina del browser, se necessario. Tutti i dati dell'area di lavoro verranno salvati.

Gestione dell'azienda e dell'elenco delle aree di lavoro

Questa sezione descrive come visualizzare le informazioni sull'azienda e l'elenco delle aree di lavoro registrate con il proprio account in Kaspersky Security Center Cloud Console, modificare le informazioni sull'azienda e sulle aree di lavoro ed eliminare un'area di lavoro e un'azienda.

Al momento è possibile registrare una sola azienda e creare una sola area di lavoro. Nelle versioni future di Kaspersky Security Center Cloud Console, sarà possibile creare aree di lavoro aggiuntive per l'azienda. Questo consentirà di mappare la struttura dell'azienda in aree di lavoro, creando un'area di lavoro distinta per ogni sezione dell'azienda.

Modifica delle informazioni su un'azienda e un'area di lavoro

È possibile modificare le informazioni su un'azienda e un'area di lavoro specificate in fase di aggiunta dell'azienda a Kaspersky Security Center Cloud Console.

Per modificare le informazioni su un'azienda e/o un'area di lavoro:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.
2. Accedere all'account in Kaspersky Security Center Cloud Console specificando il nome utente e la password.
3. Se si configura la verifica in due passaggi, immettere il codice di sicurezza monouso inviato tramite SMS o generato nell'app di autenticazione (a seconda del metodo di verifica in due passaggi configurato).

   La pagina del portale visualizza l'azienda di cui l'utente è un amministratore e un elenco delle relative aree di lavoro.
4. Se si desidera modificare il nome e la descrizione dell'azienda, procedere come segue:

   a. Fare clic sull'icona **Modifica** (✎) nell'area con le informazioni sull'azienda.

b. Modificare il nome e/o la descrizione dell'azienda come desiderato.

c. Fare clic sul pulsante **Salva**.

Per annullare le modifiche, fare clic sul pulsante **Annulla**.

5. Se si desidera modificare il nome dell'area di lavoro, attenersi alla seguente procedura:

a. Fare clic sull'icona **Modifica** (✎) nell'area con le informazioni sull'area di lavoro.

b. Modificare il nome dell'area di lavoro come desiderato.

c. Fare clic sul pulsante **Salva**.

Per annullare le modifiche, fare clic sul pulsante **Annulla**.

Le informazioni modificate vengono visualizzate in Kaspersky Security Center Cloud Console.

Eliminazione di un'area di lavoro e di un'azienda

L'area di lavoro di un'azienda può essere eliminata manualmente o automaticamente. Dopo l'eliminazione dell'ultima area di lavoro, anche le informazioni relative all'azienda vengono eliminate automaticamente.

Eliminazione manuale

È possibile eliminare l'area di lavoro di un'azienda se quest'ultima ha deciso di non utilizzare più l'area di lavoro.

> Dopo l'eliminazione dell'area di lavoro, tutte le applicazioni di protezione rimarranno nei dispositivi gestiti. Prima di eliminare l'area di lavoro è quindi consigliabile disabilitare la protezione tramite password di tutte le applicazioni di protezione o disinstallare le applicazioni di protezione dai dispositivi gestiti.

Per eliminare un'area di lavoro e un'azienda:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.

2. Accedere all'account in Kaspersky Security Center Cloud Console specificando il nome utente e la password.

3. Se si configura la verifica in due passaggi, immettere il codice di sicurezza monouso inviato tramite SMS o generato nell'app di autenticazione (a seconda del metodo di verifica in due passaggi configurato).

La pagina del portale visualizza l'azienda di cui l'utente è un amministratore e un elenco delle relative aree di lavoro.

4. Selezionare l'area di lavoro che si desidera eliminare.

5. A destra, nella sezione contenente l'area di lavoro selezionata, fare clic sull'icona **Elimina** (🗑).

Viene aperta la finestra **Elimina area di lavoro**.

6. Nella finestra **Elimina area di lavoro** confermare che si desidera eliminare l'area di lavoro.

L'area di lavoro viene contrassegnata per l'eliminazione. La sezione delle informazioni per l'area di lavoro viene evidenziata con un bordo rosso.

La sezione delle informazioni per l'area di lavoro viene duplicata nella parte inferiore della pagina, nella sezione **Contrassegnate per l'eliminazione**.

Non è possibile accedere a un'area di lavoro contrassegnata per l'eliminazione e gestirla.

Se non è possibile contrassegnare un'area di lavoro per l'eliminazione, contattare il Servizio di assistenza tecnica di Kaspersky. In seguito alla ricezione della richiesta da parte di un esperto dell'Assistenza tecnica di Kaspersky, l'area di lavoro e l'azienda vengono eliminate.

Le aree di lavoro contrassegnate per l'eliminazione possono mantenere questo stato per un periodo di sette giorni da quando sono state contrassegnate. Dopo sette giorni vengono automaticamente eliminate.

Durante questo periodo è possibile eliminare forzatamente un'area di lavoro contrassegnata per l'eliminazione o annullare l'eliminazione di un'area di lavoro.

Per eliminare forzatamente un'area di lavoro:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.
2. Accedere all'account in Kaspersky Security Center Cloud Console specificando il nome utente e la password.
3. Se si configura la verifica in due passaggi, immettere il codice di sicurezza monouso inviato tramite SMS o generato nell'app di autenticazione (a seconda del metodo di verifica in due passaggi configurato).

   La pagina del portale visualizza l'azienda di cui l'utente è un amministratore e un elenco delle relative aree di lavoro.
4. Nella sezione **Contrassegnati per l'eliminazione** della parte dedicata alle informazioni sull'area di lavoro contrassegnata per l'eliminazione fare clic sull'opzione **Forza eliminazione**.

   Viene aperta la finestra **Elimina area di lavoro**.
5. Nella finestra **Elimina area di lavoro** immettere l'ID dell'area di lavoro che si desidera eliminare.

   Sarà necessario confermare l'ID dell'area di lavoro per assicurarsi di non eliminare accidentalmente l'area di lavoro. Dopo l'eliminazione di un'area di lavoro, quest'ultima non potrà essere ripristinata.

   L'ID area di lavoro viene visualizzato nella sezione delle informazioni sull'area di lavoro sotto il relativo nome.
6. Nella finestra **Elimina area di lavoro** fare clic su **OK**.

L'area di lavoro viene eliminata. Tutti i dati relativi agli utenti, ai dispositivi gestiti e alle relative impostazioni vengono eliminati.

Eliminazione automatica

Kaspersky Security Center Cloud Console elimina automaticamente un'area di lavoro:

- 30 giorni dopo la scadenza della licenza di prova.
- 90 giorni dopo la scadenza di tutte le licenze commerciali o in abbonamento nell'archivio dell'Administration Server.
- 90 giorni dopo l'eliminazione dell'ultima chiave di licenza (attiva, di riserva o non in uso) aggiunta manualmente nell'archivio.

Kaspersky Security Center Cloud Console invia una notifica agli amministratori dell'area di lavoro 30 giorni, 7 giorni e 1 giorno prima dell'eliminazione.

Annullamento dell'eliminazione di un'area di lavoro

È possibile annullare l'eliminazione di un'area di lavoro contrassegnata per l'eliminazione.

Non è possibile annullare l'eliminazione di un'area di lavoro che è già stata eliminata.

Per annullare l'eliminazione di un'area di lavoro:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.
2. Accedere all'account in Kaspersky Security Center Cloud Console specificando il nome utente e la password.
3. Se si configura la verifica in due passaggi, immettere il codice di sicurezza monouso inviato tramite SMS o generato nell'app di autenticazione (a seconda del metodo di verifica in due passaggi configurato).

   La pagina del portale visualizza l'azienda di cui l'utente è un amministratore e un elenco delle relative aree di lavoro.
4. Nella sezione **Contrassegnate per l'eliminazione**, nella sezione delle informazioni relativa all'area di lavoro contrassegnata per l'eliminazione fare clic sul collegamento **Annulla eliminazione**.

L'eliminazione dell'area di lavoro viene annullata. A questo punto è possibile accedere all'area di lavoro e continuare a utilizzarla.

Gestione dell'accesso all'azienda e alle relative aree di lavoro

Questa sezione contiene informazioni sulla concessione e sulla revoca dell'accesso all'azienda e alle relative aree di lavoro.

Kaspersky Security Center Cloud Console offre due livelli di accesso:

- **Amministratore**

  Un utente con questo livello di accesso può gestire completamente l'azienda e le relative aree di lavoro.
- **Utente**

  Un utente con questo livello di accesso può visualizzare l'elenco delle aree di lavoro disponibili e accedervi.

Concessione dell'accesso all'azienda e alle relative aree di lavoro

È possibile concedere l'accesso all'azienda e alle relative aree di lavoro se si desidera che un altro utente sia in grado di accedere all'azienda e gestirla in base al livello di accesso selezionato.

Prima di poter concedere l'accesso a un utente, quest'ultimo deve creare un account in Kaspersky Security Center Cloud Console.

Per concedere l'accesso all'azienda e alle relative aree di lavoro:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.
2. Accedere all'account in Kaspersky Security Center Cloud Console specificando il nome utente e la password.
3. Se si configura la verifica in due passaggi, immettere il codice di sicurezza monouso inviato tramite SMS o generato nell'app di autenticazione (a seconda del metodo di verifica in due passaggi configurato).

   La pagina del portale visualizza l'azienda di cui l'utente è un amministratore e un elenco delle relative aree di lavoro.
4. Fare clic sul collegamento **Mostra controllo dell'accesso**.

   L'elenco degli account con accesso all'azienda si espande.
5. Fare clic sul collegamento **Concedi l'accesso**.
6. Nel campo **Indirizzo e-mail** specificare l'indirizzo e-mail dell'account a cui si desidera concedere l'accesso.
7. Nell'elenco **Livello di accesso** selezionare il livello di accesso che si desidera assegnare all'account inserito:

   - **Amministratore**

     Un utente con questo livello di accesso può gestire completamente l'azienda e le relative aree di lavoro.
   - **Utente**

     Un utente con questo livello di accesso può visualizzare l'elenco delle aree di lavoro disponibili e accedervi.

   Non è possibile concedere più livelli di accesso allo stesso account all'interno della stessa azienda.
8. Fare clic sul pulsante **Concedi**.

All'account specificato viene concesso l'accesso all'azienda e alle relative aree di lavoro. L'utente può accedere all'azienda e gestirla in base al livello di accesso selezionato.

Se è stato concesso il livello di accesso **Utente** all'account, è necessario assegnare un ruolo all'utente aggiunto. In caso contrario, l'utente non sarà in grado di accedere all'area di lavoro.

Revoca dell'accesso all'azienda e alle relative aree di lavoro

È possibile revocare l'accesso all'azienda e alle relative aree di lavoro se non si desidera più che un utente sia in grado di accedere all'azienda e gestirla (ad esempio dopo che l'utente lascia l'azienda).

Non è possibile revocare il proprio accesso all'azienda.

Per revocare l'accesso all'azienda e alle relative aree di lavoro:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.

2. Accedere all'account in Kaspersky Security Center Cloud Console specificando il nome utente e la password.
3. Se si configura la verifica in due passaggi, immettere il codice di sicurezza monouso inviato tramite SMS o generato nell'app di autenticazione (a seconda del metodo di verifica in due passaggi configurato).

   La pagina del portale visualizza l'azienda di cui l'utente è un amministratore e un elenco delle relative aree di lavoro.
4. Fare clic sul collegamento **Mostra controllo dell'accesso**.

   L'elenco degli account con accesso all'azienda si espande.
5. Fare clic sull'icona **Revoca** (🗑) accanto all'account di cui si desidera revocare l'accesso.
6. Nella finestra **Revocare l'accesso all'azienda** visualizzata fare clic su **OK** per confermare l'operazione.

L'accesso dell'account selezionato all'azienda e alle relative aree di lavoro viene revocato. L'utente non può più accedere all'azienda e gestirla.

Reimpostazione della password

Se si dimentica la password dell'account Kaspersky Security Center Cloud Console, è possibile ripristinare l'accesso all'account reimpostando la password.

Per reimpostare la password dell'account:

1. Nel browser accedere a Kaspersky Security Center Cloud Console.
2. Fare clic sul pulsante **Accedi**, quindi sul collegamento **Password dimenticata?**.
3. Immettere l'indirizzo e-mail specificato durante la creazione dell'account.
4. Fare clic su **Reimposta password**.

   All'indirizzo specificato verrà inviato un messaggio e-mail contenente un collegamento per la reimpostazione della password.
5. Fare clic sul collegamento nel messaggio e-mail.
6. Nella finestra visualizzata digitare una nuova password e confermarla.
7. Se è stata configurata una domanda segreta, rispondere alla domanda.

   Se si configura la verifica in due passaggi, immettere il codice di sicurezza monouso inviato tramite SMS o generato nell'app di autenticazione (a seconda del metodo di verifica in due passaggi configurato).
8. Fare clic su **Continua**.

   La nuova password per l'accesso a Kaspersky Security Center Cloud Console viene salvata.

Se non si riceve un messaggio e-mail, controllare l'indirizzo e-mail immesso e la cartella della posta indesiderata, quindi riprovare. Se non si riceve un messaggio quando si riprova, è probabile che l'indirizzo e-mail specificato non sia registrato nel sito Web. Contattare il Servizio di assistenza tecnica di Kaspersky.

Modifica delle impostazioni di un account in Kaspersky Security Center Cloud Console

Questa sezione contiene istruzioni su come modificare ed eliminare un account in Kaspersky Security Center Cloud Console.

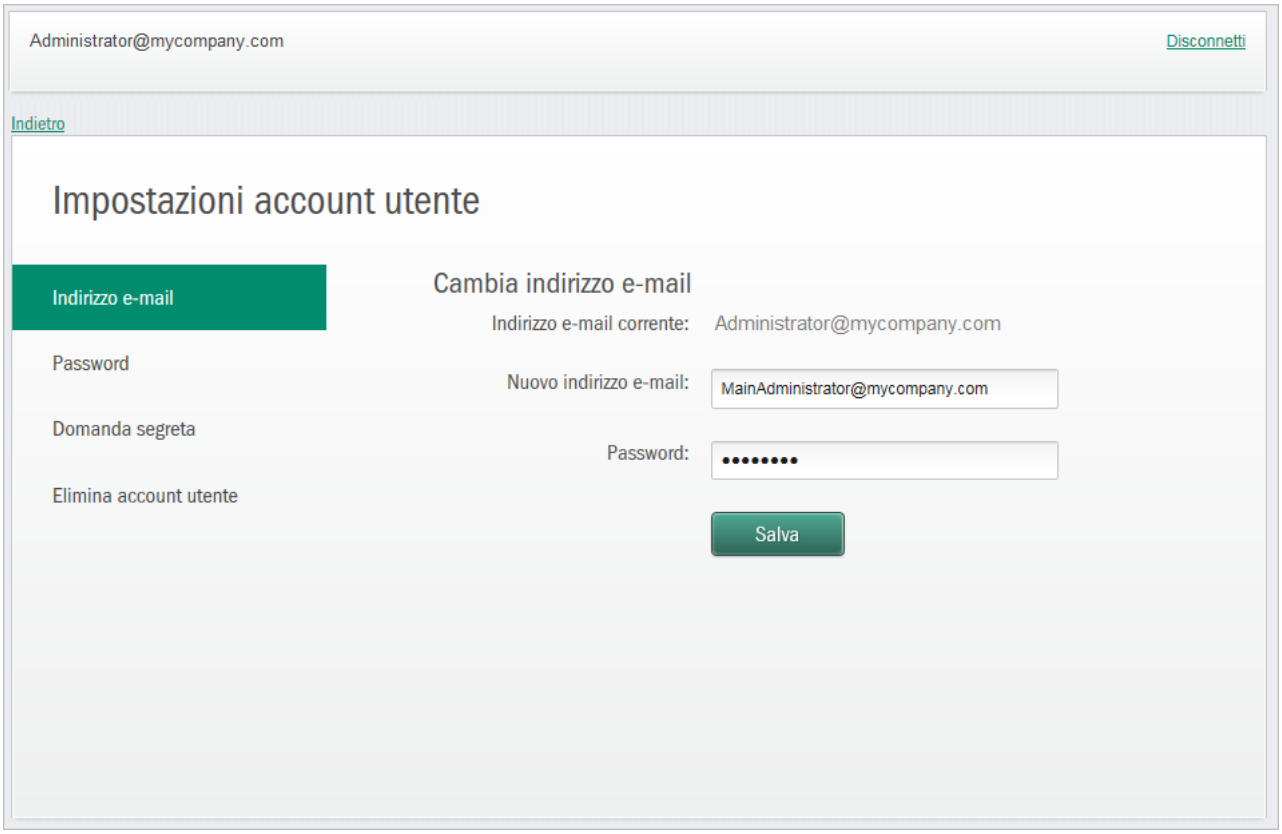
Modifica di un indirizzo e-mail

Per modificare l'indirizzo e-mail nelle impostazioni dell'account in Kaspersky Security Center Cloud Console:

1. In Kaspersky Security Center Cloud Console fare clic sul collegamento con il nome del proprio account e selezionare **Gestisci account utente**.

   Si aprirà la finestra **Impostazioni account utente**.

2. Selezionare la sezione **Indirizzo e-mail** (vedere la figura di seguito).



Modifica dell'indirizzo e-mail nelle impostazioni di un account in Kaspersky Security Center Cloud Console

   La sezione **Indirizzo e-mail** consente di visualizzare l'indirizzo e-mail corrente, un campo per immettere il nuovo indirizzo, un campo di immissione per immettere la password e il pulsante **Salva**.

3. Nel campo di immissione **Nuovo indirizzo e-mail** immettere il nuovo indirizzo e-mail.

   Immettere l'indirizzo con attenzione. Se l'utente immette un indirizzo non valido, non sarà in grado di procedere all'account e quindi utilizzare Kaspersky Security Center Cloud Console.

4. Nel campo di immissione **Password** immettere la password corrente.

5. Fare clic sul pulsante **Salva**.

6. Tornare a Kaspersky Security Center Cloud Console facendo clic sul collegamento **Indietro** o uscire dal portale facendo clic sul collegamento **Disconnetti**.

L'indirizzo e-mail viene modificato nelle impostazioni dell'account Kaspersky Security Center Cloud Console e nelle impostazioni dell'account My Kaspersky. Viene inviato un messaggio al nuovo indirizzo e-mail come notifica della modifica dell'indirizzo e-mail per ottenere l'accesso all'account. Al successivo accesso a Kaspersky Security Center Cloud Console, sarà necessario specificare il nuovo indirizzo e-mail.

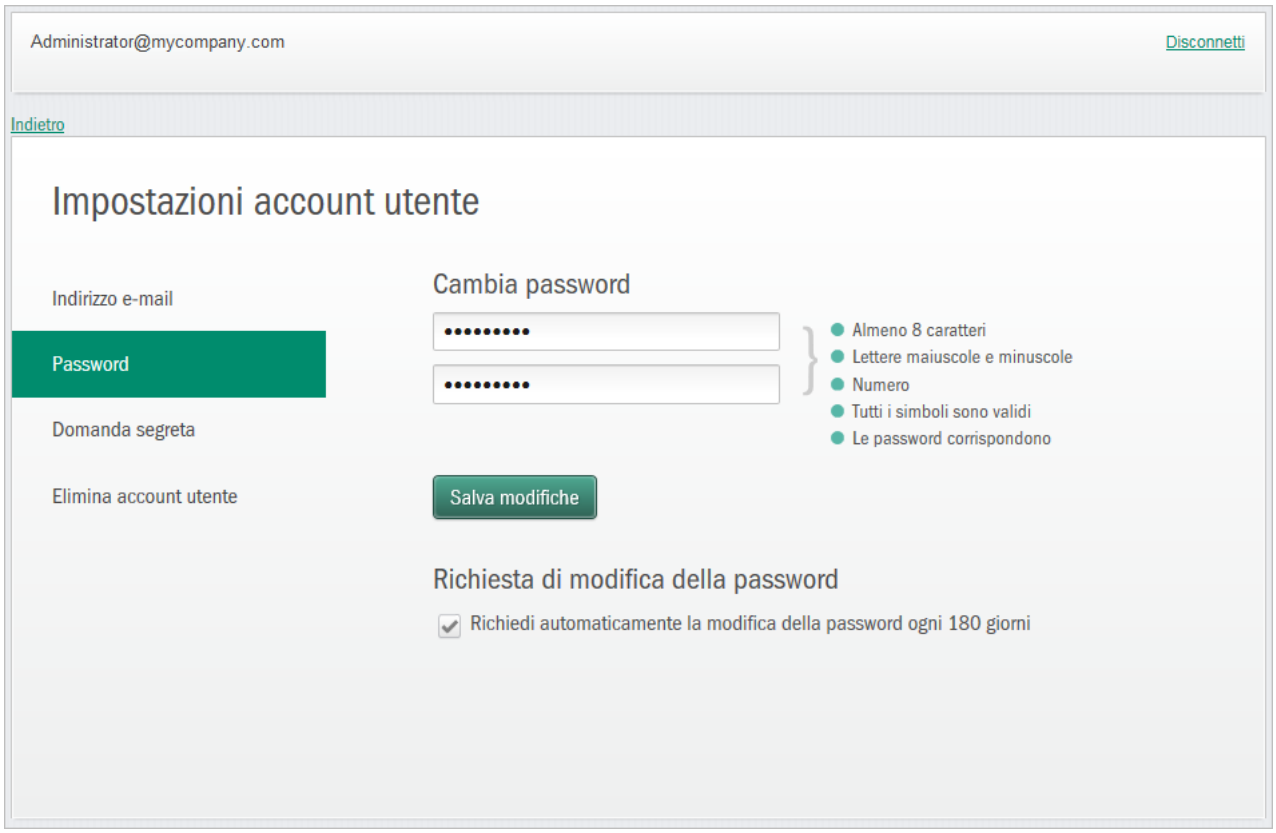
Modifica di una password

Per modificare la password nelle impostazioni dell'account in Kaspersky Security Center Cloud Console:

1. In Kaspersky Security Center Cloud Console fare clic sul collegamento con il nome del proprio account e selezionare **Gestisci account utente**.

   Si aprirà la finestra **Impostazioni account utente**.

2. Selezionare la sezione **Password** (vedere la figura di seguito).



Modifica della password dell'account in Kaspersky Security Center Cloud Console

Questa sezione consente di visualizzare i campi per l'immissione di una nuova password e la relativa conferma, nonché il pulsante **Salva modifiche**.

3. Immettere una nuova password e confermarla nei rispettivi campi di immissione.

   A destra del campo di immissione della password, vengono mostrati i requisiti per la password. Non è possibile salvare la nuova password se non si soddisfano i requisiti.

4. Selezionare o deselezionare la casella di controllo **Richiedi automaticamente la modifica della password ogni 180 giorni**.

   Per impostazione predefinita, questa casella di controllo è selezionata.

5. Fare clic sul pulsante **Salva modifiche**.

6. Tornare a Kaspersky Security Center Cloud Console facendo clic sul collegamento **Indietro** o uscire dal portale facendo clic sul collegamento **Disconnetti**.

La password è stata modificata. Sarà necessario immettere la nuova password quando si accede a Kaspersky Security Center Cloud Console e quando si accede a My Kaspersky.

Utilizzo della verifica in due passaggi

Questa sezione illustra la verifica in due passaggi, che può contribuire a potenziare la sicurezza dell'account in Kaspersky Security Center Cloud Console.

Informazioni sulla verifica in due passaggi

La verifica in due passaggi può contribuire a potenziare la sicurezza dell'account in Kaspersky Security Center Cloud Console. Quando questa funzionalità è abilitata, ogni volta che si accede a Kaspersky Security Center Cloud Console con l'indirizzo e-mail e la password si inserisce un codice di sicurezza monouso aggiuntivo. Con la verifica in due passaggi gli utenti malintenzionati non possono accedere all'account nel caso in cui la password venga rubata o indovinata, a meno che non abbiano accesso anche al cellulare. Inoltre, quando la verifica in due passaggi è abilitata, è necessario immettere un codice di sicurezza monouso aggiuntivo se la password è stata dimenticata.

Dopo la configurazione della verifica in due passaggi, l'utente ha la responsabilità di tenere fisicamente al sicuro il cellulare e di mantenere l'accesso al numero di telefono.

È possibile ottenere un codice di sicurezza monouso in uno dei seguenti modi:

- Un codice di sicurezza viene inviato tramite SMS al numero di cellulare.

  In questo caso, se si perde l'accesso al telefono cellulare, non sarà possibile accedere al proprio account in Kaspersky Security Center Cloud Console finché non si ripristinerà l'accesso al numero di telefono.

- Un codice di sicurezza viene generato in un'app di autenticazione installata nel cellulare.

  È consigliabile configurare la verifica in due passaggi utilizzando un'app di autenticazione. In questo caso è possibile accedere all'account anche se il cellulare non è connesso a Internet o a una rete mobile.

  Sono stati eseguiti test di compatibilità con Kaspersky Security Center Cloud Console solo su Google Authenticator e Microsoft Authenticator e queste applicazioni erano utilizzabili gratuitamente al momento. Le interfacce di queste applicazioni potrebbero essere non disponibili nella lingua desiderata. Verificare inoltre la conformità al GDPR e le informative sulla privacy delle applicazioni prima di utilizzarle. Kaspersky non è in alcun modo sponsorizzata o sostenuta dai proprietari di tali applicazioni o affiliata ad essi.

  > Microsoft Authenticator può essere installato solo nei dispositivi mobili.

  È inoltre consigliabile installare un'app di autenticazione in un dispositivo diverso dal proprio cellulare. In questo modo sarà possibile accedere al proprio account in caso di furto o smarrimento del cellulare.

  In questo caso, se si perde l'accesso al telefono cellulare e non si dispone di un'app di autenticazione in un altro dispositivo, non sarà possibile accedere al proprio account in Kaspersky Security Center Cloud Console finché non si ripristinerà l'accesso al numero di telefono. Successivamente, utilizzare il codice di sicurezza inviato tramite SMS.

Se in precedenza è stata configurata una domanda segreta per ripristinare la password in caso di smarrimento, la funzionalità della domanda di sicurezza verrà definitivamente disabilitata dopo la configurazione della verifica in due passaggi.

Scenario: Configurazione della verifica in due passaggi

La verifica in due passaggi può contribuire a potenziare la sicurezza dell'account in Kaspersky Security Center Cloud Console. Dopo il completamento dello scenario in questa sezione, verrà configurata la verifica in due passaggi dell'account.

Lo scenario procede per fasi:

1. **Aggiunta del numero di telefono**

   In questa fase si configura la verifica in due passaggi tramite SMS.

2. **Installazione e configurazione di un'app di autenticazione**

   Installare e configurare un'app di autenticazione.

   È consigliabile configurare la verifica in due passaggi utilizzando un'app di autenticazione. In questo caso è possibile accedere all'account anche se il cellulare non è connesso a Internet o a una rete mobile.

   È inoltre consigliabile installare un'app di autenticazione in un dispositivo diverso dal proprio cellulare. In questo modo sarà possibile accedere al proprio account in caso di furto o smarrimento del cellulare.

3. **Modifica del numero di telefono**

   Se necessario, è possibile modificare il numero di telefono utilizzato per la verifica in due passaggi.

Configurazione della verifica in due passaggi tramite SMS

Per configurare la verifica in due passaggi tramite SMS:

1. In Kaspersky Security Center Cloud Console fare clic sul collegamento con il nome del proprio account e selezionare **Gestisci account utente**.

   Si aprirà la finestra **Impostazioni account utente**.

2. Selezionare la sezione **Verifica in due passaggi**.

3. Fare clic sul pulsante **Configura**.

4. In **Immettere la password corrente** specificare la password dell'account in Kaspersky Security Center Cloud Console, quindi fare clic sul pulsante **Continua**.

5. In **Specificare il numero di cellulare** specificare il numero di cellulare da utilizzare nella verifica in due passaggi, quindi fare clic sul pulsante **Avanti**.

   È possibile utilizzare lo stesso numero di telefono per un massimo di cinque account.

   Al numero di telefono specificato viene inviato un codice di sicurezza a 6 cifre.

6. In **Confermare il numero di telefono** immettere il codice di sicurezza ricevuto.

La verifica in due passaggi è configurata. Adesso ogni volta che si accede con l'indirizzo e-mail e la password o se si dimentica la password, sarà necessario inserire un codice di sicurezza monouso che si riceve via SMS al numero di telefono specificato.

Adesso è possibile installare e configurare un'app di autenticazione, modificare il numero di telefono o disabilitare la verifica in due passaggi.

Configurazione della verifica in due passaggi utilizzando un'app di autenticazione

Le app di autenticazione non possono essere utilizzate in Kaspersky Security Center Cloud Console come metodo di verifica indipendente. È prima necessario configurare la verifica in due passaggi tramite SMS. Se si disabilita la verifica in due passaggi tramite il numero di cellulare, la verifica tramite un'app di autenticazione viene automaticamente disattivata. Dopo aver configurato sia la verifica tramite SMS che tramite un'app, sarà possibile selezionare un metodo di verifica nella pagina di accesso o se la password viene dimenticata.

Per configurare la verifica in due passaggi da parte di un'app di autenticazione:

1. Configurare la verifica in due passaggi tramite SMS.

2. Scaricare, installare ed eseguire l'app di autenticazione che si desidera utilizzare.

   Sono stati eseguiti test di compatibilità con Kaspersky Security Center Cloud Console solo su Google Authenticator e Microsoft Authenticator e queste applicazioni erano utilizzabili gratuitamente al momento. Le interfacce di queste applicazioni potrebbero essere non disponibili nella lingua desiderata. Verificare inoltre la conformità al GDPR e le informative sulla privacy delle applicazioni prima di utilizzarle. Kaspersky non è in alcun modo sponsorizzata o sostenuta dai proprietari di tali applicazioni o affiliata ad essi.

   > Microsoft Authenticator può essere installato solo nei dispositivi mobili.

   Se lo si desidera, è possibile utilizzare altre app a proprio rischio. L'app utilizzata deve supportare i codici di sicurezza a 6 cifre.

   È inoltre consigliabile installare un'app di autenticazione in un dispositivo diverso dal proprio cellulare. In questo modo sarà possibile accedere al proprio account in caso di furto o smarrimento del cellulare.

3. In Kaspersky Security Center Cloud Console fare clic sul collegamento con il nome del proprio account e selezionare **Gestisci account utente**.

   Si aprirà la finestra **Impostazioni account utente**.

4. Selezionare la sezione **Verifica in due passaggi**.

5. Fare clic sul pulsante **Ottieni la chiave segreta**.

6. In **Immettere la password corrente** specificare la password dell'account in Kaspersky Security Center Cloud Console, quindi fare clic sul pulsante **Continua**.

   La pagina del portale visualizza una chiave segreta di 16 caratteri e un codice QR.

7. Nell'app di autenticazione presente in ogni dispositivo creare un account e immettere la chiave segreta visualizzata. In alternativa, è possibile eseguire la scansione del codice QR con il cellulare. In questo caso, l'account verrà creato automaticamente. Per ulteriori informazioni, consultare la documentazione dell'app.

Nelle app di autenticazione viene generato un codice di sicurezza a 6 cifre.

8. Verificare che i codici di sicurezza generati nelle app corrispondano in ciascun dispositivo.

9. In Kaspersky Security Center Cloud Console immettere il codice di sicurezza generato.

La verifica in due passaggi da parte di un'app di autenticazione è stata configurata. Adesso ogni volta che si accede con l'indirizzo e-mail e la password o se si dimentica la password, sarà necessario inserire un codice di sicurezza monouso generato nell'app di autenticazione.

Adesso è possibile disabilitare l'utilizzo di un'app di autenticazione o disabilitare completamente la verifica in due passaggi.

Modifica del numero di cellulare

Per modificare il numero di telefono utilizzato nella verifica in due passaggi tramite SMS:

1. In Kaspersky Security Center Cloud Console fare clic sul collegamento con il nome del proprio account e selezionare **Gestisci account utente**.

   Si aprirà la finestra **Impostazioni account utente**.

2. Selezionare la sezione **Verifica in due passaggi**.

3. In **Numero di telefono** fare clic sul collegamento **Modificare il numero di telefono**.

4. In **Specificare il numero di cellulare** specificare il nuovo numero di cellulare da utilizzare nella verifica in due passaggi, quindi fare clic sul pulsante **Avanti**.

5. In **Immettere la password corrente** specificare la password dell'account in Kaspersky Security Center Cloud Console, quindi fare clic sul pulsante **Continua**.

   Al numero di telefono specificato viene inviato un codice di sicurezza a 6 cifre.

6. In **Confermare il numero di telefono** immettere il codice di sicurezza ricevuto.

Il numero di cellulare è stato modificato. Adesso un codice di sicurezza monouso verrà inviato al nuovo numero di telefono.

Disabilitazione della verifica in due passaggi

Se non si desidera più utilizzare la verifica in due passaggi, è possibile disabilitarla, come descritto in questa sezione.

La disattivazione della verifica in due passaggi ridurrà la sicurezza dell'account. È consigliabile continuare a utilizzare la verifica in due passaggi.

Se si configura la verifica in due passaggi tramite SMS, è possibile disabilitare la verifica in due passaggi. Se si configura la verifica in due passaggi da parte di un'app di autenticazione, è possibile disabilitare l'utilizzo dell'app o disabilitare completamente la verifica in due passaggi.

Per disabilitare l'utilizzo di un'app di autenticazione:

1. In Kaspersky Security Center Cloud Console fare clic sul collegamento con il nome del proprio account e selezionare **Gestisci account utente**.

   Si aprirà la finestra **Impostazioni account utente**.

2. Selezionare la sezione **Verifica in due passaggi**.

3. In **App di autenticazione** fare clic sul collegamento **Disabilitare l'utilizzo dell'app di autenticazione**.

4. In **Immettere la password corrente** specificare la password dell'account in Kaspersky Security Center Cloud Console, quindi fare clic sul pulsante **Continua**.

L'utilizzo di un'app di autenticazione è disabilitato. Le impostazioni di verifica in due passaggi da parte di un'app di autenticazione vengono eliminate. Adesso è possibile eliminare gli account nelle app di autenticazione.

In un secondo momento è possibile configurare nuovamente la verifica in due passaggi da parte di un'app di autenticazione.

Per disabilitare completamente la verifica in due passaggi:

1. In Kaspersky Security Center Cloud Console fare clic sul collegamento con il nome del proprio account e selezionare **Gestisci account utente**.

   Si aprirà la finestra **Impostazioni account utente**.

2. Selezionare la sezione **Verifica in due passaggi**.

3. In **Numero di telefono** fare clic sul collegamento **Disabilitare la verifica in due passaggi**.

4. In **Immettere la password corrente** specificare la password dell'account in Kaspersky Security Center Cloud Console, quindi fare clic sul pulsante **Continua**.

La verifica in due passaggi è disabilitata. Se si utilizzava la verifica in due passaggi da parte di un'app di autenticazione, le impostazioni della verifica in due passaggi vengono eliminate. Adesso è possibile eliminare gli account nelle app di autenticazione.

In un secondo momento è possibile configurare nuovamente la verifica in due passaggi.

Eliminazione di un account in Kaspersky Security Center Cloud Console

Se si desidera interrompere l'utilizzo di Kaspersky Security Center Cloud Console, è possibile eliminare l'account.

Quando si elimina un account, tutti i dati associati a tale account andranno persi.

In seguito all'eliminazione dell'account non sarà più possibile ottenere l'accesso alle aree di lavoro in Kaspersky Endpoint Security Cloud, Kaspersky Security for Microsoft Office 365 e Kaspersky Security Center Cloud Console. Se l'utente era l'unico amministratore in un'area di lavoro, l'area di lavoro verrà eliminata. Si perderà inoltre l'accesso all'account My Kaspersky.

Per eliminare un account in Kaspersky Security Center Cloud Console:

1. In Kaspersky Security Center Cloud Console fare clic sul collegamento con il nome del proprio account e selezionare **Gestisci account utente**.

   Si aprirà la finestra **Impostazioni account utente**.

2. Selezionare la sezione **Elimina account utente**.

   La sezione **Elimina account utente** consente di visualizzare informazioni sulle conseguenze dell'eliminazione dell'account e, sotto le informazioni, il pulsante **Elimina**.

3. Leggere le informazioni sull'eliminazione dell'account, quindi fare clic sul pulsante **Elimina**.

   Viene aperta la finestra **Immettere la password dell'account utente**.

4. Nel campo di immissione della password immettere la password, quindi fare clic sul pulsante **Continua**.

L'account viene eliminato.

Selezione dei datacenter utilizzati per l'archiviazione delle informazioni di Kaspersky Security Center Cloud Console

Un'area di lavoro per Kaspersky Security Center Cloud Console viene creata utilizzando i server di una rete di datacenter globali basati sulla piattaforma cloud Microsoft Azure. La selezione dei datacenter che devono ospitare un'area di lavoro dipende dal paese specificato durante la registrazione dell'area di lavoro in Kaspersky Security Center Cloud Console (vedere la tabella di seguito). I pacchetti di distribuzione delle applicazioni di protezione sono ospitati negli stessi server delle aree di lavoro.

Corrispondenza dell'ubicazione dell'azienda con un'area geografica Microsoft Azure

Paese in cui è situata l'azienda	Area geografica del datacenter Microsoft
Argentina	Brasile meridionale
Bolivia	Brasile meridionale
Brasile	Brasile meridionale
Cile	Brasile meridionale
Colombia	Brasile meridionale
Ecuador	Brasile meridionale
Guyana	Brasile meridionale
Perù	Brasile meridionale
Paraguay	Brasile meridionale
Suriname	Brasile meridionale
Uruguay	Brasile meridionale
Venezuela	Brasile meridionale
Antigua e Barbuda	Stati Uniti orientali
Anguilla	Stati Uniti orientali
Aruba	Stati Uniti orientali
Barbados	Stati Uniti orientali
Saint Barthelemy	Stati Uniti orientali

Bonaire, Sint Eustatius e Saba	Stati Uniti orientali
Belize	Stati Uniti orientali
Costa Rica	Stati Uniti orientali
Cuba	Stati Uniti orientali
Curacao	Stati Uniti orientali
Dominica	Stati Uniti orientali
Repubblica dominicana	Stati Uniti orientali
Grenada	Stati Uniti orientali
Guadalupa	Stati Uniti orientali
Guatemala	Stati Uniti orientali
Honduras	Stati Uniti orientali
Haiti	Stati Uniti orientali
Giamaica	Stati Uniti orientali
Saint Kitts e Nevis	Stati Uniti orientali
Isole Cayman	Stati Uniti orientali
Saint Lucia	Stati Uniti orientali
Saint Martin	Stati Uniti orientali
Martinica	Stati Uniti orientali
Montserrat	Stati Uniti orientali
Nicaragua	Stati Uniti orientali
Panama	Stati Uniti orientali
Portorico	Stati Uniti orientali
Sint Maarten	Stati Uniti orientali
Trinidad e Tobago	Stati Uniti orientali
Saint Vincent e Grenadine	Stati Uniti orientali
Isole Vergini britanniche	Stati Uniti orientali
Isole Vergini Americane	Stati Uniti orientali
Giappone	Stati Uniti orientali
Canada (Nuovo Brunswick)	Stati Uniti orientali
Canada (Terranova e Labrador)	Stati Uniti orientali
Canada (Nuova Scozia)	Stati Uniti orientali
Canada (Ontario)	Stati Uniti orientali
Canada (Isola del Principe Edoardo)	Stati Uniti orientali
Canada (Quebec)	Stati Uniti orientali
Stati Uniti d'America (Alabama)	Stati Uniti orientali
Stati Uniti d'America (Arkansas)	Stati Uniti orientali

Stati Uniti d'America (Connecticut)	Stati Uniti orientali
Stati Uniti d'America (Distretto di Columbia)	Stati Uniti orientali
Stati Uniti d'America (Delaware)	Stati Uniti orientali
Stati Uniti d'America (Florida)	Stati Uniti orientali
Stati Uniti d'America (Georgia)	Stati Uniti orientali
Stati Uniti d'America (Iowa)	Stati Uniti orientali
Stati Uniti d'America (Illinois)	Stati Uniti orientali
Stati Uniti d'America (Indiana)	Stati Uniti orientali
Stati Uniti d'America (Kentucky)	Stati Uniti orientali
Stati Uniti d'America (Louisiana)	Stati Uniti orientali
Stati Uniti d'America (Massachusetts)	Stati Uniti orientali
Stati Uniti d'America (Maryland)	Stati Uniti orientali
Stati Uniti d'America (Maine)	Stati Uniti orientali
Stati Uniti d'America (Michigan)	Stati Uniti orientali
Stati Uniti d'America (Minnesota)	Stati Uniti orientali
Stati Uniti d'America (Missouri)	Stati Uniti orientali
Stati Uniti d'America (Mississippi)	Stati Uniti orientali
Stati Uniti d'America (Carolina del Nord)	Stati Uniti orientali
Stati Uniti d'America (New Hampshire)	Stati Uniti orientali
Stati Uniti d'America (New Jersey)	Stati Uniti orientali
Stati Uniti d'America (New York)	Stati Uniti orientali
Stati Uniti d'America (Ohio)	Stati Uniti orientali
Stati Uniti d'America (Pennsylvania)	Stati Uniti orientali
Stati Uniti d'America (Rhode Island)	Stati Uniti orientali
Stati Uniti d'America (Carolina del Sud)	Stati Uniti orientali
Stati Uniti d'America (Tennessee)	Stati Uniti orientali
Stati Uniti d'America (Virginia)	Stati Uniti orientali
Stati Uniti d'America (Vermont)	Stati Uniti orientali
Stati Uniti d'America (Wisconsin)	Stati Uniti orientali
Stati Uniti d'America (Virginia Occidentale)	Stati Uniti orientali
Albania	Europa settentrionale (Irlanda)
Bosnia ed Erzegovina	Europa settentrionale (Irlanda)
Bulgaria	Europa settentrionale (Irlanda)
Bielorussia	Europa settentrionale (Irlanda)
Repubblica Ceca	Europa settentrionale (Irlanda)
Danimarca	Europa settentrionale (Irlanda)

Estonia	Europa settentrionale (Irlanda)
Finlandia	Europa settentrionale (Irlanda)
Regno Unito	Europa settentrionale (Irlanda)
Groenlandia	Europa settentrionale (Irlanda)
Grecia	Europa settentrionale (Irlanda)
Croazia	Europa settentrionale (Irlanda)
Ungheria	Europa settentrionale (Irlanda)
Irlanda	Europa settentrionale (Irlanda)
Islanda	Europa settentrionale (Irlanda)
Kirghizistan	Europa settentrionale (Irlanda)
Kazakistan	Europa settentrionale (Irlanda)
Lituania	Europa settentrionale (Irlanda)
Lettonia	Europa settentrionale (Irlanda)
Moldavia	Europa settentrionale (Irlanda)
Montenegro	Europa settentrionale (Irlanda)
Macedonia	Europa settentrionale (Irlanda)
Mongolia	Europa settentrionale (Irlanda)
Norvegia	Europa settentrionale (Irlanda)
Polonia	Europa settentrionale (Irlanda)
Romania	Europa settentrionale (Irlanda)
Serbia	Europa settentrionale (Irlanda)
Federazione russa	Europa settentrionale (Irlanda)
Svezia	Europa settentrionale (Irlanda)
Slovenia	Europa settentrionale (Irlanda)
Slovacchia	Europa settentrionale (Irlanda)
Tagikistan	Europa settentrionale (Irlanda)
Turkmenistan	Europa settentrionale (Irlanda)
Uzbekistan	Europa settentrionale (Irlanda)
Canada (Alberta)	Stati Uniti occidentali
Canada (Columbia Britannica)	Stati Uniti occidentali
Canada (Manitoba)	Stati Uniti occidentali
Canada (Territori del Nord-Ovest)	Stati Uniti occidentali
Canada (Nunavut)	Stati Uniti occidentali
Canada (Yukon)	Stati Uniti occidentali
Canada (Saskatchewan)	Stati Uniti occidentali
Messico	Stati Uniti occidentali

Stati Uniti d'America (Alaska)	Stati Uniti occidentali
Stati Uniti d'America (Arizona)	Stati Uniti occidentali
Stati Uniti d'America (California)	Stati Uniti occidentali
Stati Uniti d'America (Colorado)	Stati Uniti occidentali
Stati Uniti d'America (Hawaii)	Stati Uniti occidentali
Stati Uniti d'America (Idaho)	Stati Uniti occidentali
Stati Uniti d'America (Kansas)	Stati Uniti occidentali
Stati Uniti d'America (Montana)	Stati Uniti occidentali
Stati Uniti d'America (Dakota del Nord)	Stati Uniti occidentali
Stati Uniti d'America (Nebraska)	Stati Uniti occidentali
Stati Uniti d'America (Nuovo Messico)	Stati Uniti occidentali
Stati Uniti d'America (Nevada)	Stati Uniti occidentali
Stati Uniti d'America (Oklahoma)	Stati Uniti occidentali
Stati Uniti d'America (Oregon)	Stati Uniti occidentali
Stati Uniti d'America (Dakota del Sud)	Stati Uniti occidentali
Stati Uniti d'America (Texas)	Stati Uniti occidentali
Stati Uniti d'America (Utah)	Stati Uniti occidentali
Stati Uniti d'America (Washington)	Stati Uniti occidentali
Stati Uniti d'America (Wyoming)	Stati Uniti occidentali
Stati Uniti d'America (altre divisioni amministrative)	Stati Uniti orientali
Altri paesi	Europa occidentale (Paesi Bassi)

Accesso ai server DNS pubblici

Se non è possibile accedere ai server Kaspersky utilizzando il DNS di sistema, Kaspersky Security Center Cloud Console può utilizzare i seguenti server DNS pubblici, nel seguente ordine:

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Le richieste a questi server DNS possono contenere indirizzi di dominio e l'indirizzo IP pubblico dei dispositivi client, poiché Network Agent stabilisce una connessione TCP/UDP al server DNS. Se Kaspersky Security Center Cloud Console utilizza un server DNS pubblico, il trattamento dei dati è disciplinato dall'informativa sulla privacy del servizio pertinente.

Scenario: Creazione di una gerarchia di Administration Server gestiti tramite Kaspersky Security Center Cloud Console

In questo scenario vengono descritte le azioni che è necessario eseguire per creare una gerarchia di Administration Server gestiti tramite Kaspersky Security Center Cloud Console, che assume quindi il ruolo di Administration Server primario. Questa gerarchia può essere successivamente utilizzata per la migrazione di dispositivi e oggetti gestiti da Kaspersky Security Center a Kaspersky Security Center Cloud Console, nonché per la gestione di Administration Server secondari e dispositivi tramite Kaspersky Security Center Cloud Console.

Kaspersky Security Center Cloud Console può fungere solo da Administration Server primario, mentre gli Administration Server in esecuzione in locale possono fungere solo da Administration Server secondari. Non sono disponibili altri schemi gerarchici.

Prerequisiti

Prima di iniziare, assicurarsi che vengano soddisfatti i seguenti prerequisiti:

- Upgrade dell'Administration Server in esecuzione in locale alla versione 12 o successive.
- Installazione di Kaspersky Security Center Web Console nell'Administration Server in esecuzione in locale.
- Installazione dei plug-in Web per le applicazioni che si intende gestire tramite Kaspersky Security Center Cloud Console.
- Upgrade delle applicazioni gestite alle versioni supportate da Kaspersky Security Center Cloud Console.
- Verifica che per l'attività Scarica aggiornamenti nell'archivio dell'Administration Server nell'Administration Server in esecuzione in locale non sia assegnato l'Administration Server primario come sorgente aggiornamenti. Se necessario, conseguente modifica delle impostazioni dell'attività.

Dopo la creazione della gerarchia, i criteri e le attività validi in Kaspersky Security Center Cloud Console vengono applicati nell'Administration Server secondario, sostituendo quindi i criteri e le attività esistenti. Se si desidera evitare questo comportamento, eliminare tutti i criteri e le attività di Kaspersky Security Center Cloud Console prima della creazione della gerarchia. In alternativa, è possibile modificare lo stato di ciascun criterio di Kaspersky Security Center Cloud Console in **Inattivo** nelle relative impostazioni e disabilitare l'opzione **Distribuisci negli Administration Server secondari e virtuali** nelle impostazioni di ogni attività di Kaspersky Security Center Cloud Console.

È possibile eliminare la gerarchia di Administration Server in qualsiasi momento, se necessario.

Passaggi della creazione della gerarchia

Lo scenario di base prevede un Administration Server secondario a cui non è possibile accedere tramite Internet. Tuttavia, il set di azioni all'interno di alcuni dei passaggi descritti di seguito può variare se l'Administration Server secondario è accessibile tramite Internet. Inoltre, alcuni passaggi devono essere ignorati in questo caso.

La creazione di una gerarchia di Administration Server comprende i seguenti passaggi:

1. **Recupero del certificato dell'Administration Server secondario**

   Se l'Administration Server secondario è accessibile tramite Internet, ignorare questo passaggio.

   In Kaspersky Security Center Web Console in esecuzione in locale aprire le proprietà dell'Administration Server e nella scheda **Generale**, aprire la sezione **Generale**. Fare clic sul collegamento **Visualizza certificato di Administration Server**. Il file del certificato, in formato CER, viene salvato automaticamente nella cartella specificata nelle impostazioni del browser.

2. **Recupero delle impostazioni di connessione e dei certificati da Kaspersky Security Center Cloud Console**

   Se l'Administration Server secondario è accessibile tramite Internet, ignorare questo passaggio.

   In Kaspersky Security Center Cloud Console aprire le proprietà dell'Administration Server e nella scheda **Generale** aprire la sezione **Gerarchia di Administration Server**. Vengono visualizzate le seguenti impostazioni di connessione:

   - Indirizzo HDS

     Visualizza l'indirizzo Web utilizzato per la connessione a HDS (Hosted Discovery Service).

   - Porta HDS

     Visualizza il numero della porta utilizzata per la connessione a HDS.

   La sezione contiene inoltre due collegamenti:

   - Visualizza certificato di Administration Server

     Facendo clic su questo collegamento viene avviato il download della chiave pubblica del certificato dell'istanza di Kaspersky Security Center Cloud Console.

   - Certificato autorità di certificazione radice HDS

     Facendo clic su questo collegamento viene avviato il download del file in formato PEM contenente un elenco di certificati radice attendibili rilasciati da autorità di certificazione. Questo file è destinato all'utilizzo da parte dell'Administration Server secondario: è necessario per verificare il certificato HDS.

   Copiare manualmente le impostazioni di connessione, utilizzando gli Appunti o un altro modo, e salvarle in un file del formato desiderato. Fare clic sul collegamento **Visualizza certificato di Administration Server** e attendere il download del file del certificato. Fare clic sul collegamento **Certificato autorità di certificazione radice HDS** e attendere il download del file con l'elenco dei certificati radice attendibili rilasciati delle autorità di certificazione. Entrambi i file vengono salvati nella cartella specificata nelle impostazioni del browser.

3. **Selezione dell'Administration Server secondario per la connessione**

   Nelle proprietà dell'Administration Server passare alla scheda **Administration Server**. Nella gerarchia dei gruppi di amministrazione selezionare la casella di controllo accanto al gruppo di amministrazione in cui si desidera inserire l'Administration Server secondario con tutti i relativi dispositivi gestiti. Fare clic sul pulsante **Connetti Administration Server secondario**.

Nella pagina visualizzata, nel campo **Nome visualizzato dell'Administration Server secondario** specificare il nome con cui deve essere visualizzato l'Administration Server secondario nella gerarchia. Viene utilizzato solo per comodità e può differire dal nome effettivo dell'Administration Server secondario, se necessario. Fare clic su **Avanti**.

Se l'Administration Server secondario è accessibile tramite Internet, è necessario specificare anche l'indirizzo dell'Administration Server secondario nel campo **Indirizzo dell'Administration Server secondario (facoltativo)**.

Nella pagina successiva fare clic sul pulsante **Sfoglia** e specificare il file con estensione PEM salvato dall'Administration Server secondario. Fare clic su **Avanti**.

4. **Abilitazione e configurazione del server proxy**

   Le azioni descritte in questo passaggio sono facoltative. Eseguirle solo se la connessione richiede l'utilizzo del server proxy.

   Fare clic su **Avanti**. Nella pagina **Definire la modalità di connessione dell'Administration Server secondario all'Administration Server primario**, è possibile abilitare e configurare l'utilizzo del server proxy, se necessario. Selezionare la casella di controllo **Usa server proxy** e specificare le seguenti impostazioni del proxy:

   - Indirizzo

     L'indirizzo del server proxy.

   - Nome utente

     Nome utente per accedere al server proxy.

   - Password

     Password per accedere al server proxy.

5. **Specifica delle impostazioni di autenticazione e aggiunta dell'Administration Server secondario alla gerarchia**

   Fare clic su **Avanti**. Nella pagina **Credenziali per l'Administration Server secondario**, specificare le seguenti impostazioni:

   - Nome utente

     Il nome utente con cui si accede all'Administration Server secondario.

   - Password

     Password utilizzata per accedere all'Administration Server secondario.

   Fare clic su **Avanti** e attendere che l'Administration Server secondario venga visualizzato nella gerarchia.

   Se l'Administration Server secondario è accessibile tramite Internet, questo si connette all'Administration Server primario.

Se l'Administration Server secondario è accessibile tramite Internet e la connessione tra i due Administration Server è stata stabilita correttamente, ignorare tutti i passaggi successivi.

Se non è possibile accedere all'Administration Server secondario tramite Internet, questo diventa visibile, ma per controllarlo è necessario eseguire azioni aggiuntive nell'Administration Server secondario.

6. **Configurazione della connessione in Kaspersky Security Center Web Console in esecuzione in locale**

   In Kaspersky Security Center Web Console in esecuzione in locale aprire le proprietà dell'Administration Server e nella scheda **Generale** aprire la sezione **Gerarchia di Administration Server**. Selezionare la casella di controllo **Questo Administration Server è secondario nella gerarchia**. Nell'elenco **Tipo di Administration Server primario**, selezionare l'opzione **Kaspersky Security Center Cloud Console**.

   Kaspersky Security Center Web Console verifica se l'Administration Server primario è specificato come sorgente degli aggiornamenti nell'attività *Scarica aggiornamenti nell'archivio di Administration Server*. Se l'Administration Server primario viene specificato come sorgente aggiornamenti, l'utente riceve il messaggio di avviso corrispondente e un collegamento alle impostazioni dell'attività. È possibile modificare le impostazioni e quindi tornare alla creazione della gerarchia oppure ignorare questa azione e procedere con la creazione della gerarchia.

   Nel gruppo **Impostazioni per stabilire la connessione tra gli Administration Server secondari e primari**, specificare le seguenti impostazioni:

   - Indirizzo server HDS (dall'Administration Server primario in Cloud Console)

     Immettere l'indirizzo del server HDS in formato FQDN (Fully Qualified Domain Name), copiato e salvato dalle proprietà dell'Administration Server in Kaspersky Security Center Cloud Console.

   - Porte del server HDS

     Immettere i numeri delle porte del server HDS, copiati e salvati dalle proprietà dell'Administration Server in Kaspersky Security Center Cloud Console.

7. **Aggiunta dei certificati dell'Administration Server secondario**

   Fare clic sul pulsante **Specifica certificato Administration Server primario** e specificare il file di certificato salvato dalle proprietà dell'Administration Server in Kaspersky Security Center Cloud Console.

   Fare clic sul pulsante **Specifica certificati Hosted Discovery Service** e specificare il file PEM salvato dalle proprietà dell'Administration Server in Kaspersky Security Center Cloud Console.

   Se è stato abilitato l'utilizzo del server proxy durante la connessione dell'Administration Server secondario in Kaspersky Security Center Cloud Console, selezionare la casella di controllo **Usa server proxy** e specificare le stesse impostazioni proxy presenti in Kaspersky Security Center Cloud Console.

   È inoltre possibile selezionare la casella di controllo **Connetti l'Administration Server primario all'Administration Server secondario nella rete perimetrale** se l'Administration Server secondario si trova in una rete perimetrale.

   L'Administration Server secondario si connette all'Administration Server primario.

Risultati

Dopo aver eseguito i passaggi precedenti, è possibile assicurarsi che la gerarchia venga creata correttamente:

- I criteri attivi dell'Administration Server primario diventano effettivi nell'Administration Server secondario. Le attività dell'Administration Server primario vengono distribuite all'Administration Server secondario. Se l'opzione **Distribuisci negli Administration Server secondari e virtuali** è abilitata nelle impostazioni di un'attività di gruppo, ogni attività viene distribuita anche nell'Administration Server secondario.

- Per le impostazioni dei criteri per cui sono vietate le modifiche nell'Administration Server primario viene visualizzato lo stato Blocco delle modifiche in tutti i criteri dell'Administration Server secondario.

- I criteri applicati dall'Administration Server primario vengono visualizzati nell'elenco dei criteri dell'Administration Server secondario (**Risorse (dispositivi)** → **Criteri e profili**).

- Le attività di gruppo distribuite dall'Administration Server primario vengono visualizzate nell'elenco delle attività dell'Administration Server secondario (**Risorse (dispositivi)** → **Attività**).

- I criteri e le attività creati nell'Administration Server primario non possono essere modificati nell'Administration Server secondario.

- In Kaspersky Security Center Cloud Console, nella struttura dei gruppi di amministrazione l'Administration Server secondario viene visualizzato all'interno del gruppo selezionato quando è stato aggiunto l'Administration Server.

Migrazione a Kaspersky Security Center Cloud Console

Questa sezione descrive il processo di migrazione da Kaspersky Security Center Web Console versione 12 (o successive) in esecuzione in locale a Kaspersky Security Center Cloud Console.

Metodi di migrazione a Kaspersky Security Center Cloud Console

Questa sezione fornisce informazioni sui metodi disponibili per la migrazione da Kaspersky Security Center in esecuzione in locale a Kaspersky Security Center Cloud Console.

Utilizzando la funzionalità di migrazione, è possibile trasferire i dispositivi della rete da Kaspersky Security Center, nell'ambito della gestione di Kaspersky Security Center Cloud Console. Verrà eseguito il passaggio dei dispositivi gestiti mantenendo le impostazioni principali, come l'appartenenza a gruppi di amministrazione; nonché gli oggetti essenziali, quali criteri e attività relativi alle applicazioni gestite.

È possibile scegliere uno dei due metodi disponibili per la migrazione degli Administration Server a Kaspersky Security Center Cloud Console:

- Migrazione senza una gerarchia di Administration Server:
  - Consente il trasferimento dei dispositivi gestiti e degli oggetti correlati a Kaspersky Security Center Cloud Console anche se l'Administration Server locale non è secondario rispetto a Kaspersky Security Center Cloud Console.
  - Potrebbe richiedere il trasferimento di file (su un'unità rimovibile, tramite e-mail, tramite cartelle condivise o in altro modo) se Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console sono aperti in diversi dispositivi fisici.

  È inoltre possibile eseguire la migrazione con gli Administration Server virtuali se inclusi nella rete.

- Migrazione con l'utilizzo di una gerarchia di Administration Server:
  - Consente il trasferimento dei dispositivi gestiti e degli oggetti correlati a Kaspersky Security Center Cloud Console utilizzando solo l'interfaccia di Kaspersky Security Center Cloud Console, pertanto non è necessario il trasferimento fisico dei file.
  - Richiede che l'Administration Server in esecuzione in locale funga da secondario per Kaspersky Security Center Cloud Console. È possibile creare tale gerarchia prima di iniziare la migrazione.

Per il criptaggio dell'intero disco, Kaspersky Security Center Cloud Console supporta solo BitLocker.

Scenario: Migrazione senza una gerarchia di Administration Server

Questa sezione descrive la migrazione dei dispositivi gestiti e degli oggetti correlati (ad esempio criteri, attività, rapporti) da Kaspersky Security Center Web Console in esecuzione in locale a Kaspersky Security Center Cloud Console. È possibile includere un singolo gruppo di amministrazione nell'ambito della migrazione per ripristinare lo stesso gruppo di amministrazione in Kaspersky Security Center Cloud Console.

Questo gruppo deve contenere i dispositivi gestiti di un singolo sistema operativo. Se la rete include i dispositivi di diversi sistemi operativi o distribuzioni Linux, allocarli in diversi gruppi di amministrazione, quindi eseguire la migrazione di ciascun gruppo separatamente.

Dopo aver completato la migrazione, tutti i Network Agent nell'ambito della migrazione verranno aggiornati e gestiti da Kaspersky Security Center Cloud Console.

I passaggi elencati in questa sezione illustrano il processo di migrazione eseguito quando non esiste una gerarchia di Administration Server, ovvero non è stata stabilita alcuna connessione tra Kaspersky Security Center Cloud Console e Kaspersky Security Center Web Console in esecuzione in locale.

Prerequisiti

Prima di iniziare, procedere come segue:

- Eseguire l'upgrade di Administration Server in esecuzione in locale alla seguente versione:
  - Per dispositivi Windows, versione 12 o successiva
  - Per dispositivi Linux, versione 12 Patch A o successiva
- Installare Kaspersky Security Center Web Console versione 12.1 o successiva.
- Eseguire l'upgrade di Network Agent nei dispositivi gestiti alla versione 12 o successiva.
- Nei dispositivi Windows utilizzare Network Agent senza una password di disinstallazione.

  Se la password è già stata impostata, eseguire una delle seguenti operazioni in Kaspersky Security Center Web Console:
  - Disabilitare l'opzione **Usa password di disinstallazione** in impostazioni del criterio di Network Agent.
  - Disinstallare Network Agent da remoto utilizzando l'attività *Disinstalla l'applicazione in remoto*. Nel campo **Applicazione da disinstallare** dell'attività, selezionare **Kaspersky Security Center Network Agent**. Non dimenticare di inserire la password di disinstallazione.
- Eseguire l'upgrade delle applicazioni gestite alle versioni supportate da Kaspersky Security Center Cloud Console.
- Assicurarsi di disporre dei criteri per le versioni più recenti delle applicazioni gestite. Se si utilizzano criteri obsoleti, crearne di nuovi per le versioni delle applicazioni supportate da Kaspersky Security Center Cloud Console.
- Per utilizzare criteri validi, eseguire l'upgrade dei plug-in Web per le applicazioni che si intende gestire tramite Kaspersky Security Center Cloud Console.
- Disinstallare le applicazioni Kaspersky dai dispositivi gestiti se queste applicazioni non sono supportate da Kaspersky Security Center Cloud Console, quindi sostituire le applicazioni disinstallate con quelle supportate.
- Decriptare tutti i dati (a livello di disco o di file) criptati da Kaspersky Endpoint Security for Windows nei dispositivi gestiti che eseguono il sistema operativo Windows, quindi disabilitare la funzionalità di criptaggio nei dispositivi gestiti tramite i criteri dell'applicazione o in locale. Per ulteriori informazioni, vedere la Guida relativa a Kaspersky Endpoint Security for Windows.

Se in un dispositivo Windows sono ancora archiviati file o cartelle criptati tramite Kaspersky Endpoint Security for Windows, l'upgrade di Network Agent verrà annullato durante il processo di migrazione. Una notifica richiederà di decriptare tutti i dati nel dispositivo e disabilitare la funzionalità di criptaggio.

Kaspersky Security Center Cloud Console consente un massimo di 25.000 dispositivi gestiti per un Administration Server.

Fasi della migrazione

La migrazione a Kaspersky Security Center Cloud Console comprende le seguenti fasi:

1. **Pianificazione dell'ambito della migrazione e verifica dei prerequisiti**

   Stimare l'ambito del processo di migrazione, quindi esaminare il gruppo di amministrazione da esportare e valutare il numero di dispositivi gestiti che contiene. Assicurarsi inoltre che tutte le attività elencate come prerequisiti per la migrazione siano state completate correttamente.

2. **Esportazione di impostazioni, oggetti e dispositivi gestiti da Kaspersky Security Center Web Console**

   Utilizzare la Migrazione guidata di Kaspersky Security Center Web Console in esecuzione in locale per esportare i dispositivi gestiti insieme ai relativi oggetti.

   Le dimensioni massime del file di esportazione sono pari a 4 GB.

3. **Importazione del file di esportazione in Kaspersky Security Center Cloud Console**

   Trasferire le informazioni sui dispositivi e sugli oggetti gestiti in Kaspersky Security Center Cloud Console. A tale scopo, utilizzare la Migrazione guidata di Kaspersky Security Center Cloud Console per importare il file di esportazione e creare un pacchetto di installazione indipendente di Network Agent.

4. **Reinstallazione di Network Agent nei dispositivi gestiti**

   Tornare alla Migrazione guidata in Kaspersky Security Center Web Console in esecuzione in locale per creare un'attività di installazione remota. Sarà possibile utilizzare questa attività (immediatamente o in seguito) per reinstallare Network Agent nei dispositivi gestiti e completare il processo di migrazione.

Risultati

Al termine della migrazione, è possibile verificare che il processo abbia avuto esito positivo:

- Network Agent è stato reinstallato in tutti i dispositivi gestiti.
- Tutti i dispositivi sono gestiti tramite Kaspersky Security Center Cloud Console.
- Tutte le impostazioni degli oggetti applicate prima della migrazione sono state mantenute.

Migrazione guidata

Questa sezione fornisce informazioni sulla Migrazione guidata in Kaspersky Security Center Cloud Console e Kaspersky Security Center Web Console versione 12 o successive.

Passaggio 1. Esportazione di impostazioni, oggetti e dispositivi gestiti da Kaspersky Security Center Web Console

Per eseguire la migrazione dei dispositivi gestiti da Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console, è innanzitutto necessario creare un file di esportazione contenente le informazioni sulla gerarchia dei gruppi di amministrazione presenti nell'Administration Server attuale in esecuzione in locale. Il file di esportazione deve contenere anche informazioni sugli oggetti e sulle relative impostazioni. Questo file di esportazione verrà utilizzato per la successiva importazione in Kaspersky Security Center Cloud Console.

Le dimensioni massime del file di esportazione sono pari a 4 GB.

Per esportare gli oggetti e le relative impostazioni da Kaspersky Security Center Web Console:

1. Nel menu principale di Kaspersky Security Center Web Console, passare a **Operazioni** → **Migrazione**.
2. Nella pagina iniziale della Migrazione guidata fare clic su **Avanti**. Verrà visualizzata la pagina **Dispositivi gestiti da esportare**, che mostra l'intera gerarchia dei gruppi di amministrazione dell'Administration Server corrispondente.
3. Nella pagina **Dispositivi gestiti da esportare** fare clic sull'icona della freccia di espansione (>) accanto al nome del gruppo **Dispositivi gestiti** per espandere la gerarchia dei gruppi di amministrazione. Selezionare il gruppo di amministrazione che si desidera esportare.

   Dopo la migrazione da Kaspersky Security Center in esecuzione in locale a Kaspersky Security Center Cloud Console eseguita per due gruppi di amministrazione, le attività di installazione remota per questi gruppi vengono visualizzate con lo stesso nome.

4. Selezionare le applicazioni gestite per cui i criteri e le attività devono essere trasferiti in Kaspersky Security Center Cloud Console insieme agli oggetti del gruppo. Per selezionare le applicazioni gestite di cui devono essere esportati gli oggetti, selezionare le caselle di controllo accanto ai relativi nomi nell'elenco.

   Sebbene Kaspersky Security Center Administration Server sia presente nell'elenco, la selezione della casella di controllo corrispondente non comporta l'esportazione dei relativi criteri.

   Per assicurarsi che le applicazioni gestite siano supportate da Kaspersky Security Center Cloud Console, fare clic sul collegamento corrispondente. Si verrà reindirizzati all'argomento della Guida in linea contenente l'elenco delle applicazioni gestite da Kaspersky Security Center Cloud Console.

   Se selezioni applicazioni che non sono supportate da Kaspersky Security Center Cloud Console, i criteri e le attività di queste applicazioni verranno comunque esportati e quindi importati, ma non sarà possibile gestirli in Kaspersky Security Center Cloud Console a causa della mancata disponibilità dei plug-in dedicati.

5. Visualizzare l'elenco degli oggetti di gruppo esportati per impostazione predefinita e, se necessario, specificare gli oggetti non di gruppo da esportare insieme al gruppo di amministrazione selezionato. Configurare l'ambito di esportazione includendo o escludendo vari oggetti, come attività globali, selezioni dispositivi personalizzate, rapporti, ruoli personalizzati, utenti interni, gruppi di sicurezza e categorie di applicazioni personalizzate. Questa pagina include le seguenti sezioni:

   - **Attività globali**

L'elenco delle attività globali delle applicazioni gestite, nonché delle attività globali di Network Agent.

Se un'attività globale selezionata è applicabile a una selezione di oggetti specifici, anche questa selezione verrà esportata.

Sebbene le attività globali di Administration Server siano presenti nell'elenco, non è possibile esportarle; la selezione di tali attività non influisce sull'ambito di esportazione. Anche le attività di installazione remota rimangono al di fuori dell'ambito di esportazione, poiché i rispettivi pacchetti di installazione non possono essere esportati.

- **Selezioni dispositivi**

  L'elenco delle selezioni dispositivi personalizzate.

- **Rapporti**

  L'elenco modificabile delle istanze dei rapporti da esportare.

  Se un rapporto selezionato è applicabile a una selezione di oggetti specifici, anche questa selezione verrà esportata.

  Kaspersky Security Center Cloud Console contiene lo stesso set di modelli di rapporto di Kaspersky Security Center Web Console, quindi è possibile selezionare per l'esportazione solo i rapporti creati manualmente o riconfigurati.

- **Oggetti del gruppo**

L'elenco degli oggetti di gruppo da esportare per impostazione predefinita. I seguenti oggetti correlati al gruppo di amministrazione selezionato verranno esportati completamente per impostazione predefinita:

- Struttura del gruppo di amministrazione, ovvero tutti i sottogruppi del gruppo di amministrazione selezionato
- Dispositivi inclusi nei gruppi di amministrazione da esportare
- Tag assegnati ai dispositivi da esportare

  Se un tag è stato creato in Kaspersky Security Center Web Console ma non è mai stato assegnato ad alcun dispositivo, non verrà esportato. Nemmeno le regole di tagging automatico verranno esportate.

- Criteri di gruppo delle applicazioni gestite selezionate

  I criteri di Administration Server e i criteri di Network Agent non vengono esportati.

- Attività di gruppo delle applicazioni gestite che sono state selezionate e attività di gruppo di Network Agent

  Le attività di Administration Server non vengono esportate.

È anche possibile impedire l'esportazione di alcuni tipi di oggetti non di gruppo:

- Per annullare l'esportazione dei ruoli personalizzati (ovvero quelli creati solo dall'utente), selezionare la casella di controllo **Escludi i ruoli personalizzati dall'esportazione**.
- Per annullare l'esportazione di utenti interni e gruppi di sicurezza, selezionare la casella di controllo **Escludi gli utenti interni e i gruppi di protezione dall'esportazione**.
- Per annullare l'esportazione delle categorie di applicazioni personalizzate con il contenuto aggiunto manualmente, selezionare la casella di controllo **Escludi le categorie di applicazioni personalizzate dall'esportazione**.

Se si trasferiscono dispositivi di vari sistemi operativi a Kaspersky Security Center Cloud Console, la migrazione degli oggetti non di gruppo deve essere eseguita una sola volta.

La Migrazione guidata controlla il numero totale di dispositivi gestiti inclusi nel gruppo di amministrazione selezionato. Se questo numero è superiore a 10.000 viene visualizzato un messaggio di errore. Il pulsante **Avanti** resta non disponibile (in grigio) finché il numero di dispositivi gestiti nel gruppo di amministrazione selezionato non rientra nel limite.

6. Dopo aver definito l'ambito della migrazione, fare clic su **Avanti** per avviare il processo di esportazione. Verrà visualizzata la pagina **Creazione del file di esportazione**, in cui è possibile visualizzare lo stato di avanzamento dell'esportazione per ciascun tipo di oggetto incluso nell'ambito della migrazione. Attendere finché le icone di aggiornamento (🔄) accanto a tutti gli elementi nell'elenco di oggetti non vengono sostituite con segni di spunta verdi (✓). Il processo di esportazione viene completato e il file di esportazione viene scaricato automaticamente

nella posizione di download predefinita specificata nelle impostazioni del browser. Il nome del file di esportazione viene visualizzato nella parte inferiore della finestra del browser.

7. Quando viene visualizzata la pagina **Esportazione completata**, procedere alla fase successiva eseguita in Kaspersky Security Center Cloud Console.

Se si utilizza Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console in dispositivi diversi, sarà necessario copiare il file di esportazione in un'unità rimovibile o scegliere altri modi per trasferire il file.

Passaggio 2. Importazione del file di esportazione in Kaspersky Security Center Cloud Console

Per trasferire le informazioni sui dispositivi gestiti, gli oggetti e le relative impostazioni esportate da Kaspersky Security Center Web Console, è necessario importarle in Kaspersky Security Center Cloud Console distribuita nell'area di lavoro. Ciò consente di creare un pacchetto di installazione indipendente e utilizzarlo per la reinstallazione di Network Agent nei dispositivi gestiti.

Prima di avviare la Migrazione guidata in Kaspersky Security Center Cloud Console, assicurarsi che la lingua di localizzazione corrente sia la stessa della lingua di Kaspersky Security Center Web Console durante il processo di esportazione. Se necessario, cambiare la lingua.

Se in precedenza è stato completato l'Avvio rapido guidato nell'area di lavoro di Kaspersky Security Center Cloud Console, il gruppo **Dispositivi gestiti** include criteri e attività creati con le impostazioni predefinite. Eliminare tali criteri e attività prima di importare quelli esportati da Kaspersky Security Center Web Console.

Per importare il file di esportazione in Kaspersky Security Center Cloud Console:

1. Nel menu principale di Kaspersky Security Center Web Console, passare a **Operazioni** → **Migrazione**.

2. Nella pagina iniziale della Migrazione guidata fare clic su **Importa**. Nella finestra Esplora file di Windows visualizzata selezionare il file di esportazione passando alla cartella in cui è stato salvato e fare clic su **Apri**. Attendere finché l'icona di aggiornamento (🔄) accanto allo stato di caricamento del file non viene sostituita con un segno di spunta verde (✓).

3. Fare clic su **Avanti**. Verrà visualizzata la pagina successiva, che mostra l'intera gerarchia dei gruppi di amministrazione di Administration Server in Kaspersky Security Center Cloud Console.

4. Selezionare la casella di controllo accanto al gruppo di amministrazione di destinazione in cui devono essere ripristinati gli oggetti del gruppo e fare clic su **Avanti**. La Migrazione guidata visualizza un elenco di pacchetti di installazione di Network Agent disponibili in Kaspersky Security Center Cloud Console.

5. Selezionare il pacchetto di installazione contenente la versione e la localizzazione appropriate di Network Agent e fare clic su **Avanti**.

Selezionare il pacchetto di installazione di Kaspersky Network Agent per Windows solo se in precedenza è stato completato l'avvio rapido guidato nell'area di lavoro di Kaspersky Security Center Cloud Console e se si esegue la migrazione dei dispositivi Windows.

Attendere finché la Migrazione guidata non crea un pacchetto di installazione indipendente. Le dimensioni massime del file del pacchetto di installazione indipendente per Network Agent sono pari a 200 MB.

Il file viene decompresso e scaricato automaticamente nella posizione di download predefinita specificata nelle impostazioni del browser. Gli oggetti non di gruppo e gli oggetti di gruppo vengono ripristinati nel gruppo di amministrazione di destinazione.

Al termine dell'importazione, la struttura esportata dei gruppi di amministrazione, inclusi i dettagli dei dispositivi, viene visualizzata sotto il gruppo di amministrazione di destinazione selezionato. Se il nome dell'oggetto ripristinato è identico al nome di un oggetto esistente, all'oggetto ripristinato viene aggiunto un suffisso incrementale.

Se è stato importato l'intero gruppo **Dispositivi gestiti**, è consigliabile rinominare il nuovo sottogruppo importato per evitare confusione:

a. Passare alla sezione **Gerarchia dei gruppi**.

b. Fare clic sul nome del sottogruppo nella struttura dei gruppi.

c. Nella finestra delle proprietà visualizzata, nel campo **Nome**, immettere un nome diverso (ad esempio "Dispositivi migrati").

È consigliabile verificare se gli oggetti (criteri, attività e dispositivi gestiti) inclusi nell'ambito di esportazione sono stati importati correttamente in Kaspersky Security Center Cloud Console. A tale scopo, accedere alla sezione **Risorse (dispositivi)** e visualizzare se gli oggetti importati vengono visualizzati negli elenchi delle sottosezioni **Criteri e profili**, **Attività** e **Dispositivi gestiti**.

Non è possibile ridurre a icona la Migrazione guidata ed eseguire operazioni simultanee durante l'importazione. Attendere finché le icone di aggiornamento (🔄) accanto a tutti gli elementi nell'elenco di oggetti non vengono sostituite con segni di spunta verdi (✓). A questo punto, l'importazione è stata completata. Successivamente, i dispositivi iniziano il passaggio a Kaspersky Security Center Cloud Console.

6. Fare clic su **Fine** per chiudere la finestra della Migrazione guidata.

7. Se si desidera trovare e scaricare nuovamente il pacchetto di installazione indipendente, accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione** e fare clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti**. Nell'elenco visualizzato selezionare il pacchetto di installazione indipendente creato e fare clic sul pulsante **Scarica**.

Se si utilizza Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console in dispositivi diversi, è necessario copiare il pacchetto di installazione indipendente in un'unità rimovibile o scegliere altri modi per trasferire il file.

Passaggio 3. Reinstallazione di Network Agent nei dispositivi gestiti tramite Kaspersky Security Center Cloud Console

Dopo aver creato il pacchetto di installazione indipendente di Network Agent, è possibile procedere alla creazione di un'attività di installazione remota. L'esecuzione di questa attività consente di reinstallare Network Agent in tutti i dispositivi gestiti, in modo da configurare tali dispositivi per la gestione tramite Kaspersky Security Center Cloud Console.

Per ridurre il rischio di perdita di dati è consigliabile eseguire prima le azioni per un piccolo gruppo di amministrazione con un massimo di 20 dispositivi gestiti situati all'interno della rete aziendale e senza server fisici. Dopo aver terminato queste azioni, verificare se la reinstallazione è stata completata correttamente e procedere con l'ambito della reinstallazione completo.

Per creare un'attività di installazione remota e reinstallare Network Agent:

1. Tornare alla Migrazione guidata in Kaspersky Security Center Web Console in esecuzione in locale.

   Si consiglia di utilizzare la Migrazione guidata per creare un'attività di installazione remota per reinstallare Network Agent come descritto di seguito. Se è necessario utilizzare un'attività di installazione remota personalizzata, occorre innanzitutto creare manualmente un pacchetto di installazione personalizzato dal pacchetto di installazione indipendente di Network Agent. Si noti che quando si crea un pacchetto di installazione personalizzato, è necessario specificare la chiave "-s" nella riga di comando del file eseguibile. In caso contrario, la reinstallazione di Network Agent da questo pacchetto di installazione personalizzato viene completata con un errore.

   A seconda dello stato corrente della Migrazione guidata, è possibile effettuare una delle seguenti operazioni:

   - Se la Migrazione guidata non è stata chiusa dopo l'esportazione e la sessione non è scaduta, fare clic sul pulsante **Vai al passaggio 3 della Migrazione guidata**. Selezionare la casella di controllo **Carica pacchetto di installazione indipendente** e fare clic sul pulsante **Seleziona pacchetto di installazione indipendente**. Nella finestra del browser visualizzata specificare il pacchetto di installazione indipendente di Network Agent.

   - Se per qualsiasi motivo è necessario riavviare la Migrazione guidata, selezionare la casella di controllo **Carica pacchetto di installazione indipendente** e fare clic sul pulsante **Seleziona pacchetto di installazione indipendente**. Nella finestra del browser visualizzata specificare il pacchetto di installazione indipendente di Network Agent. Successivamente, la Migrazione guidata visualizza nuovamente la gerarchia dei gruppi di amministrazione di questo Administration Server. Selezionare lo stesso gruppo per cui è stato creato il file di esportazione e fare clic su **Avanti**.

     La Migrazione guidata controlla nuovamente il numero totale di dispositivi gestiti inclusi nel gruppo di amministrazione selezionato. Se questo numero è superiore a 10.000 viene visualizzato un messaggio di errore. Il pulsante **Avanti** resta non disponibile (in grigio) finché il numero di dispositivi gestiti nel gruppo di amministrazione selezionato non rientra nel limite.

2. Attendere il caricamento del pacchetto di installazione indipendente, quindi fare clic su **Avanti**. La Migrazione guidata crea un pacchetto di installazione personalizzato e un'attività di installazione remota per tale pacchetto. L'ambito dell'attività includerà il gruppo di amministrazione selezionato nella pagina **Dispositivi gestiti da esportare**. La pianificazione di avvio dell'attività verrà impostata su **Manualmente** per impostazione predefinita. La Migrazione guidata visualizza lo stato di avanzamento della creazione. Attendere finché le icone di aggiornamento (🔄) non sono sostituite da segni di spunta verdi (✓) e fare clic su **Avanti**.

3. Se necessario, selezionare la casella di controllo **Esegui l'attività di installazione remota appena creata** (deselezionata per impostazione predefinita) per i dispositivi nel gruppo di amministrazione selezionato dell'Administration Server in esecuzione in locale e tutti i relativi sottogruppi. In questo caso, i dispositivi verranno configurati per la gestione tramite Kaspersky Security Center Cloud Console, ma solo al termine dell'installazione di Network Agent. Sarà visualizzato il percorso completo del gruppo di amministrazione in cui verrà eseguita l'attività.

L'attività deve essere avviata solo al termine dell'importazione in Kaspersky Security Center Cloud Console. In caso contrario, i nomi dei dispositivi potrebbero essere duplicati nell'elenco.

4. Fare clic su **Fine** per chiudere la Migrazione guidata e avviare l'attività di installazione remota per i seguenti scopi:

   - Upgrade delle istanze di Network Agent
   - Configurazione delle istanze di Network Agent per la gestione tramite Kaspersky Security Center Cloud Console

   Se la casella di controllo **Esegui l'attività di installazione remota appena creata** è stata mantenuta deselezionata, è possibile avviare manualmente l'attività in un secondo momento, se necessario.

È possibile verificare di poter gestire le istanze di Network Agent di cui è stata eseguita la migrazione tramite Kaspersky Security Center Cloud Console. A tale scopo, accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**. Assicurarsi che i dispositivi gestiti di cui è stata eseguita la migrazione abbiano l'icona di conferma (✓) nelle colonne **Visibile**, **Network Agent installato** e **Network Agent è in esecuzione**. Assicurarsi inoltre che questi dispositivi non dispongano della descrizione dello stato *Connessione non eseguita da molto tempo*.

Migrazione con una gerarchia di Administration Server

Questa sezione descrive la migrazione dei dispositivi gestiti e degli oggetti correlati da Kaspersky Security Center Web Console in esecuzione in locale a Kaspersky Security Center Cloud Console. Il processo prevede una gerarchia: Kaspersky Security Center Web Console in esecuzione in locale funge da Administration Server secondario e Kaspersky Security Center Cloud Console funge da Administration Server primario.

Ogni gruppo di amministrazione trasferito a Kaspersky Security Center Cloud Console deve contenere i dispositivi gestiti di un singolo sistema operativo. Se la rete include i dispositivi di diversi sistemi operativi, allocarli in diversi gruppi di amministrazione, quindi eseguire la migrazione di ciascun gruppo separatamente.

Dopo aver completato la migrazione, tutti i Network Agent del gruppo nell'ambito della migrazione verranno aggiornati e gestiti tramite Kaspersky Security Center Cloud Console.

Prima di iniziare, procedere come segue:

- Eseguire l'upgrade di Administration Server in esecuzione in locale alla seguente versione:
  - Per dispositivi Windows, versione 12 o successiva
  - Per dispositivi Linux, versione 12 Patch A o successiva
- Installare Kaspersky Security Center Web Console versione 12.1 o successiva.
- Eseguire l'upgrade di Network Agent nei dispositivi gestiti alla versione 12 o successiva.
- Nei dispositivi Windows utilizzare Network Agent senza una password di disinstallazione.

  Se la password è già stata impostata, eseguire una delle seguenti operazioni in Kaspersky Security Center Web Console:

- Disabilitare l'opzione **Usa password di disinstallazione** in impostazioni del criterio di Network Agent.
- Disinstallare Network Agent da remoto utilizzando l'attività *Disinstalla l'applicazione in remoto*. Nel campo **Applicazione da disinstallare** dell'attività, selezionare **Kaspersky Security Center Network Agent**. Non dimenticare di inserire la password di disinstallazione.

- Eseguire l'upgrade delle applicazioni gestite alle versioni supportate da Kaspersky Security Center Cloud Console.
- Assicurarsi di disporre dei criteri per le versioni più recenti delle applicazioni gestite. Se si utilizzano criteri obsoleti, crearne di nuovi per le versioni delle applicazioni supportate da Kaspersky Security Center Cloud Console.
- Per utilizzare criteri validi, eseguire l'upgrade dei plug-in Web per le applicazioni che si intende gestire tramite Kaspersky Security Center Cloud Console.
- Disinstallare le applicazioni Kaspersky dai dispositivi gestiti se queste applicazioni non sono supportate da Kaspersky Security Center Cloud Console, quindi sostituire le applicazioni disinstallate con quelle supportate.
- Decriptare tutti i dati (a livello di disco o di file) criptati da Kaspersky Endpoint Security for Windows nei dispositivi gestiti che eseguono il sistema operativo Windows, quindi disabilitare la funzionalità di criptaggio nei dispositivi gestiti tramite i criteri dell'applicazione o in locale. Per ulteriori informazioni, vedere la Guida relativa a Kaspersky Endpoint Security for Windows.

  Se in un dispositivo Windows sono ancora archiviati file o cartelle criptati tramite Kaspersky Endpoint Security for Windows, l'upgrade di Network Agent verrà annullato durante il processo di migrazione. Una notifica richiederà di decriptare tutti i dati nel dispositivo e disabilitare la funzionalità di criptaggio.

Kaspersky Security Center Cloud Console consente un massimo di 25.000 dispositivi gestiti per un Administration Server.

Per eseguire una migrazione a Kaspersky Security Center Cloud Console:

1. Stimare l'ambito del processo di migrazione, quindi esaminare il gruppo di amministrazione da esportare e valutare il numero di dispositivi gestiti che contiene. Assicurarsi che tutte le attività elencate come prerequisiti per la migrazione siano state completate correttamente.
2. In Kaspersky Security Center Cloud Console passare all'Administration Server secondario per i dispositivi gestiti di cui si desidera eseguire la migrazione.
3. Nel menu principale, passare a **Operazioni** → **Migrazione**.

   Verrà visualizzata la pagina iniziale della Migrazione guidata.
4. Nella pagina di benvenuto fare clic su **Avanti**.

   Verrà visualizzata la pagina **Dispositivi gestiti da esportare**, che mostra l'intera gerarchia dei gruppi di amministrazione dell'Administration Server secondario.
5. Nella pagina **Dispositivi gestiti da esportare** fare clic sull'icona della freccia di espansione (>) accanto al nome del gruppo **Dispositivi gestiti** e espandere la gerarchia dei gruppi di amministrazione. Selezionare il gruppo di amministrazione che si desidera esportare.

La Migrazione guidata controlla il numero totale di dispositivi gestiti inclusi nel gruppo di amministrazione selezionato. Se questo numero è superiore a 10.000 viene visualizzato un messaggio di errore. Il pulsante **Avanti** resta non disponibile (in grigio) finché il numero di dispositivi gestiti nel gruppo di amministrazione selezionato non rientra nel limite.

6. Selezionare le applicazioni gestite per cui i criteri e le attività devono essere trasferiti in Kaspersky Security Center Cloud Console insieme agli oggetti del gruppo. Per selezionare le applicazioni gestite di cui devono essere esportati gli oggetti, selezionare le caselle di controllo accanto ai relativi nomi nell'elenco.

   Sebbene Kaspersky Security Center Administration Server sia presente nell'elenco, la selezione della casella di controllo corrispondente non comporta l'esportazione dei relativi criteri.

   Per assicurarsi che le applicazioni gestite siano supportate da Kaspersky Security Center Cloud Console, fare clic sul collegamento corrispondente. Si verrà reindirizzati all'argomento della Guida in linea contenente l'elenco delle applicazioni gestite da Kaspersky Security Center Cloud Console.

   Se vengono selezionate applicazioni che non sono supportate da Kaspersky Security Center Cloud Console, i criteri e le attività di queste applicazioni verranno comunque migrati, ma non sarà possibile gestirli in Kaspersky Security Center Cloud Console a causa della mancata disponibilità dei plug-in dedicati.

7. Visualizzare l'elenco degli oggetti di gruppo esportati per impostazione predefinita. È inoltre possibile specificare oggetti non di gruppo da esportare insieme al gruppo di amministrazione selezionato, se necessario: attività globali, selezioni dispositivi personalizzate, rapporti, ruoli personalizzati, utenti interni e gruppi di protezione e categorie di applicazioni personalizzate con contenuti aggiunti manualmente. Questa pagina include le seguenti sezioni:

   - **Attività globali**

     L'elenco delle attività globali delle applicazioni gestite, nonché delle attività globali di Network Agent.

     Se un'attività globale selezionata è applicabile a una selezione di oggetti specifici, anche questa selezione verrà esportata.

     Sebbene le attività globali di Administration Server siano presenti nell'elenco, non è possibile esportarle; la selezione di tali attività non influisce sull'ambito di esportazione. Anche le attività di installazione remota rimangono al di fuori dell'ambito di esportazione, poiché i rispettivi pacchetti di installazione non possono essere esportati.

   - **Selezioni dispositivi**

     L'elenco delle selezioni dispositivi personalizzate.

   - **Rapporti**

L'elenco modificabile delle istanze dei rapporti da esportare.

Se un rapporto selezionato è applicabile a una selezione di oggetti specifici, anche questa selezione verrà esportata.

Kaspersky Security Center Cloud Console contiene lo stesso set di modelli di rapporto di Kaspersky Security Center Web Console, quindi è possibile selezionare per l'esportazione solo i rapporti creati manualmente o riconfigurati.

- **Oggetti del gruppo**

L'elenco degli oggetti di gruppo da esportare per impostazione predefinita. I seguenti oggetti correlati al gruppo di amministrazione selezionato verranno esportati completamente per impostazione predefinita:

- Struttura del gruppo di amministrazione, ovvero tutti i sottogruppi del gruppo di amministrazione selezionato
- Dispositivi inclusi nei gruppi di amministrazione da esportare
- Tag assegnati ai dispositivi da esportare

  Se un tag è stato creato in Kaspersky Security Center Web Console ma non è mai stato assegnato ad alcun dispositivo, non verrà esportato. Nemmeno le regole di tagging automatico verranno esportate.

- Criteri di gruppo delle applicazioni gestite selezionate

  I criteri di Administration Server e i criteri di Network Agent non vengono esportati.

- Attività di gruppo delle applicazioni gestite che sono state selezionate e attività di gruppo di Network Agent

  Le attività di Administration Server non vengono esportate.

È anche possibile impedire l'esportazione di alcuni tipi di oggetti non di gruppo:

- Per annullare l'esportazione dei ruoli personalizzati (ovvero quelli creati solo dall'utente), selezionare la casella di controllo **Escludi i ruoli personalizzati dall'esportazione**.
- Per annullare l'esportazione di utenti interni e gruppi di sicurezza, selezionare la casella di controllo **Escludi gli utenti interni e i gruppi di protezione dall'esportazione**.
- Per annullare l'esportazione delle categorie di applicazioni personalizzate con il contenuto aggiunto manualmente, selezionare la casella di controllo **Escludi le categorie di applicazioni personalizzate dall'esportazione**.

Se si trasferiscono dispositivi di vari sistemi operativi a Kaspersky Security Center Cloud Console, la migrazione degli oggetti non di gruppo deve essere eseguita una sola volta.

8. Dopo aver definito l'ambito della migrazione, fare clic su **Avanti** per avviare il processo di esportazione. Verrà visualizzata la pagina **Creazione del file di esportazione**, in cui è possibile visualizzare lo stato di avanzamento dell'esportazione per ciascun tipo di oggetto incluso nell'ambito della migrazione. Attendere che ciascuna icona di aggiornamento (🔄) accanto a ogni elemento nell'elenco di oggetti venga sostituita con un segno di spunta verde (✓). L'esportazione viene completata e il file di esportazione viene automaticamente salvato in una cartella temporanea. Viene aperta la pagina successiva, che mostra l'intera gerarchia dei gruppi di amministrazione in Kaspersky Security Center Cloud Console, che funge da Administration Server primario.

9. Selezionare la casella di controllo accanto al gruppo di amministrazione in cui devono essere importati gli oggetti del gruppo, quindi fare clic su **Avanti**. Il file è decompresso, e gli oggetti non di gruppo e gli oggetti di gruppo vengono ripristinati nel gruppo di amministrazione di destinazione.

   Se il nome dell'oggetto ripristinato è identico al nome di un oggetto esistente, all'oggetto ripristinato viene aggiunto un suffisso incrementale.

   Al termine dell'importazione, la struttura esportata dei gruppi di amministrazione, inclusi i dettagli dei dispositivi, viene visualizzata sotto il gruppo di amministrazione di destinazione selezionato. Anche gli oggetti non di gruppo vengono importati.

   Non è possibile ridurre a icona la Migrazione guidata ed eseguire operazioni simultanee durante l'importazione. Attendere che ciascuna icona di aggiornamento (🔄) accanto a ogni elemento nell'elenco di oggetti venga sostituita con un segno di spunta verde (✓) e che l'importazione venga completata. Successivamente, i dispositivi iniziano il passaggio a Kaspersky Security Center Cloud Console.

10. Al termine dell'importazione, la Migrazione guidata visualizza un elenco di pacchetti di installazione di Network Agent disponibili in Kaspersky Security Center Cloud Console per un sistema operativo appropriato. Selezionare il pacchetto di installazione contenente la versione e la localizzazione appropriate di Network Agent.

    Selezionare il pacchetto di installazione di Kaspersky Network Agent per Windows solo se in precedenza è stato completato l'avvio rapido guidato nell'area di lavoro di Kaspersky Security Center Cloud Console e se si esegue la migrazione dei dispositivi Windows.

11. Fare clic su **Avanti**.

    La Migrazione guidata crea un nuovo pacchetto di installazione indipendente (o ne utilizza uno esistente) e un pacchetto di installazione personalizzato basato su di esso, nonché l'attività di installazione remota corrispondente. L'ambito dell'attività include il gruppo di amministrazione selezionato nella pagina **Dispositivi gestiti da esportare**. La pianificazione di avvio dell'attività è impostata su **Manualmente** per impostazione predefinita. La Migrazione guidata visualizza lo stato di avanzamento della creazione.

12. Attendere che ciascuna icona di aggiornamento (🔄) venga sostituita con un segno di spunta verde (✓), quindi fare clic su **Avanti**.

13. Se necessario, selezionare la casella di controllo **Esegui l'attività di installazione remota appena creata** (deselezionata per impostazione predefinita) per i dispositivi nel gruppo di amministrazione selezionato in Kaspersky Security Center Web Console in esecuzione in locale e tutti i relativi sottogruppi. Al termine dell'installazione di Network Agent, è possibile gestire i dispositivi selezionati tramite Kaspersky Security Center Cloud Console. Viene visualizzato il percorso completo del gruppo di amministrazione in cui verrà eseguita l'attività.

L'attività di installazione remota deve essere avviata solo al termine dell'importazione in Kaspersky Security Center Cloud Console. In caso contrario, i dispositivi potrebbero essere duplicati.

14. Fare clic su **Fine** per chiudere la Migrazione guidata e avviare l'attività di installazione remota per i seguenti scopi:

    - Upgrade delle istanze di Network Agent
    - Gestione delle istanze di Network Agent tramite Kaspersky Security Center Cloud Console

    Se la casella di controllo **Esegui attività di installazione remota** è stata mantenuta deselezionata, è possibile avviare manualmente l'attività in un secondo momento, se necessario.

È possibile verificare di poter gestire le istanze di Network Agent di cui è stata eseguita la migrazione tramite Kaspersky Security Center Cloud Console. A tale scopo, accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**. Assicurarsi che i dispositivi gestiti di cui è stata eseguita la migrazione abbiano l'icona di conferma (✓) nelle colonne **Visibile**, **Network Agent installato** e **Network Agent è in esecuzione**. Assicurarsi inoltre che questi dispositivi non dispongano della descrizione dello stato *Connessione non eseguita da molto tempo*.

Scenario: Migrazione di dispositivi che eseguono sistemi operativi Linux o macOS

Questa sezione descrive come eseguire la migrazione dei dispositivi che eseguono sistemi operativi Linux o macOS da Kaspersky Security Center Web Console in esecuzione in locale a Kaspersky Security Center Cloud Console. Gli scenari di base di migrazione senza una gerarchia di Administration Server e migrazione con tale gerarchia consentono il trasferimento di tutti i dispositivi e degli oggetti correlati a Kaspersky Security Center Cloud Console. Tuttavia, se la rete include dispositivi che eseguono non solo Windows, ma anche Linux o macOS, è necessario trasferire separatamente i dispositivi di ciascun tipo di sistema operativo. Di conseguenza, è necessario eseguire più volte la migrazione.

Prerequisiti

Prima di iniziare, procedere come segue:

- Eseguire l'upgrade dell'Administration Server in esecuzione in locale alla versione 12 Patch A o successiva.
- Installare Kaspersky Security Center Web Console versione 12.1 o successiva.
- Eseguire l'upgrade di Network Agent nei dispositivi gestiti alla versione 12 o successiva.
- Eseguire l'upgrade delle applicazioni gestite alle versioni supportate da Kaspersky Security Center Cloud Console.
- Assicurarsi di disporre dei criteri per le versioni più recenti delle applicazioni gestite. Se si utilizzano criteri obsoleti, crearne di nuovi per le versioni delle applicazioni supportate da Kaspersky Security Center Cloud Console.
- Per utilizzare criteri validi, eseguire l'upgrade dei plug-in Web per le applicazioni che si intende gestire tramite Kaspersky Security Center Cloud Console.

- Disinstallare le applicazioni Kaspersky dai dispositivi gestiti se queste applicazioni non sono supportate da Kaspersky Security Center Cloud Console, quindi sostituire le applicazioni disinstallate con quelle supportate.

Kaspersky Security Center Cloud Console consente un massimo di 25.000 dispositivi gestiti per un Administration Server.

Fasi della migrazione

La migrazione a Kaspersky Security Center Cloud Console comprende le seguenti fasi:

1. **Raggruppamento dei dispositivi gestiti in base ai relativi sistemi operativi**

   Se la rete include dispositivi che eseguono diversi sistemi operativi (Windows, Linux o macOS), posizionare i dispositivi di ciascun sistema operativo in gruppi di amministrazione separati in Kaspersky Security Center Web Console. Creare inoltre un gruppo di amministrazione per ogni distribuzione Linux. Se ad esempio si dispone di dispositivi Debian e Red Hat Linux, allocarli in diversi gruppi di amministrazione. In questo modo sarà possibile eseguire correttamente la migrazione poiché sono necessari diversi pacchetti di installazione di Network Agent per vari sistemi operativi.

2. **Eseguire separatamente la migrazione di ogni gruppo di amministrazione e dei relativi oggetti dell'applicazione**

   La migrazione dei dispositivi gestiti di ciascun sistema operativo deve avvenire separatamente, per includere i relativi criteri e attività. Se ad esempio si dispone di dispositivi Windows, macOS, Ubuntu e CentOS, trasferire prima i dispositivi che eseguono il sistema operativo Windows in Kaspersky Security Center Cloud Console, quindi i dispositivi macOS, poi Ubuntu e infine CentOS. È possibile trasferire i dispositivi gestiti in qualsiasi ordine.

   A tale scopo, eseguire la migrazione senza la gerarchia di Administration Server o la migrazione con tale gerarchia, a seconda che la rete includa Administration Server secondari o meno. Durante la migrazione, utilizzare il pacchetto di installazione di Network Agent corrispondente al sistema operativo dei dispositivi trasferiti. Selezionare ad esempio Kaspersky Security Center 13.2 Network Agent per dispositivi Linux per eseguire correttamente la migrazione.

   Tenere presente che per gli oggetti non di gruppo, come le attività globali, le selezioni dispositivi personalizzate o i rapporti, la migrazione deve essere eseguita una sola volta.

Risultati

Al termine della migrazione, è possibile verificare che il processo abbia avuto esito positivo:

- La versione corretta di Network Agent viene reinstallata in ogni dispositivo gestito che esegue il sistema operativo Linux o macOS.
- Tutti i dispositivi Linux o macOS sono gestiti tramite Kaspersky Security Center Cloud Console.
- Tutte le impostazioni degli oggetti applicate prima della migrazione sono state mantenute.

Scenario: Migrazione inversa da Kaspersky Security Center Cloud Console a Kaspersky Security Center

Potrebbe essere utile eseguire la migrazione dei dispositivi gestiti da Kaspersky Security Center Cloud Console a Kaspersky Security Center Administration Server. Questo processo può ad esempio essere utilizzato per eseguire il rollback della migrazione a Kaspersky Security Center Cloud Console.

Prerequisiti

Prima di iniziare, assicurarsi che vengano soddisfatti i seguenti prerequisiti:

- Kaspersky Security Center Cloud Console è disponibile e sono connessi dispositivi gestiti.
- Kaspersky Security Center 14.2 (o versione successiva) Administration Server è disponibile e include un pacchetto di installazione di Network Agent versione 13 o successiva.

Fasi della migrazione inversa

La migrazione inversa prevede i seguenti passaggi:

1. **Creazione di un pacchetto di installazione indipendente di Network Agent in Kaspersky Security Center Administration Server in locale**

   In Kaspersky Security Center Administration Server in esecuzione in locale creare un pacchetto di installazione indipendente di Network Agent.

   Durante il processo di creazione è possibile selezionare l'opzione **Sposta i dispositivi non assegnati in questo gruppo** per specificare un gruppo di amministrazione in cui si desidera spostare i Network Agent dopo l'installazione. Se è stato specificato il gruppo di amministrazione, viene creata una regola di spostamento automatico che sposterà nel gruppo di amministrazione di destinazione tutti i Network Agent installati con questo pacchetto di installazione indipendente.

   > Per garantire la corretta migrazione inversa, assicurarsi di selezionare la versione di Network Agent, uguale o successiva alla versione utilizzata in Kaspersky Security Center Cloud Console.

2. **Creazione di un pacchetto di installazione personalizzato in Kaspersky Security Center Cloud Console**

   In Kaspersky Security Center Cloud Console creare un pacchetto di installazione personalizzato basato sul pacchetto di installazione indipendente creato e salvato da Kaspersky Security Center Administration Server in esecuzione in locale.

   Per abilitare l'installazione del pacchetto in modalità automatica, nel campo **Riga di comando file eseguibile** specificare la chiave `-s`.

3. **Creazione di un'attività di installazione remota**

   In Kaspersky Security Center Cloud Console creare un'attività di installazione remota utilizzando il pacchetto di installazione personalizzato creato.

4. **Esecuzione dell'attività di installazione remota**

   Avviare l'attività di installazione remota creata. L'attività avvia la reinstallazione di tutti i Network Agent nel gruppo di amministrazione specificato; e inserisce inoltre i Network Agent nell'ambito della gestione di Kaspersky Security Center Administration Server in esecuzione in locale modificando l'indirizzo di connessione e modificando altre impostazioni di connessione.

   > Se durante la creazione del pacchetto di installazione indipendente non è stato specificato alcun gruppo di amministrazione di destinazione, tutti i dispositivi vengono spostati nel gruppo **Dispositivi non assegnati**.

Risultati

Al termine della migrazione, è possibile verificare che il processo abbia avuto esito positivo:

- Tutti i dispositivi nell'ambito dell'attività di installazione remota precedentemente gestiti tramite Kaspersky Security Center Cloud Console adesso vengono gestiti da Kaspersky Security Center Administration Server in esecuzione in locale.
- I dispositivi vengono automaticamente spostati nel gruppo di amministrazione specificato nelle impostazioni del pacchetto di installazione.

Non è possibile completare l'attività di installazione remota in Kaspersky Security Center Cloud Console: non sono più disponibili dispositivi di destinazione poiché tutte le relative impostazioni di connessione sono state modificate. È necessario arrestare l'attività manualmente dopo aver verificato che l'icona dell'errore (!) sia visualizzata nella colonna **Visibile** dell'elenco Dispositivi gestiti per tutti i dispositivi dell'ambito della migrazione.

Migrazione con Administration Server virtuali

Se si dispone di Administration Server virtuali nell'infrastruttura locale Kaspersky Security Center esistente, non è possibile eseguire la migrazione da Kaspersky Security Center locale a Kaspersky Security Center Cloud Console utilizzando la Migrazione guidata. Sarà inoltre possibile eseguire la migrazione solo dei dispositivi dei clienti. Sarà necessario creare manualmente criteri, attività e rapporti.

È possibile eseguire uno dei seguenti scenari di migrazione:

- Spostamento dei dispositivi dei clienti dagli Administration Server virtuali a un Administration Server primario
- Esecuzione della migrazione manuale dagli Administration Server virtuali

Scenario: Migrazione con Administration Server virtuali tramite lo spostamento dei dispositivi

Per eseguire la migrazione da Kaspersky Security Center Web Console in esecuzione in locale a Kaspersky Security Center Cloud Console, è possibile spostare i dispositivi da Administration Server virtuali a un Administration Server primario.

Prerequisiti

Prima della migrazione, è necessario eseguire una serie di azioni, tra cui l'upgrade di Administration Server in esecuzione in locale alla versione 12 o successiva e l'upgrade delle applicazioni gestite alle versioni supportate da Kaspersky Security Center Cloud Console.

Scenario di migrazione

Lo scenario procede per fasi:

1. **Creazione di un gruppo di amministrazione per ogni Administration Server virtuale**

L'utente crea il gruppo in Kaspersky Security Center in esecuzione in locale.

2. **Spostamento dei dispositivi dei clienti**

   In Kaspersky Security Center in esecuzione in locale spostare i dispositivi dei clienti da ciascun Administration Server virtuale al rispettivo gruppo di amministrazione creato nel passaggio precedente.

3. **Migrazione**

   Eseguire la migrazione come descritto per la rete senza una gerarchia di Administration Server.

4. **Spostamento dei dispositivi nell'ambito della gestione di Administration Server virtuali (passaggio facoltativo)**

   Se si desidera gestire i clienti tramite Administration Server virtuali, spostare i dispositivi dai gruppi di amministrazione nell'ambito della gestione di Administration Server virtuali.

5. **Creazione di criteri, attività e rapporti**

   Creare criteri, attività e rapporti come richiesto.

Risultati

Al termine della migrazione, è possibile verificare che il processo abbia avuto esito positivo:

- Network Agent è stato reinstallato in tutti i dispositivi gestiti.
- Tutti i dispositivi sono gestiti tramite Kaspersky Security Center Cloud Console.
- Tutte le impostazioni degli oggetti applicate prima della migrazione sono state mantenute.

Scenario: Migrazione manuale con Administration Server virtuali

È possibile eseguire manualmente la migrazione da Kaspersky Security Center Web Console in esecuzione in locale a Kaspersky Security Center Cloud Console.

Prerequisiti

Prima della migrazione, è necessario eseguire una serie di azioni, tra cui l'upgrade di Administration Server in esecuzione in locale alla versione 12 o successiva e l'upgrade delle applicazioni gestite alle versioni supportate da Kaspersky Security Center Cloud Console.

Scenario di migrazione

Lo scenario procede per fasi:

1. **Creazione di un gruppo di amministrazione per ogni Administration Server virtuale**

   In Kaspersky Security Center Cloud Console creare un gruppo di amministrazione corrispondente a ciascuno degli Administration Server virtuali.

2. **Creazione di un pacchetto di installazione indipendente per Network Agent**

Creare un pacchetto di installazione indipendente per Network Agent. Durante la creazione specificare il gruppo di amministrazione creato nel passaggio precedente. Questo significa che è necessario creare un singolo pacchetto di installazione indipendente per ciascun gruppo di amministrazione.

Questo passaggio avviene in Kaspersky Security Center Cloud Console.

3. **Download dei pacchetti di installazione indipendenti**

   Scaricare i pacchetti di installazione indipendenti creati nel passaggio precedente. Questo passaggio avviene in Kaspersky Security Center Cloud Console.

4. **Creazione di un archivio con ciascun pacchetto di installazione indipendente**

   I tipi di archivio disponibili sono: ZIP, CAB, TAR o TAR.GZ.

5. **Creazione di pacchetti di installazione personalizzati per Network Agent**

   Creare pacchetti di installazione personalizzati per Network Agent. Durante la creazione, utilizzare gli archivi creati nel passaggio precedente.

   Questo passaggio avviene in Kaspersky Security Center in esecuzione in locale.

6. **Creazione di attività di installazione remota**

   Creare attività di installazione remota per installare Network Agent dai pacchetti di installazione personalizzati creati.

   Quando si crea un'attività, specificare un gruppo di amministrazione corrispondente.

   Questo passaggio avviene in Kaspersky Security Center in esecuzione in locale.

7. **Esecuzione delle attività di installazione remota create**

   I Network Agent vengono aggiornati. L'Administration Server di Kaspersky Security Center Cloud Console si occupa della relativa gestione.

   Viene eseguita la migrazione di tutti i dispositivi in Kaspersky Security Center Cloud Console e questi vengono inseriti in gruppi di amministrazione specificati durante la creazione dei pacchetti di installazione indipendenti per Network Agent.

8. **Spostamento dei dispositivi nell'ambito della gestione di Administration Server virtuali (passaggio facoltativo)**

   Se si desidera gestire i clienti tramite Administration Server virtuali, spostare i dispositivi dai gruppi di amministrazione nell'ambito della gestione di Administration Server virtuali.

9. **Creazione di criteri, attività e rapporti**

   Creare criteri, attività e rapporti come richiesto.

Risultati

Al termine della migrazione, è possibile verificare che il processo abbia avuto esito positivo:

- Network Agent è stato reinstallato in tutti i dispositivi gestiti.
- Tutti i dispositivi sono gestiti tramite Kaspersky Security Center Cloud Console.

  Tutte le impostazioni degli oggetti applicate prima della migrazione sono state mantenute.

Scenario: Spostamento dei dispositivi da gruppi di amministrazione gestiti da server virtuali

Potrebbe essere necessario gestire i clienti tramite Administration Server virtuali. Se è stata eseguita la migrazione dei dispositivi e di altri elementi da Kaspersky Security Center in locale a Kaspersky Security Center Cloud Console, i dispositivi si trovano nei gruppi di amministrazione. Per gestire i dispositivi dei clienti tramite Administration Server virtuali, è necessario spostare i dispositivi dai gruppi di amministrazione all'ambito di gestione degli Administration Server virtuali.

Prerequisiti

È stato creato un Administration Server virtuale per ciascun cliente.

Tutti i dispositivi di ciascun cliente si trovano in un singolo gruppo di amministrazione.

Passaggi

Lo scenario procede per fasi:

1. **Creazione di un pacchetto di installazione indipendente per Network Agent**

   Passare a ciascun Administration Server virtuale creato, quindi creare un pacchetto di installazione indipendente per Network Agent. È possibile passare da un Administration Server all'altro nel menu principale facendo clic sull'icona della freccia di espansione () a destra del nome dell'Administration Server corrente, per poi selezionare l'Administration Server desiderato.

2. **Download dei pacchetti di installazione indipendenti**

   Scaricare i pacchetti di installazione indipendenti creati nel passaggio precedente.

3. **Creare un archivio con ciascun pacchetto di installazione indipendente**

   I tipi di archivio disponibili sono: ZIP, CAB, TAR o TAR.GZ.

4. **Creazione di pacchetti di installazione personalizzati per Network Agent**

   Creare pacchetti di installazione personalizzati per Network Agent. Durante la creazione, utilizzare gli archivi creati nel passaggio precedente.

   Questo passaggio avviene nell'Administration Server primario.

5. **Creazione di attività di installazione remota**

   Creare attività di installazione remota per installare Network Agent dai pacchetti di installazione personalizzati creati.

   Quando si crea un'attività, specificare un gruppo di amministrazione corrispondente.

   Questo passaggio avviene nell'Administration Server primario.

6. **Eseguire le attività di installazione remota create**

   I Network Agent vengono aggiornati. I dispositivi vengono spostati all'ambito di gestione degli Administration Server virtuali.

7. **Creazione di criteri, attività e rapporti**

Creare criteri, attività e rapporti come richiesto.

Risultati

Adesso è possibile gestire i dispositivi dei clienti di cui è stata eseguita la migrazione utilizzando Administration Server virtuali.

Avvio rapido guidato

Questa sezione fornisce sull'Avvio rapido guidato di Kaspersky Security Center Cloud Console.

Informazioni sull'avvio rapido guidato

L'avvio rapido guidato in Kaspersky Security Center Cloud Console consente di creare una quantità minima di attività e criteri necessari, regolare una quantità minima di impostazioni e iniziare a creare i pacchetti di installazione delle applicazioni Kaspersky. Utilizzando la procedura guidata, è possibile apportare le seguenti modifiche a Kaspersky Security Center Cloud Console:

- Avviare il download dei pacchetti di installazione per le applicazioni Kaspersky gestite.
- Creare un pacchetto di installazione indipendente di Network Agent per i dispositivi che eseguono Windows, Linux o macOS.
- Creare il criterio di Kaspersky Security Center Network Agent.
- Creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.
- Creare criteri e attività per le applicazioni Kaspersky gestite.
- Configurare l'interazione con Kaspersky Security Network (KSN).

Al termine dell'Avvio rapido guidato, vengono visualizzati i pacchetti di installazione per Network Agent e le applicazioni Kaspersky gestite nell'elenco **Individuazione e distribuzione → Distribuzione e assegnazione → Pacchetti di installazione**.

L'avvio rapido guidato crea criteri per le applicazioni gestite, come Kaspersky Endpoint Security for Windows, a meno che tali criteri non siano stati creati per il gruppo Dispositivi gestiti. L'avvio rapido guidato crea attività se non esistono attività con gli stessi nomi per il gruppo Dispositivi gestiti.

Kaspersky Security Center Cloud Console richiede automaticamente di eseguire l'avvio rapido guidato dopo aver creato un'area di lavoro aziendale e avviato Kaspersky Security Center Cloud Console per la prima volta. È anche possibile avviare manualmente l'avvio rapido guidato in qualsiasi momento.

Esecuzione dell'avvio rapido guidato

Kaspersky Security Center Cloud Console richiede automaticamente di eseguire l'avvio rapido guidato dopo aver creato un'area di lavoro aziendale e avviato Kaspersky Security Center Cloud Console per la prima volta. È anche possibile avviare manualmente l'avvio rapido guidato in qualsiasi momento.

Se si avvia nuovamente l'avvio rapido guidato, non è possibile creare nuovamente attività e criteri creati nell'esecuzione precedente della procedura guidata.

Per avviare manualmente l'avvio rapido guidato:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome di Administration Server.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Generale**.

3. Fare clic su **Esegui l'Avvio rapido guidato**.

   In alternativa, è possibile avviare l'Avvio rapido guidato selezionando **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Avvio rapido guidato**.

La procedura guidata richiede di eseguire la configurazione iniziale di Kaspersky Security Center Cloud Console. Seguire le istruzioni della procedura guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**. Utilizzare il pulsante **Indietro** per tornare al passaggio precedente della procedura guidata.

Passaggio 1. Selezione dei pacchetti di installazione da scaricare

Nell'elenco selezionare le applicazioni Kaspersky da installare sui dispositivi client. Kaspersky Security Center Cloud Console creerà pacchetti di installazione per le applicazioni selezionate. Successivamente verranno utilizzati i pacchetti di installazione creati per installare le applicazioni.

Quando si seleziona un pacchetto di installazione da scaricare, prestare attenzione alla lingua: i pacchetti di installazione sono disponibili in diverse lingue.

Selezionare le seguenti applicazioni:

- Kaspersky Security Center Network Agent

  Durante la selezione dei pacchetti di installazione di Network Agent, tenere in considerazione i seguenti aspetti:

  - Network Agent deve essere installato in ogni dispositivo client. Selezionare quindi un Network Agent adeguato per ciascun sistema operativo in esecuzione nei dispositivi client.

  - Network Agent deve essere installato manualmente tramite un pacchetto di installazione indipendente in un dispositivo selezionato per fungere da punto di distribuzione. I punti di distribuzione devono eseguire il polling della rete e l'installazione remota delle applicazioni di protezione Kaspersky nei dispositivi client. È quindi necessario selezionare almeno un pacchetto di installazione di Network Agent. Mentre si procede con i passaggi successivi della procedura guidata, Kaspersky Security Center Cloud Console crea il pacchetto di installazione indipendente di Network Agent.

    Rispetto ai punti di distribuzione basati su Windows, i punti di distribuzione basati su Linux e macOS hanno funzionalità limitate. È consigliabile selezionare i computer basati su Windows che fungeranno da punti di distribuzione.

    È possibile selezionare Network Agent per Windows, Linux e macOS. Se si seleziona Network Agent solo per un sistema operativo, ad esempio macOS, verrà creato un pacchetto di installazione indipendente per il sistema operativo selezionato. Se si seleziona Network Agent per diversi sistemi operativi, Kaspersky Security Center Cloud Console crea un solo pacchetto di installazione indipendente in base alle seguenti priorità: Windows ha la massima priorità, a seguire Linux e infine macOS. Se ad esempio si selezionano Network Agent per Linux e macOS, Kaspersky Security Center Cloud Console crea un pacchetto di installazione indipendente per Network Agent per Linux. È possibile creare manualmente un pacchetto di installazione indipendente di Network Agent per uno di questi sistemi operativi in qualsiasi momento.

- Applicazioni di protezione Kaspersky

  Selezionare i pacchetti di installazione appropriati ai sistemi operativi installati nei dispositivi client dell'organizzazione.

Passaggio 2. Configurazione di un server proxy

Se l'organizzazione utilizza un server proxy per connettersi a Internet, è necessario specificare le impostazioni del server proxy in questo passaggio della procedura guidata. Queste impostazioni vengono aggiunte al pacchetto di installazione di Network Agent. Dopo l'installazione, Network Agent utilizza automaticamente queste impostazioni in ciascun dispositivo client.

Specificare le seguenti impostazioni per la connessione al server proxy:

- **Usa server proxy**
- **Indirizzo**
- **Numero di porta**
- **Autenticazione server proxy**

  Se questa opzione è abilitata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Nome utente**

  Nome utente dell'account con cui viene stabilita la connessione al server proxy.

  È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

- **Password**

  Password dell'account con cui viene stabilita la connessione al server proxy.

  È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

Passaggio 3. Configurazione di Kaspersky Security Network

Se durante il primo passaggio della procedura guidata è stato scaricato il pacchetto di installazione di Kaspersky Endpoint Security for Windows, viene visualizzato il testo dell'Informativa KSN per le seguenti applicazioni:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security Center installato nei dispositivi locali
- Kaspersky Security Center Cloud Console installato nell'ambiente cloud

Se non è stato scaricato il pacchetto di installazione di Kaspersky Endpoint Security for Windows, l'Informativa KSN per questa applicazione non viene visualizzata.

In modalità di prova viene visualizzata solo l'Informativa KSN per Kaspersky Endpoint Security for Windows.

Leggere attentamente l'Informativa di Kaspersky Security Network. Selezionare una delle seguenti opzioni:

- **Accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center Cloud Console e le applicazioni gestite installate nei dispositivi client trasferiranno automaticamente i dettagli sull'esecuzione a Kaspersky Security Network. La partecipazione a Kaspersky Security Network garantisce aggiornamenti più rapidi dei database contenenti le informazioni sui virus e sulle altre minacce, assicurando una risposta più rapida alle minacce per la sicurezza emergenti.

- **Non accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center Cloud Console e le applicazioni gestite non forniranno informazioni a Kaspersky Security Network.

  Se si seleziona questa opzione, l'utilizzo di Kaspersky Security Network sarà disabilitato.

Per impostazione predefinita, l'utilizzo di KSN è disabilitato. Se successivamente si cambia idea sull'utilizzo di KSN, è possibile abilitare (o disabilitare) l'opzione corrispondente nella finestra delle proprietà di Administration Server, nella sezione **Impostazioni KSN**.

Passaggio 4. Configurazione della gestione degli aggiornamenti di terze parti

Questo passaggio non viene visualizzato se l'attività *Trova vulnerabilità e aggiornamenti richiesti* esiste già.

Se si desidera ottenere un elenco di aggiornamenti per le applicazioni installate nei dispositivi gestiti e un elenco di vulnerabilità rilevate e correzioni consigliate per tali applicazioni, abilitare l'opzione **Cerca aggiornamenti e correzioni vulnerabilità per il software di terze parti**. Se questa opzione è abilitata, Kaspersky Security Center Cloud Console crea l'attività *Trova vulnerabilità e aggiornamenti richiesti*.

Passaggio 5. Creazione di una configurazione della protezione di rete di base

In questo passaggio della procedura guidata fare clic sul pulsante **Crea** per creare gli oggetti necessari per la protezione iniziale dei dispositivi client.

Kaspersky Security Center Cloud Console esegue due operazioni:

- Creazione di criteri e attività di base con impostazioni predefinite

  Vengono creati i seguenti criteri:

  - Criterio per Kaspersky Security Center Network Agent
  - Criteri per le applicazioni Kaspersky gestite

  Vengono create le seguenti attività:

  - L'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*
  - Attività *Trova vulnerabilità e aggiornamenti richiesti*

Questa attività viene creata solo se è stata abilitata l'opzione **Cerca aggiornamenti e correzioni vulnerabilità per il software di terze parti** nel passaggio precedente della procedura guidata.

- Attività per le applicazioni Kaspersky gestite

- Creazione di un pacchetto di installazione indipendente per Network Agent

  Questo pacchetto verrà utilizzato per installare Network Agent nei punti di distribuzione. Kaspersky Security Center Cloud Console crea il pacchetto di installazione indipendente in base al pacchetto di installazione di Network Agent selezionato nel passaggio precedente della procedura guidata. Durante la creazione del pacchetto, è necessario leggere e accettare i termini del Contratto di licenza con l'utente finale per Network Agent. Quando viene creato il pacchetto di installazione indipendente, verrà richiesto di scaricarlo nel dispositivo in uso al momento.

  La creazione del pacchetto di installazione indipendente di Network Agent può richiedere tempo. È possibile procedere al passaggio successivo della procedura guidata. Il processo continuerà in background. È possibile tenere traccia del processo nella scheda **In corso ()** della sezione **Pacchetti di installazione** (**Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**).

  Per motivi di autenticazione, ogni pacchetto di installazione indipendente viene firmato utilizzando un certificato. Il certificato viene riemesso periodicamente. Dopo ogni procedura di riemissione del certificato, Kaspersky Security Center Cloud Console aggiorna automaticamente le firme di tutti i pacchetti di installazione indipendenti creati. Per i pacchetti di installazione indipendenti scaricati, non è possibile eseguire un aggiornamento automatico delle firme. Pertanto, il certificato scade e potrebbe verificarsi un errore del certificato durante l'installazione di un'applicazione da un pacchetto di installazione indipendente. In questo caso, scaricare nuovamente il pacchetto di installazione indipendente.

Passaggio 6. Chiusura dell'Avvio rapido guidato.

Nella pagina di completamento dell'Avvio rapido guidato leggere informazioni sulle operazioni aggiuntive che è necessario eseguire per distribuire le applicazioni di protezione Kaspersky nei dispositivi client. Seguire i passaggi specificati nello scenario di distribuzione iniziale delle applicazioni Kaspersky.

Distribuzione iniziale delle applicazioni Kaspersky

Questa sezione descrive la distribuzione iniziale delle applicazioni Kaspersky nei dispositivi client dell'organizzazione.

Scenario: distribuzione iniziale delle applicazioni Kaspersky

Questo scenario descrive come installare le applicazioni Kaspersky nei dispositivi client in Kaspersky Security Center Cloud Console. Prima di tutto è necessario distribuire i punti di distribuzione nella rete. Quindi, tramite i punti di distribuzione, è necessario eseguire il polling della rete e rilevare i dispositivi presenti nella rete. Successivamente è possibile distribuire le applicazioni Kaspersky nei dispositivi della rete.

Al termine dello scenario, le applicazioni Kaspersky vengono distribuite nei dispositivi client selezionati nella rete dell'organizzazione. È possibile gestire tutti i dispositivi in cui sono installate applicazioni Kaspersky.

Prerequisiti

Prima di iniziare, assicurarsi che vengano soddisfatti i seguenti prerequisiti:

- L'Avvio rapido guidato è terminato.
- Sono stati creati i pacchetti di installazione di Network Agent e delle applicazioni di protezione.
- L'indirizzo https://aes.s.kaspersky-labs.com/endpoints/ è incluso nelle eccezioni del firewall del dispositivo gestito.
- Si dispone delle informazioni sulle impostazioni Internet per i dispositivi client dell'organizzazione, delle informazioni sul gateway e delle impostazioni del server proxy.

Passaggi

La distribuzione iniziale delle applicazioni Kaspersky prevede diversi passaggi:

1. **Selezione di un dispositivo a cui assegnare il ruolo di punto di distribuzione**

   In Kaspersky Security Center Cloud Console un punto di distribuzione prevede le seguenti finalità:

   - Polling della rete e individuazione dispositivi
   - Installazione remota di Network Agent ne dispositivi client
   - Connessione dei dispositivi client ad Administration Server (quando un punto di distribuzione funge da gateway di connessione)

   Selezionare un dispositivo nella rete dell'organizzazione a cui assegnare il ruolo di punto di distribuzione per un gruppo di amministrazione. Il dispositivo selezionato deve soddisfare i requisiti per il punto di distribuzione. A seconda della quantità di dispositivi client nella rete dell'organizzazione, selezionare il numero corretto di dispositivi che fungeranno da punti di distribuzione.

2. **Creazione di un pacchetto di installazione indipendente per Network Agent**

   Creare un pacchetto di installazione indipendente per Network Agent da installare nel punto di distribuzione.

Se i dispositivi client non dispongono dell'accesso diretto a Internet per connettersi ad Administration Server, nelle impostazioni del pacchetto di installazione di Network Agent configurare le impostazioni del gateway di connessione e del server proxy.

3. **Installazione di Network Agent nel dispositivo selezionato per fungere da punto di distribuzione**

   Distribuire il pacchetto di installazione indipendente per Network Agent al dispositivo selezionato con qualsiasi metodo. È ad esempio possibile copiare il pacchetto di installazione indipendente in un'unità rimovibile (come un'unità flash) o posizionarlo in una cartella condivisa.

   Nella finestra **Proprietà** del file del pacchetto di installazione indipendente verificare che il pacchetto di installazione indipendente per Network Agent sia firmato da Kaspersky.

   Eseguire l'installazione del pacchetto di installazione indipendente per Network Agent nel dispositivo selezionato. Network Agent viene installato in base alle impostazioni del pacchetto di installazione di Network Agent e collegato ad Administration Server. Il dispositivo con Network Agent viene inserito nel gruppo di amministrazione specificato al momento della creazione di un pacchetto di installazione indipendente per Network Agent.

   Se si installa Network Agent utilizzando un pacchetto di installazione indipendente in un dispositivo che esegue Microsoft Windows XP Professional for Embedded Systems a 32 bit, l'installazione non va a buon fine. Per risolvere il problema, installare prima l'aggiornamento KB2868626 per Windows XP dal sito Web Microsoft: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

4. **Assegnazione del ruolo di punto di distribuzione al dispositivo in cui è installato Network Agent**

   Assegnare al dispositivo in cui è installato Network Agent il ruolo di punto di distribuzione.

5. **Configurazione ed esecuzione del polling della rete per il punto di distribuzione**

   Configurare il polling della rete per il punto di distribuzione in cui è installato Network Agent. Eventualmente è possibile configurare il polling della rete nel criterio di Network Agent.

   Al termine del polling della rete in base alla pianificazione, i dispositivi client connessi alla rete dell'organizzazione vengono rilevati e posizionati nel gruppo **Dispositivi non assegnati**.

6. **Creazione di pacchetti di installazione per Network Agent e le applicazioni Kaspersky gestite**

   Se non è stato avviato l'Avvio rapido guidato o è stato ignorato il passaggio di creazione dei pacchetti di installazione, creare pacchetti di installazione per le applicazioni Kaspersky. È necessario creare pacchetti di installazione sia per Network Agent che per le applicazioni Kaspersky gestite appropriate al sistema operativo installato nei dispositivi client della rete dell'organizzazione.

7. **Rimozione di applicazioni di protezione di terze parti**

   Se nei dispositivi client nella rete dell'organizzazione sono installate applicazioni di protezione di terze parti, rimuoverle prima dell'installazione dell'applicazione Kaspersky.

8. **Installazione delle applicazioni Kaspersky nei dispositivi client**

   Creare attività per installare Network Agent e le applicazioni Kaspersky gestite nei dispositivi client nella rete dell'organizzazione. Quando si creano le attività, utilizzare il tipo di attività **Installa l'applicazione in remoto**. Per l'attività di installazione di Network Agent, utilizzare l'opzione **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**. Per l'attività di installazione delle applicazioni Kaspersky gestite, utilizzare l'opzione **Utilizzando Network Agent**. Dopo la creazione delle attività, è possibile configurarne le impostazioni. Assicurarsi che la pianificazione per ciascuna attività soddisfi i requisiti. Prima di tutto è necessario eseguire l'attività di installazione di Network Agent. Quindi, dopo aver installato Network Agent nei dispositivi client, è necessario eseguire l'attività per installare le applicazioni Kaspersky gestite.

   Eventualmente è possibile creare un'attività di installazione remota per installare Network Agent e le applicazioni Kaspersky gestite nei dispositivi client nella rete dell'organizzazione. In questo caso, nella sezione **Pacchetti di installazione** utilizzare l'opzione **Selezionare il pacchetto di installazione** e l'opzione **Selezionare Network Agent**; nella sezione **Forza il download del pacchetto di installazione** utilizzare l'opzione **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**.

È inoltre possibile creare diverse attività di installazione remota per installare le applicazioni Kaspersky gestite per diversi gruppi di amministrazione o diverse selezioni dispositivi.

Se si dispone di dispositivi client esterni alla rete con il punto di distribuzione, ad esempio laptop di utenti remoti, è necessario creare e distribuire il pacchetto di installazione indipendente di Network Agent a tali dispositivi client con qualsiasi metodo. Installare il pacchetto di installazione indipendente di Network Agent in locale in tali dispositivi client. Quindi è possibile installare le applicazioni Kaspersky gestite nei dispositivi degli utenti remoti seguendo le stesse istruzioni valide per gli altri dispositivi rilevati dal punto di distribuzione.

Eseguire le attività di installazione remota.

Eventualmente, per installare le applicazioni Kaspersky è possibile avviare la Distribuzione guidata della protezione.

9. **Installazione di Kaspersky Security for Mobile**

   Se si intende gestire i dispositivi mobili aziendali, seguire le istruzioni fornite nella Guida di Kaspersky Security for Mobile per informazioni sulla distribuzione di Kaspersky Endpoint Security for Android.

10. **Verifica della distribuzione iniziale delle applicazioni Kaspersky**

    Generare e visualizzare il **Rapporto sulle versioni del software Kaspersky**. Assicurarsi che le applicazioni Kaspersky gestite siano installate in tutti i dispositivi client dell'organizzazione.

Per il criptaggio dell'intero disco, Kaspersky Security Center Cloud Console supporta solo BitLocker.

Creazione di pacchetti di installazione per le applicazioni Kaspersky

Per distribuire applicazioni Kaspersky nei dispositivi nella rete dell'organizzazione, è necessario creare pacchetti di installazione delle applicazioni Kaspersky in Kaspersky Security Center Cloud Console.

Per creare un pacchetto di installazione dell'applicazione Kaspersky:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   È anche possibile visualizzare le notifiche relative ai nuovi pacchetti nell'elenco delle notifiche sullo schermo. Se sono presenti notifiche relative a un nuovo pacchetto, è possibile fare clic sul collegamento accanto alla notifica e passare all'elenco dei pacchetti di installazione disponibili.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Fare clic su **Aggiungi**.

   Viene avviata la Creazione guidata nuovo pacchetto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nella prima pagina della procedura guidata selezionare **Crea pacchetto di installazione per un'applicazione Kaspersky**.

   Verrà visualizzato un elenco dei pacchetti di distribuzione disponibili sui server Web di Kaspersky.

4. Fare clic sul nome di un pacchetto di distribuzione, ad esempio **Kaspersky Endpoint Security for Windows (<numero di versione>)**.

Verrà visualizzata una finestra con le informazioni sul pacchetto di distribuzione.

5. Leggere le informazioni e fare clic sul pulsante **Scarica e crea pacchetto di installazione**.

   Se un pacchetto di distribuzione non può essere automaticamente convertito in un pacchetto di installazione, viene visualizzato il pulsante **Scarica pacchetto di distribuzione** anziché il pulsante **Scarica e crea pacchetto di installazione**. In questo caso scaricare il pacchetto di distribuzione, quindi utilizzare il file scaricato per creare un pacchetto di installazione personalizzato.

   Verrà avviato il download del pacchetto di installazione. È possibile chiudere la finestra della procedura guidata o procedere al passaggio successivo della procedura. Se si chiude la finestra della procedura guidata, il processo di download continuerà in background.

   Se si desidera tenere traccia del processo di download di un pacchetto di installazione:

   a. Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione** → **In corso ()**.

   b. Tenere traccia dello stato di avanzamento dell'operazione nella colonna **Stato di avanzamento del download** e nella colonna **Stato del download** della tabella.

   Al termine del processo, il pacchetto di installazione viene aggiunto all'elenco nella scheda **Download eseguito**. Se il processo di download si interrompe e lo stato del download passa a **Accetta Contratto di licenza con l'utente finale**, fare clic sul nome del pacchetto di installazione, quindi procedere al passaggio successivo della procedura.

   Se si prevede di eseguire la migrazione da Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console e le normative di protezione dell'organizzazione richiedono l'utilizzo del proxy durante l'accesso alla rete aziendale, ciò potrebbe influire sul processo di migrazione. Dopo la creazione di un pacchetto di installazione di Network Agent, è necessario specificare le impostazioni del proxy per garantire la connessione tra le istanze di Network Agent nei dispositivi gestiti e l'area di lavoro di Kaspersky Security Center Cloud Console:

   a. Fare clic sul nome del pacchetto di installazione.

   b. Nella finestra delle proprietà del pacchetto di installazione visualizzata accedere alla scheda **Impostazioni**.

   c. Aprire la sezione **Connessione**.

   d. Selezionare l'opzione **Usa server proxy** e compilare i campi **Indirizzo server proxy** e **Porta server proxy**.

6. Per alcune applicazioni Kaspersky, durante il processo di download viene visualizzato il pulsante **Mostra Contratto di licenza con l'utente finale**. Se viene visualizzato, procedere come segue:

   a. Fare clic sul pulsante **Mostra Contratto di licenza con l'utente finale** per leggere il Contratto di licenza con l'utente finale (EULA).

   b. Leggere il Contratto di licenza con l'utente finale visualizzato, quindi fare clic sul pulsante **Accetta**.

      Dopo aver accettato il Contratto di licenza con l'utente finale, il download prosegue. Se si fa clic su **Rifiuta**, il download viene interrotto.

7. Al termine del download, fare clic sul pulsante **Chiudi** (✕) per chiudere la finestra con le informazioni sul pacchetto di distribuzione.

Il pacchetto di installazione è stato creato. Il pacchetto di installazione viene visualizzato nell'elenco dei pacchetti di installazione.

Distribuzione dei pacchetti di installazione agli Administration Server secondari

Per distribuire i pacchetti di installazione agli Administration Server secondari:

1. Stabilire una connessione all'Administration Server che controlla gli Administration Server secondari desiderati.
2. Creare un'attività di distribuzione del pacchetto di installazione negli Administration Server secondari in uno dei seguenti modi:
   - Se si desidera creare un'attività per gli Administration Server secondari del gruppo di amministrazione selezionato, avviare la creazione di un'attività di gruppo.
   - Se si desidera creare un'attività per specifici Administration Server secondari, avviare la creazione di un'attività per dispositivi specifici.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

   Nella finestra **Nuova attività** della Creazione guidata nuova attività, nel campo **Tipo di attività** selezionare **Distribuisci pacchetto di installazione**. È inoltre possibile modificare il nome predefinito dell'attività nel campo **Nome attività**.

   Nel passaggio successivo specificare gli Administration Server secondari per l'ambito dell'attività e seguire le istruzioni della Creazione guidata nuova attività. Al termine verrà creata l'attività per la distribuzione dei pacchetti di installazione selezionati a specifici Administration Server secondario.

   > Quando si crea l'attività Distribuisci pacchetto di installazione per gli Administration Server secondario in esecuzione in locale, l'ambito di distribuzione, oltre ai pacchetti di installazione personalizzati, includerà solo i pacchetti di installazione delle applicazioni Kaspersky supportate da Kaspersky Security Center Web Console in esecuzione in locale, indipendentemente dall'opzione di distribuzione selezionata (**Tutti i pacchetti di installazione** o **Pacchetti di installazione selezionati**).
3. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

I pacchetti di installazione selezionati verranno copiati negli specifici Administration Server secondari.

Creazione di un pacchetto di installazione indipendente per Network Agent

Gli utenti dei dispositivi nell'organizzazione possono utilizzare pacchetti di installazione indipendenti per installare Network Agent nei dispositivi in locale. È possibile creare pacchetti di installazione indipendenti per i dispositivi che eseguono Windows, Linux o macOS.

> In Kaspersky Security Center Cloud Console è possibile creare pacchetti di installazione indipendenti solo per Network Agent.

Un pacchetto di installazione indipendente è un file eseguibile che può essere inviato per e-mail o trasferito in altro modo a un dispositivo client. Il file ricevuto può essere eseguito in locale nel dispositivo client per installare Network Agent senza utilizzare Kaspersky Security Center Cloud Console.

Per Network Agent per Linux e Network Agent per macOS, il pacchetto di installazione indipendente è un file di script con estensione sh. Quando si esegue questo file, lo script decomprime l'archivio allegato, che contiene il pacchetto di installazione e le relative impostazioni, quindi avvia l'installazione.

Se si installa Network Agent utilizzando un pacchetto di installazione indipendente in un dispositivo che esegue Microsoft Windows XP Professional for Embedded Systems a 32 bit, l'installazione non va a buon fine. Per risolvere il problema, installare prima l'aggiornamento KB2868626 per Windows XP dal sito Web Microsoft: https://www.catalog.update.microsoft.com/Search.aspx?q=KB2868626.

Per motivi di autenticazione, ogni pacchetto di installazione indipendente viene firmato utilizzando un certificato. Il certificato viene riemesso periodicamente. Dopo ogni procedura di riemissione del certificato, Kaspersky Security Center Cloud Console aggiorna automaticamente le firme di tutti i pacchetti di installazione indipendenti creati. Per i pacchetti di installazione indipendenti scaricati, non è possibile eseguire un aggiornamento automatico delle firme. Pertanto, il certificato scade e potrebbe verificarsi un errore del certificato durante l'installazione di un'applicazione da un pacchetto di installazione indipendente. In questo caso, scaricare nuovamente il pacchetto di installazione indipendente.

Per creare un pacchetto di installazione indipendente:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione. Se il pacchetto di installazione di Network Agent non è nell'elenco, creare manualmente questo pacchetto di installazione.

2. Nell'elenco dei pacchetti di installazione fare clic sul nome del pacchetto di installazione di Network Agent.

   Verrà visualizzata la finestra delle proprietà del pacchetto di installazione di Network Agent.

3. Se necessario, configurare le impostazioni del pacchetto di installazione di Network Agent e chiudere la finestra delle proprietà del pacchetto di installazione di Network Agent.

4. Nell'elenco dei pacchetti di installazione selezionare un pacchetto di installazione e, sopra l'elenco, fare clic sul pulsante **Distribuisci**.

5. Selezionare l'opzione **Utilizzo di un pacchetto indipendente**.

   Verrà avviata la Creazione guidata pacchetto di installazione indipendente. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

6. Nella prima pagina della procedura guidata assicurarsi che l'opzione **Installa Network Agent con questa applicazione** sia abilitata, se si desidera installare Network Agent insieme all'applicazione selezionata.

   Per impostazione predefinita, questa opzione è abilitata. È consigliabile abilitare questa opzione se non si è sicuri che Network Agent sia installato nel dispositivo. Se Network Agent è già installato nel dispositivo, dopo l'installazione del pacchetto di installazione indipendente con Network Agent, Network Agent verrà aggiornato alla versione più recente.

   Se si disabilita questa opzione, Network Agent non verrà installato nel dispositivo e il dispositivo non sarà gestito.

   Se un pacchetto di installazione indipendente per l'applicazione selezionata esiste già in Administration Server, la procedura guidata informa l'utente. In questo caso, è necessario selezionare una delle seguenti azioni:

- **Crea pacchetto di installazione indipendente**. Selezionare questa opzione se ad esempio si desidera creare un pacchetto di installazione indipendente per una nuova versione dell'applicazione e si desidera mantenere anche un pacchetto di installazione indipendente creato per una versione precedente dell'applicazione. Il nuovo pacchetto di installazione indipendente viene inserito in un'altra cartella.

- **Usa pacchetto di installazione indipendente esistente**. Selezionare questa opzione se si desidera utilizzare un pacchetto di installazione indipendente esistente. Il processo di creazione del pacchetto non verrà avviato.

- **Ricrea pacchetto di installazione indipendente esistente**. Selezionare questa opzione se si desidera creare nuovamente un pacchetto di installazione indipendente per la stessa applicazione. Il pacchetto di installazione indipendente viene inserito nella stessa cartella.

7. Nella pagina **Sposta nell'elenco dei dispositivi gestiti** della procedura guidata l'opzione **Non spostare i dispositivi** è selezionata per impostazione predefinita. Se non si desidera spostare il dispositivo client in un gruppo di amministrazione dopo l'installazione di Network Agent, non modificare la scelta dell'opzione.

   Se si desidera spostare il dispositivo client dopo l'installazione di Network Agent, selezionare l'opzione **Sposta i dispositivi non assegnati in questo gruppo** e specificare un gruppo di amministrazione in cui spostare il dispositivo client. Per impostazione predefinita, il dispositivo viene spostato nel gruppo **Dispositivi gestiti**.

8. Nella pagina successiva della procedura guidata selezionare l'opzione **Apri l'elenco dei pacchetti indipendenti** se si desidera visualizzare l'elenco dei pacchetti di installazione indipendenti al termine della procedura guidata.

9. Fare clic sul pulsante **Fine**.

   La Creazione guidata pacchetto di installazione indipendente verrà chiusa.

Viene creato il pacchetto di installazione indipendente di Network Agent. Il pacchetto di installazione indipendente creato viene visualizzato nell'elenco dei pacchetti di installazione indipendenti, che è possibile visualizzare.

Visualizzazione dell'elenco dei pacchetti di installazione indipendenti

È possibile visualizzare l'elenco dei pacchetti di installazione indipendenti e le proprietà di ciascun pacchetto di installazione indipendente.

Per visualizzare l'elenco dei pacchetti di installazione indipendenti per tutti i pacchetti di installazione:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione.

2. Sopra l'elenco, fare clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti**.

Verrà visualizzato un elenco dei pacchetti di installazione indipendenti.

Nell'elenco dei pacchetti di installazione indipendenti le relative proprietà vengono visualizzate come segue:

- **Nome pacchetto**. Nome del pacchetto di installazione indipendente, formato automaticamente dal nome dell'applicazione incluso nel pacchetto e dalla versione dell'applicazione.
- **Nome pacchetto di installazione di Network Agent**.
- **Versione di Network Agent**.
- **Dimensione**. Dimensione del file in megabyte (MB).
- **Gruppo**. Nome del gruppo in cui viene spostato il dispositivo client dopo l'installazione di Network Agent.
- **Data creazione**. Data e ora di creazione del pacchetto di installazione indipendente.
- **Ultima modifica**. Data e ora di modifica del pacchetto di installazione indipendente.
- **Hash del file**. La proprietà viene utilizzata per certificare che il pacchetto di installazione indipendente non è stato modificato da terze parti e che un utente ha lo stesso file che è stato creato e trasferito all'utente.

Per visualizzare l'elenco dei pacchetti di installazione indipendenti per un pacchetto di installazione specifico:

Selezionare il pacchetto di installazione nell'elenco e, sopra l'elenco, fare clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti**.

Nell'elenco dei pacchetti di installazione indipendenti è possibile eseguire le seguenti operazioni:

- Scaricare un pacchetto di installazione indipendente nel dispositivo facendo clic sul pulsante **Scarica**.

  Per motivi di autenticazione, ogni pacchetto di installazione indipendente viene firmato utilizzando un certificato. Il certificato viene riemesso periodicamente. Dopo ogni procedura di riemissione del certificato, Kaspersky Security Center Cloud Console aggiorna automaticamente le firme di tutti i pacchetti di installazione indipendenti creati. Per i pacchetti di installazione indipendenti scaricati, non è possibile eseguire un aggiornamento automatico delle firme. Pertanto, il certificato scade e potrebbe verificarsi un errore del certificato durante l'installazione di un'applicazione da un pacchetto di installazione indipendente. In questo caso, scaricare nuovamente il pacchetto di installazione indipendente.

- Rimuovere un pacchetto di installazione indipendente facendo clic sul pulsante **Rimuovi**.

Creazione di pacchetti di installazione personalizzati

È possibile utilizzare pacchetti di installazione personalizzati per le seguenti operazioni:

- Per installare un'applicazione (ad esempio un editor di testo) in un dispositivo client che utilizza Kaspersky Security Center Cloud Console, ad esempio mediante un'attività.
- Creare un pacchetto di installazione indipendente.

Un pacchetto di installazione personalizzato è una cartella con un set di file, compreso un file eseguibile. L'origine per creare un pacchetto di installazione personalizzato è un file di archivio. Il file di archivio contiene uno o più file che devono essere inclusi nel pacchetto di installazione personalizzato. Con la creazione di un pacchetto di installazione personalizzato, è possibile specificare le opzioni della riga di comando, ad esempio per installare l'applicazione in modalità automatica.

Per creare un pacchetto di installazione personalizzato:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Individuazione e distribuzione → Distribuzione e assegnazione → Pacchetti di installazione**.
   - Nel menu principale accedere a **Operazioni → Archivi → Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Fare clic su **Aggiungi**.

   Viene avviata la Creazione guidata nuovo pacchetto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nella prima pagina della procedura guidata selezionare **Crea pacchetto di installazione da un file**.

4. Nella pagina successiva della procedura guidata specificare il nome del pacchetto di installazione e fare clic sul pulsante **Sfoglia**.

   Una finestra **Apri** standard consente di scegliere un file di archivio per creare il pacchetto di installazione.

5. Selezionare un file di archivio presente sui dischi disponibili.

   È possibile caricare un file di archivio ZIP, CAB, TAR o TAR.GZ. Non è possibile creare un pacchetto di installazione da un file SFX (archivio autoestraente).

   I file vengono scaricati nell'Administration Server di Kaspersky Security Center Cloud Console.

   Se Administration Server rileva che l'archivio include l'applicazione Kaspersky, viene visualizzato un messaggio di errore. È possibile scaricare i pacchetti di installazione per le applicazioni Kaspersky dai server Web Kaspersky. Questa operazione è disponibile selezionando **Operazioni → Applicazioni Kaspersky → Versioni correnti delle applicazioni**.

6. Nella pagina successiva della procedura guidata, se il file di archivio selezionato include diversi file eseguibili, selezionare un solo file eseguibile da eseguire per l'installazione dell'applicazione utilizzando il pacchetto di installazione creato.

7. Se lo si desidera, specificare i parametri della riga di comando di un file eseguibile.

   È possibile specificare i parametri della riga di comando per installare l'applicazione dal pacchetto di installazione in modalità automatica. Fare riferimento alla documentazione del fornitore dell'applicazione per i dettagli dei parametri della riga di comando.

   Verrà avviata la creazione del pacchetto di installazione.

   La procedura guidata informa l'utente al termine della procedura.

   Se il pacchetto di installazione non viene creato, viene visualizzato un messaggio di errore.

   In Kaspersky Security Center Cloud Console il limite delle dimensioni totali di tutti i pacchetti di installazione nell'Administration Server è 500 MB. Se nel processo di creazione di un pacchetto di installazione viene superato il limite delle dimensioni totali, eliminare i pacchetti di installazione creati in precedenza. Le dimensioni di un pacchetto di installazione sono visualizzate nelle relative proprietà.

8. Fare clic sul pulsante **Fine** per chiudere la procedura guidata.

Il pacchetto di installazione personalizzato creato viene scaricato nell'Administration Server. Dopo il download, il pacchetto di installazione viene visualizzato nell'elenco dei pacchetti di installazione.

Nell'elenco dei pacchetti di installazione è possibile visualizzare le seguenti proprietà di un pacchetto di installazione personalizzato:

- **Nome**. Nome del pacchetto di installazione personalizzato.
- **Origine**. Nome del produttore dell'applicazione.
- **Applicazione**. Nome dell'applicazione inclusa nel pacchetto di installazione personalizzato.
- **Versione**. Versione applicazione.
- **Lingua**. Lingua dell'applicazione inclusa nel pacchetto di installazione personalizzato.
- **Dimensioni (MB)**. Dimensioni del pacchetto di installazione personalizzato.
- **Sistema operativo**. Sistema operativo per il quale viene creato il pacchetto di installazione personalizzato.
- **Data creazione**. Data di creazione del pacchetto di installazione.
- **Ultima modifica**. Data di modifica del pacchetto di installazione.
- **Tipo**. Applicazione Kaspersky o Applicazione di terze parti.

Nell'elenco dei pacchetti di installazione, facendo clic sul collegamento con il nome di un pacchetto di installazione personalizzato, è possibile modificare i parametri della riga di comando e il nome del pacchetto di installazione personalizzato.

Requisiti per un punto di distribuzione

Per gestire fino a 10.000 dispositivi client, un punto di distribuzione deve soddisfare almeno i seguenti requisiti (è disponibile una configurazione per un'esecuzione di test):

- CPU: Intel® Core™ i7-7700 CPU, 3,60 GHz 4 core.
- RAM: 8 GB.
- Spazio di archiviazione gratuito: 120 GB.

Inoltre, un punto di distribuzione deve disporre dell'accesso a Internet ed essere sempre connesso.

Se in Administration Server è presente un'attività di installazione remota in sospeso, il dispositivo con il punto di distribuzione richiederà inoltre una quantità di spazio disponibile sul disco pari alle dimensioni totali dei pacchetti di installazione da installare.

Se in Administration Server sono presenti una o più istanze in sospeso delle attività di installazione degli aggiornamenti (patch) e di correzione delle vulnerabilità, il dispositivo con il punto di distribuzione richiederà ulteriore spazio disponibile sul disco, una quantità pari al doppio delle dimensioni totali di tutte le patch da installare.

Impostazioni del criterio di Network Agent

Per configurare il criterio di Network Agent:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

2. Fare clic sul nome del criterio di Network Agent.

   Verrà visualizzata la finestra delle proprietà del criterio di Network Agent.

Tenere presente che per i dispositivi basati su Windows, macOS e Linux, sono disponibili varie impostazioni.

Scheda Generale

In questa scheda è possibile modificare lo stato del criterio e specificare l'ereditarietà delle impostazioni criterio:

- Nella sezione **Stato criterio** è possibile selezionare una modalità criterio:
  - **Attivo**
  - **Inattivo**

    Se questa opzione è selezionata, il criterio diventa inattivo, ma viene comunque salvato nella cartella **Criteri**. Se necessario, il criterio può essere attivato.

- Nel gruppo di impostazioni **Ereditarietà impostazioni** è possibile configurare l'ereditarietà del criterio:
  - **Eredita impostazioni dal criterio padre**

    Se questa opzione è abilitata, i valori delle impostazioni del criterio vengono ereditati dal criterio di gruppo di livello superiore e pertanto vengono bloccati.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Forza ereditarietà impostazioni nei criteri figlio**

    Se questa opzione è abilitata, una volta applicate le modifiche ai criteri, verranno eseguite le seguenti azioni:
    - I valori delle impostazioni dei criteri saranno propagati ai criteri dei sottogruppi di amministrazione, ovvero ai criteri figlio.
    - Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio figlio, l'opzione **Eredita impostazioni dal criterio padre** sarà abilitata automaticamente.

    Se questa opzione è abilitata, le impostazioni dei criteri figlio vengono bloccate.

    Per impostazione predefinita, questa opzione è disabilitata.

Scheda Configurazione eventi

Questa scheda consente di configurare la registrazione degli eventi e le notifiche degli eventi. Gli eventi vengono distribuiti in base al livello di importanza nelle seguenti sezioni nella scheda **Configurazione eventi**:

- **Errore funzionale**
- **Avviso**
- **Informazioni**

In ogni sezione l'elenco dei tipi di eventi mostra i tipi di eventi e il periodo di archiviazione predefinito per gli eventi in Administration Server (in giorni). Facendo clic sul pulsante **Proprietà** è possibile specificare le impostazioni di registrazione degli eventi e le notifiche sugli eventi selezionati nell'elenco. Per impostazione predefinita, le impostazioni di notifica comuni specificate per l'intero Administration Server vengono utilizzate per tutti i tipi di eventi. Tuttavia, è possibile modificare impostazioni specifiche per i tipi di eventi desiderati.

Scheda Impostazioni applicazione

Impostazioni

Nella sezione **Impostazioni** è possibile configurare il criterio di Network Agent:

- **Distribuisci i file solo tramite punti di distribuzione**

  Se questa opzione è abilitata, i dispositivi client ricevono gli aggiornamenti solo tramite i punti di distribuzione, non direttamente dai server di aggiornamento.

  Se questa opzione è disabilitata, i dispositivi client possono ricevere gli aggiornamenti da varie origini: direttamente dai server di aggiornamento e da una cartella locale o di rete.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima della coda di eventi (MB)**

- **L'applicazione può recuperare i dati estesi del criterio nel dispositivo**

  Network Agent installato in un dispositivo gestito trasferisce le informazioni sul criterio dell'applicazione di protezione applicato all'applicazione di protezione (ad esempio Kaspersky Endpoint Security for Windows). È possibile visualizzare le informazioni trasferite nell'interfaccia dell'applicazione di protezione.

  Network Agent trasferisce le seguenti informazioni:

  - Ora della distribuzione del criterio al dispositivo gestito
  - Nome del criterio attivo o fuori sede al momento della distribuzione del criterio al dispositivo gestito
  - Nome e percorso completo del gruppo di amministrazione che conteneva il dispositivo gestito al momento della distribuzione del criterio al dispositivo gestito
  - Elenco dei profili criterio attivi

    È possibile utilizzare le informazioni per assicurarsi che venga applicato il criterio corretto al dispositivo e per la risoluzione dei problemi. Per impostazione predefinita, questa opzione è disabilitata.

- **Proteggi il servizio Network Agent dalle operazioni non autorizzate di rimozione o terminazione e impedisci la modifica delle impostazioni**

  Quando questa opzione è abilitata, dopo l'installazione di Network Agent in un dispositivo gestito, il componente non può essere rimosso o riconfigurato senza i privilegi richiesti. Il servizio Network Agent non può essere arrestato. Questa opzione non ha effetto sui controller di dominio.

  Abilitare questa opzione per proteggere Network Agent sulle workstation gestite con diritti di amministratore locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- Usa password di disinstallazione

  Se questa opzione è abilitata, facendo clic sul pulsante **Modifica** è possibile specificare la password per l'utilità klmover e la disinstallazione remota di Network Agent.

  Per impostazione predefinita, questa opzione è disabilitata.

Archivi

Nella sezione **Archivi** è possibile selezionare i tipi di oggetti i cui dettagli verranno inviati da Network Agent ad Administration Server. Se la modifica di alcune impostazioni in questa sezione non è consentita dal criterio di Network Agent, non è possibile modificare tali impostazioni. Le impostazioni nella sezione **Archivi** sono disponibili solo nei dispositivi che eseguono Windows:

- **Informazioni dettagliate sulle applicazioni installate**
- Includi informazioni sulle patch

  Le informazioni sulle patch delle applicazioni installate nei dispositivi client vengono inviate ad Administration Server. L'abilitazione di questa opzione può aumentare il carico su Administration Server e DBMS, nonché incrementare il volume del database.

  Per impostazione predefinita, questa opzione è abilitata. È disponibile solo per Windows.

- Informazioni dettagliate sugli aggiornamenti Windows Update

  Se questa opzione è abilitata, le informazioni sugli aggiornamenti di Microsoft Windows Update da installare nei dispositivi client vengono inviate ad Administration Server.

  A volte, anche se l'opzione è disabilitata, gli aggiornamenti vengono visualizzati nelle proprietà del dispositivo, nella sezione **Aggiornamenti disponibili**. Questo potrebbe ad esempio accadere se i dispositivi dell'organizzazione presentassero vulnerabilità correggibili tramite questi aggiornamenti.

  Per impostazione predefinita, questa opzione è abilitata. È disponibile solo per Windows.

- Dettagli sulle vulnerabilità del software e sugli aggiornamenti corrispondenti

  Se questa opzione è abilitata, le informazioni sulle vulnerabilità nel software di terze parti (incluso il software Microsoft) rilevate nei dispositivi gestiti e sugli aggiornamenti software per correggere le vulnerabilità di terze parti (escluso il software Microsoft) vengono inviate ad Administration Server.

  Selezionando questa opzione (**Dettagli sulle vulnerabilità del software e sugli aggiornamenti corrispondenti**) aumentano il carico di rete, il carico sul disco di Administration Server e il consumo di risorse di Network Agent.

  Per impostazione predefinita, questa opzione è abilitata. È disponibile solo per Windows.

  Per gestire gli aggiornamenti software del software Microsoft, utilizzare l'opzione **Informazioni dettagliate sugli aggiornamenti Windows Update.**

- **Dettagli registro hardware**

Vulnerabilità e aggiornamenti software

Nella sezione **Vulnerabilità e aggiornamenti software** è possibile configurare la ricerca degli aggiornamenti di Windows, nonché abilitare la scansione dei file eseguibili per rilevare la presenza di vulnerabilità. Le impostazioni nella sezione **Vulnerabilità e aggiornamenti software** sono disponibili solo nei dispositivi che eseguono Windows:

- In **Consentire agli utenti di gestire l'installazione degli aggiornamenti Windows Update** è possibile limitare gli aggiornamenti di Windows che gli utenti possono installare manualmente nei propri dispositivi tramite Windows Update.

  Nei dispositivi che eseguono Windows 10, se Windows Update ha già rilevato aggiornamenti per il dispositivo, la nuova opzione selezionata in **Consentire agli utenti di gestire l'installazione degli aggiornamenti Windows Update** verrà applicata solo dopo l'installazione degli aggiornamenti rilevati.

  Selezionare un elemento nell'elenco a discesa:

  - Consentire agli utenti di installare tutti gli aggiornamenti Windows Update applicabili

    Gli utenti possono installare nei propri dispositivi tutti gli aggiornamenti di Microsoft Windows Update applicabili.

    Selezionare questa opzione se non si desidera interferire nell'installazione degli aggiornamenti.

    Quando l'utente installa manualmente gli aggiornamenti di Microsoft Windows Update, gli aggiornamenti possono essere scaricati dai server Microsoft anziché da Administration Server. Questo è possibile se Administration Server non ha ancora scaricato gli aggiornamenti. Il download degli aggiornamenti dai server Microsoft comporta un traffico aggiuntivo.

  - Consentire agli utenti di installare solo gli aggiornamenti Windows Update approvati

    Gli utenti possono installare nei propri dispositivi tutti gli aggiornamenti di Microsoft Windows Update applicabili e approvati dall'amministratore.

    Ad esempio, potrebbe essere utile controllare prima l'installazione degli aggiornamenti in un ambiente di test e verificare che non interferiscano con l'utilizzo dei dispositivi e solo successivamente consentire l'installazione degli aggiornamenti approvati nei dispositivi client.

    Quando l'utente installa manualmente gli aggiornamenti di Microsoft Windows Update, gli aggiornamenti possono essere scaricati dai server Microsoft anziché da Administration Server. Questo è possibile se Administration Server non ha ancora scaricato gli aggiornamenti. Il download degli aggiornamenti dai server Microsoft comporta un traffico aggiuntivo.

  - Non consentire agli utenti di installare gli aggiornamenti Windows Update

    Gli utenti non possono installare manualmente gli aggiornamenti di Microsoft Windows Update nei propri dispositivi. Tutti gli aggiornamenti applicabili vengono installati in base alla configurazione specificata dall'amministratore.

    Selezionare questa opzione se si desidera gestire l'installazione degli aggiornamenti in modo centralizzato.

    È ad esempio possibile ottimizzare la pianificazione degli aggiornamenti in modo da evitare di sovraccaricare la rete. È possibile pianificare le installazioni degli aggiornamenti in orario non lavorativo, in modo che non interferiscano con la produttività degli utenti.

- Nel gruppo di impostazioni **Modalità di ricerca di Windows Update** è possibile selezionare la modalità di ricerca degli aggiornamenti:

  - **Attiva**

    Se questa opzione è selezionata, Administration Server con il supporto di Network Agent avvia una richiesta da un Windows Update Agent nel dispositivo client alla sorgente aggiornamenti: server Windows Update o WSUS. Successivamente, Network Agent trasmette le informazioni ricevute da Windows Update Agent ad Administration Server.

    L'opzione è valida solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** dell'attività *Trova vulnerabilità e aggiornamenti richiesti* è selezionata.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Passiva**

    Se questa opzione è selezionata, Network Agent trasmette periodicamente ad Administration Server le informazioni sugli aggiornamenti recuperati durante l'ultima sincronizzazione di Windows Update Agent con la sorgente aggiornamenti. Se non viene eseguita la sincronizzazione di Windows Update Agent con una sorgente aggiornamenti, le informazioni sugli aggiornamenti in Administration Server diventano obsolete.

    Selezionare questa opzione se si desidera ottenere gli aggiornamenti dalla cache della memoria della sorgente aggiornamenti.

  - **Disabilitata**

    Se questa opzione è selezionata, Administration Server non richiede informazioni sugli aggiornamenti.

    Selezionare questa opzione se, ad esempio, si desidera prima testare gli aggiornamenti nel dispositivo locale.

- **Esegui la scansione dei file eseguibili per rilevarne le vulnerabilità al momento dell'esecuzione**

  Se questa opzione è abilitata, i file eseguibili vengono esaminati alla ricerca di vulnerabilità al momento dell'esecuzione.

  Per impostazione predefinita, questa opzione è disabilitata.

Gestione riavvio

Nella sezione **Gestione riavvio** è possibile specificare l'azione che deve essere eseguita se il sistema operativo di un dispositivo gestito deve essere riavviato per utilizzare, installare o disinstallare correttamente un'applicazione. Le impostazioni nella sezione **Gestione riavvio** sono disponibili solo nei dispositivi che eseguono Windows:

- **Non riavviare il sistema operativo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia automaticamente il sistema operativo se necessario**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

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

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Forza riavvio dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

  L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

  Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

  Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

  Per impostazione predefinita, questa opzione è disabilitata.

Condivisione desktop Windows

Nella sezione **Condivisione desktop Windows** è possibile abilitare e configurare il controllo delle azioni eseguite dall'amministratore in un dispositivo remoto quando viene condiviso l'accesso al desktop. Le impostazioni nella sezione **Condivisione desktop Windows** sono disponibili solo nei dispositivi che eseguono Windows:

- Abilita controllo

  Se questa opzione è abilitata, il controllo delle azioni dell'amministratore nel dispositivo remoto è abilitato. I record relativi alle azioni dell'amministratore nel dispositivo remoto vengono registrati:

  - Nel registro eventi del dispositivo remoto
  - In un file con estensione syslog nella cartella di installazione di Network Agent nel dispositivo remoto
  - Nel database degli eventi di Kaspersky Security Center Cloud Console

  Il controllo delle azioni dell'amministratore è disponibile quando sono soddisfatte le seguenti condizioni:

  - È in uso la licenza per Vulnerability e patch management
  - L'amministratore dispone del diritto per l'avvio dell'accesso condiviso al desktop del dispositivo remoto

  Se questa opzione è disabilitata, il controllo delle azioni dell'amministratore nel dispositivo remoto è disabilitato.

  Per impostazione predefinita, questa opzione è disabilitata.

- Maschere dei file da monitorare durante la lettura

  L'elenco contiene le maschere dei file. Quando il controllo è abilitato, l'applicazione monitora i file di lettura dell'amministratore corrispondenti alle maschere e salva le informazioni sui file letti. L'elenco è disponibile se la casella di controllo **Abilita controllo** è selezionata. È possibile modificare le maschere dei file e aggiungerne di nuove all'elenco. Ogni nuova maschera di file deve essere specificata nell'elenco su una nuova riga.

  Per impostazione predefinita, sono specificate le seguenti maschere dei file: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- Maschere dei file da monitorare durante la modifica

  L'elenco contiene maschere dei file nel dispositivo remoto. Quando il controllo è abilitato, l'applicazione monitora le modifiche apportate dall'amministratore ai file corrispondenti alle maschere e salva le informazioni su tali modifiche. L'elenco è disponibile se la casella di controllo **Abilita controllo** è selezionata. È possibile modificare le maschere dei file e aggiungerne di nuove all'elenco. Ogni nuova maschera di file deve essere specificata nell'elenco su una nuova riga.

  Per impostazione predefinita, sono specificate le seguenti maschere dei file: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Gestire patch e aggiornamenti

Nella sezione **Gestire patch e aggiornamenti** è possibile configurare il download e la distribuzione degli aggiornamenti, nonché l'installazione delle patch nei dispositivi gestiti: abilitare o disabilitare l'opzione **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito**.

Connettività

La sezione **Connettività** include tre sottosezioni:

- **Rete**

- **Profili connessione**
- **Pianificazione connessione**

Nella sottosezione **Rete**, è possibile configurare la connessione ad Administration Server, abilitare l'utilizzo di una porta UDP e specificare il numero della porta UDP.

- Nel gruppo di impostazioni **Connessione ad Administration Server**, è possibile specificare le seguenti impostazioni:
  - Comprimi traffico di rete

    Se questa opzione è abilitata, la velocità di trasferimento dei dati da parte di Network Agent viene aumentata attraverso una riduzione della quantità di informazioni da trasferire e una conseguente riduzione del carico di Administration Server.

    Il carico di lavoro sulla CPU del computer client potrebbe aumentare.

    Per impostazione predefinita, questa casella di controllo è abilitata.

  - Apri porte di Network Agent in Microsoft Windows Firewall

    Se questa opzione è abilitata, una porta UDP necessaria per l'utilizzo di Network Agent viene aggiunta all'elenco di esclusioni di Microsoft Windows Firewall.

    Per impostazione predefinita, questa opzione è abilitata.

  - Usa il gateway di connessione in un punto di distribuzione (se disponibile) con le impostazioni di connessione predefinite

    Se questa opzione è abilitata, viene utilizzato il gateway di connessione nel punto di distribuzione con le impostazioni specificate nelle proprietà del gruppo di amministrazione.

    Per impostazione predefinita, questa opzione è abilitata.

- Usa porta UDP

  Se è necessario che i dispositivi gestiti si connettano al server proxy KSN attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in **Porta UDP**. Per impostazione predefinita, questa opzione è abilitata. La porta UDP predefinita per la connessione al server proxy KSN è la 15111.

- Numero di porta UDP

  In questo campo è possibile immettere il numero della porta UDP. Il numero di porta predefinito è 15000.

  Viene utilizzato il sistema decimale per i record.

  Se il dispositivo client esegue Windows XP Service Pack 2, il firewall integrato blocca la porta UDP 15000. Si consiglia di aprire questa porta manualmente.

- Usa il punto di distribuzione per forzare una connessione ad Administration Server

Selezionare questa opzione se è stata selezionata l'opzione **Esegui server push** nella finestra delle impostazioni dei punti di distribuzione. In caso contrario, il punto di distribuzione non fungerà da server push.

Nella sottosezione **Profili connessione** non è possibile aggiungere nuovi elementi all'elenco **Profili connessione di Administration Server**, pertanto il pulsante **Aggiungi** è inattivo. Non è neanche possibile modificare i profili di connessione preimpostati.

Nella sottosezione **Pianificazione connessione** è possibile specificare gli intervalli di tempo durante i quali Network Agent invia i dati ad Administration Server:

- **Connetti quando necessario**
- **Connetti negli intervalli di tempo specificati**

Nella sottosezione **Pianificazione connessione** è possibile specificare gli intervalli di tempo durante i quali Network Agent invia i dati ad Administration Server:

- Connetti quando necessario

  Se questa opzione è selezionata, la connessione viene stabilita quando Network Agent deve inviare i dati ad Administration Server.

  Per impostazione predefinita, questa opzione è selezionata.

- Connetti negli intervalli di tempo specificati

  Se questa opzione è selezionata, Network Agent si connette ad Administration Server all'ora specificata. È possibile aggiungere diversi periodi di tempo per la connessione.

Polling di rete per punti di distribuzione

Nella sezione **Polling di rete per punti di distribuzione** è possibile configurare il polling automatico della rete. Le impostazioni del polling sono disponibili solo nei dispositivi che eseguono Windows. È possibile utilizzare le seguenti opzioni per abilitare il polling e impostarne la frequenza:

- Rete Windows

  Se questa opzione è abilitata, il punto di distribuzione esegue automaticamente il polling della rete in base alla pianificazione configurata facendo clic sui collegamenti **Imposta pianificazione di polling rapido** e **Imposta pianificazione di polling completo**.

  Se questa opzione è disabilitata, Administration Server non esegue il polling della rete.

  Per impostazione predefinita, questa opzione è abilitata.

- Intervalli IP

Se questa opzione è abilitata, il punto di distribuzione esegue automaticamente il polling degli intervalli IP in base alla pianificazione configurata facendo clic sul collegamento **Imposta pianificazione di polling**.

Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling degli intervalli IP.

Per impostazione predefinita, questa opzione è disabilitata.

- Controller di dominio

  Se l'opzione è abilitata, il punto di distribuzione esegue automaticamente il polling dei controller di dominio in base alla pianificazione configurata facendo clic sul pulsante **Imposta pianificazione di polling**.

  Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling dei controller di dominio.

  La frequenza di polling dei controller di dominio per le versioni di Network Agent precedenti alla 10.2 può essere configurata nel campo **Intervallo di polling (min.)**. Il campo è disponibile se questa opzione è abilitata.

  Per impostazione predefinita, questa opzione è disabilitata.

Impostazioni di rete per punti di distribuzione

Nella sezione **Impostazioni di rete per punti di distribuzione** è possibile specificare le impostazioni di accesso a Internet:

- **Usa server proxy**
- **Indirizzo**
- **Numero di porta**
- Ignora il server proxy per gli indirizzi locali

  Se questa opzione è abilitata, non viene utilizzato alcun server proxy per la connessione ai dispositivi nella rete locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- Autenticazione server proxy

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Nome utente**
- **Password**

Proxy KSN (punti di distribuzione)

Nella sezione **Proxy KSN (punti di distribuzione)** è possibile configurare l'applicazione per l'utilizzo del punto di distribuzione per l'inoltro delle richieste KSN dai dispositivi gestiti:

- **Abilita proxy KSN da parte del punto di distribuzione**

  Il servizio proxy KSN viene eseguito nel dispositivo utilizzato come punto di distribuzione. Utilizzare questa funzionalità per ridistribuire e ottimizzare il traffico nella rete.

  Questa funzionalità non è supportata dai dispositivi dei punti di distribuzione che eseguono Linux o macOS.

  Il punto di distribuzione invia le statistiche KSN, elencate nell'informativa di Kaspersky Security Network, a Kaspersky. Per impostazione predefinita, l'informativa KSN è disponibile in %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Per impostazione predefinita, questa opzione è disabilitata. L'attivazione di questa opzione ha effetto solo se l'opzione **Accetto di utilizzare Kaspersky Security Network** è abilitata nella finestra delle proprietà di Administration Server.

  È possibile assegnare il nodo di un cluster attivo-passivo a un punto di distribuzione e abilitare il proxy KSN in tale nodo.

- **Porta**

  Numero della porta TCP utilizzata dai dispositivi gestiti per la connessione al server proxy KSN. Il numero di porta predefinito è 13111.

- **Porta UDP**

  Se è necessario che i dispositivi gestiti si connettano al server proxy KSN attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in **Porta UDP**. Per impostazione predefinita, questa opzione è abilitata. La porta UDP predefinita per la connessione al server proxy KSN è la 15111.

Confronto tra le impostazioni dei criteri di Network Agent in base ai sistemi operativi

La seguente tabella mostra quali impostazioni dei criteri di Network Agent è possibile utilizzare per configurare Network Agent con un sistema operativo specifico.

Impostazioni dei criteri di Network Agent: confronto in base ai sistemi operativi

Sezione Criterio	Windows	macOS	Linux
Generale	✓	✓	✓
Configurazione eventi	✓	✓	✓
Impostazioni	✓	✓ Ad accezione della casella di controllo **Usa password di disinstallazione**.	✓ Ad accezione della casella di controllo **Usa password di disinstallazione**.
Archivi	✓	–	✓ Sono disponibili le seguenti opzioni:

			• Informazioni dettagliate sulle applicazioni installate • Dettagli registro hardware
Vulnerabilità e aggiornamenti software	✓	–	–
Gestione riavvio	✓	–	–
Condivisione desktop Windows	✓	–	–
Gestire patch e aggiornamenti	✓	–	–
Connettività → Rete	✓	✓ * tranne la casella di controllo **Apri porte di Network Agent in Microsoft Windows Firewall**	✓ * tranne la casella di controllo **Apri porte di Network Agent in Microsoft Windows Firewall**
Connettività → Pianificazione connessione	✓	✓	✓
Polling di rete per punti di distribuzione	✓ Sono disponibili le seguenti opzioni: • **Rete Windows** • **Intervalli IP** • **Controller di dominio** (Microsoft Active Directory)	–	✓ Sono disponibili le seguenti opzioni: • **Intervalli IP** • **Controller di dominio** (Microsoft Active Directory, Samba come Active Directory)
Impostazioni di rete per punti di distribuzione	✓	✓	✓
Proxy KSN (punti di distribuzione)	✓	–	✓

Impostazioni del pacchetto di installazione di Network Agent

Per configurare un pacchetto di installazione di Network Agent:

1. Eseguire una delle seguenti operazioni:

- Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
- Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Fare clic sul collegamento con il nome del pacchetto di installazione di Network Agent.

Verrà visualizzata la finestra delle proprietà del pacchetto di installazione di Network Agent. Le informazioni nella finestra sono raggruppate in schede e in sezioni.

Generale

Nella sezione **Generale** vengono visualizzate informazioni generali sul pacchetto di installazione:

- Nome pacchetto di installazione
- Nome e versione dell'applicazione per cui è stato creato il pacchetto di installazione
- Dimensione del pacchetto di installazione
- Data di creazione del pacchetto di installazione
- Percorso della cartella del pacchetto di installazione

Impostazioni

Questa sezione presenta le impostazioni necessarie per assicurare il corretto funzionamento di Network Agent subito dopo essere stato installato. Le impostazioni in questa sezione sono disponibili solo nei dispositivi che eseguono Windows.

Nel gruppo di impostazioni **Cartella di destinazione** è possibile selezionare la cartella del dispositivo client in cui verrà installato Network Agent.

- **Installa nella cartella predefinita**

  Se questa opzione è selezionata, Network Agent verrà installato nella cartella <Unità>:\Programmi\Kaspersky Lab\NetworkAgent. Se la cartella non esiste, verrà creata automaticamente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Installa nella cartella specificata**

  Se questa opzione è selezionata, Network Agent verrà installato nella cartella specificata nel campo di immissione.

Nel seguente gruppo di impostazioni è possibile impostare una password per l'attività di disinstallazione remota di Network Agent:

- **Usa password di disinstallazione**

Se questa opzione è abilitata, facendo clic sul pulsante **Modifica** è possibile immettere la password di disinstallazione (disponibile solo per Network Agent nei dispositivi che eseguono sistemi operativi Windows).

Per impostazione predefinita, questa opzione è disabilitata.

- **Stato**
- **Proteggi il servizio Network Agent dalle operazioni non autorizzate di rimozione o terminazione e impedisci la modifica delle impostazioni**

  Quando questa opzione è abilitata, dopo l'installazione di Network Agent in un dispositivo gestito, il componente non può essere rimosso o riconfigurato senza i privilegi richiesti. Il servizio Network Agent non può essere arrestato. Questa opzione non ha effetto sui controller di dominio.

  Abilitare questa opzione per proteggere Network Agent sulle workstation gestite con diritti di amministratore locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito**

  Se questa casella di controllo è selezionata, tutte le patch e gli aggiornamenti scaricati per Network Agent verranno installati automaticamente.

  Se questa casella di controllo è deselezionata, tutti gli aggiornamenti e le patch scaricati verranno installati solo dopo l'impostazione dello stato su *Approvato*. Gli aggiornamenti e le patch con lo stato *Indefinito* non verranno installati.

  Per impostazione predefinita, questa casella di controllo è selezionata.

Connessione

In questa sezione è possibile configurare la connessione di Network Agent ad Administration Server:

- **Usa porta UDP**

  Numero di porta UDP

  In questo campo è possibile specificare la porta utilizzata per la connessione di Administration Server a Network Agent tramite il protocollo UDP.

  La porta UDP predefinita è 15000.

- **Apri porte di Network Agent in Microsoft Windows Firewall**

  Se questa opzione è abilitata, le porte UDP utilizzate da Network Agent vengono aggiunte all'elenco di esclusioni di Microsoft Windows Firewall.

  Per impostazione predefinita, questa opzione è abilitata.

- **Non usare server proxy**
- **Usa server proxy**

  Indirizzo server proxy

Porta server proxy

- **Autenticazione server proxy**

  Se questa opzione è abilitata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

  Per impostazione predefinita, questa opzione è disabilitata.

Nome utente

Nome utente dell'account con cui viene stabilita la connessione al server proxy.

È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

Password

Password dell'account con cui viene stabilita la connessione al server proxy.

È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

Avanzate

Nella sezione **Avanzate** è possibile configurare la modalità di utilizzo del gateway di connessione:

- **Esegui la connessione ad Administration Server utilizzando un gateway di connessione**
- **Indirizzo gateway connessione**
- **Abilita modalità dinamica per VDI**

  Se questa opzione è abilitata, la modalità dinamica per Virtual Desktop Infrastructure (VDI) sarà abilitata per Network Agent installato in una macchina virtuale.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Ottimizza le impostazioni per VDI**

  Se questa opzione è abilitata, le seguenti funzionalità sono disabilitate nelle impostazioni di Network Agent:

  - Recupero delle informazioni sul software installato
  - Recupero delle informazioni sull'hardware
  - Recupero delle informazioni sulle vulnerabilità rilevate
  - Recupero delle informazioni sugli aggiornamenti richiesti

  Per impostazione predefinita, questa opzione è disabilitata.

Componenti aggiuntivi

In questa sezione è possibile selezionare i componenti aggiuntivi per l'installazione simultanea con Network Agent.

Tag

La sezione **Tag** visualizza un elenco di parole chiave (tag) che possono essere aggiunte ai dispositivi client dopo l'installazione di Network Agent. È possibile aggiungere e rimuovere tag dall'elenco, nonché rinominarli.

Se la casella di controllo accanto a un tag è selezionata, il tag viene aggiunto automaticamente ai dispositivi gestiti durante l'installazione di Network Agent.

Se la casella di controllo accanto a un tag è deselezionata, il tag non viene aggiunto automaticamente ai dispositivi gestiti durante l'installazione di Network Agent. È possibile aggiungere manualmente il tag ai dispositivi.

Rimuovendo un tag dall'elenco, il tag viene rimosso automaticamente da tutti i dispositivi a cui è stato aggiunto.

Cronologia revisioni

In questa sezione è possibile visualizzare la cronologia delle revisioni del pacchetto di installazione. È possibile confrontare le revisioni, visualizzare le revisioni, salvare le revisioni in un file e aggiungere e modificare le descrizioni delle revisioni.

Le impostazioni del pacchetto di installazione di Network Agent disponibili per un sistema operativo specifico sono riportate nella tabella seguente.

Impostazioni del pacchetto di installazione di Network Agent

Sezione delle proprietà	Windows	Mac	Linux
Generale	✓	✓	✓
Impostazioni	✓	–	–
Connessione	✓	✓ * tranne la casella di controllo **Apri porte di Network Agent in Microsoft Windows Firewall**	✓ * tranne la casella di controllo **Apri porte di Network Agent in Microsoft Windows Firewall**
Avanzate	✓	✓	✓
Componenti aggiuntivi	✓	✓	✓
Tag	✓	✓ * tranne le regole di tagging automatico	✓ * tranne le regole di tagging automatico
Cronologia revisioni	✓	✓	✓

Infrastruttura virtuale

Kaspersky Security Center Cloud Console supporta l'utilizzo di macchine virtuali. Per proteggere l'infrastruttura virtuale, è necessario installare Network Agent in ogni macchina virtuale.

Suggerimenti per la riduzione del carico sulle macchine virtuali

Durante l'installazione di Network Agent in una macchina virtuale, è consigliabile valutare se disabilitare alcune funzionalità di Kaspersky Security Center Cloud Console che risultano di scarsa utilità per le macchine virtuali.

Quando si installa Network Agent in una macchina virtuale o in un modello utilizzato per la generazione di macchine virtuali, è consigliabile eseguire le seguenti azioni:

- Se si esegue un'installazione remota, nella finestra delle proprietà del pacchetto di installazione di Network Agent, nella sezione **Avanzate** selezionare l'opzione **Ottimizza le impostazioni per VDI**.
- Se si esegue un'installazione interattiva tramite una procedura guidata, nella finestra della procedura guidata selezionare l'opzione **Ottimizza le impostazioni di Network Agent per l'infrastruttura virtuale**.

La selezione di queste opzioni modifica le impostazioni di Network Agent in modo da mantenere disabilitate le seguenti funzionalità per impostazione predefinita (prima dell'applicazione di un criterio):

- Recupero delle informazioni sul software installato
- Recupero delle informazioni sull'hardware
- Recupero delle informazioni sulle vulnerabilità rilevate
- Recupero delle informazioni sugli aggiornamenti richiesti

In genere, queste funzionalità non sono necessarie nelle macchine virtuali perché utilizzano software uniforme e hardware virtuale.

La disabilitazione delle funzionalità è reversibile. Se è richiesta una delle funzionalità disabilitate, è possibile abilitarla tramite il criterio di Network Agent o mediante le impostazioni locali di Network Agent. Le impostazioni locali di Network Agent sono disponibili tramite il menu di scelta rapida del dispositivo appropriato in Administration Console.

Supporto delle macchine virtuali dinamiche

Kaspersky Security Center Cloud Console supporta le macchine virtuali dinamiche. Se nella rete dell'organizzazione è stata distribuita un'infrastruttura virtuale, in alcuni casi è possibile utilizzare macchine virtuali (temporanee) dinamiche. Le macchine virtuali dinamiche vengono create con nomi univoci in base a un modello che è stato preparato dall'amministratore. L'utente lavora su una macchina virtuale per un certo periodo e, dopo lo spegnimento, questa macchina virtuale sarà rimossa dall'infrastruttura virtuale. Anche la macchina virtuale con Network Agent installato viene aggiunta al database di Administration Server. Dopo lo spegnimento di questa macchina virtuale, anche la voce corrispondente deve essere rimossa dal database di Administration Server.

Per rendere disponibile la funzionalità di rimozione automatica delle voci nelle macchine virtuali, durante l'installazione di Network Agent in un modello per le macchine virtuali dinamiche, selezionare l'opzione **Abilita modalità dinamica per VDI**:

- Per l'installazione remota - Nella finestra delle proprietà del pacchetto di installazione di Network Agent (sezione **Avanzate**)
- Per l'installazione interattiva - Nell'Installazione guidata di Network Agent

Evitare di selezionare l'opzione **Abilita modalità dinamica per VDI** durante l'installazione di Network Agent nei dispositivi fisici.

Se si desidera archiviare gli eventi generati dalle macchine virtuali dinamiche in Administration Server per un certo periodo dopo la rimozione delle macchine virtuali, nella finestra delle proprietà di Administration Server, nella sezione **Archivio eventi**, selezionare l'opzione **Archivia eventi dopo l'eliminazione dei dispositivi** e specificare il periodo di archiviazione massimo degli eventi (in giorni).

Supporto della copia delle macchine virtuali

Kaspersky Security Center Cloud Console supporta la copia di una macchina virtuale con Network Agent installato o la creazione di una macchina da un modello con Network Agent installato.

Network Agent è in grado di rilevare automaticamente la copia delle macchine virtuali nei seguenti casi:

- L'opzione **Abilita modalità dinamica per VDI** era selezionata durante l'installazione di Network Agent: dopo ogni riavvio del sistema operativo, questa macchina virtuale sarà riconosciuta come un nuovo dispositivo, indipendentemente dal fatto che sia stata copiata.
- È in uso uno dei seguenti hypervisor: VMware™, HyperV® o Xen®: Network Agent rileva la copia della macchina virtuale in base agli ID modificati dell'hardware virtuale.

L'analisi delle modifiche nell'hardware virtuale non è assolutamente affidabile. Prima di applicare questo metodo su larga scala, è necessario testarlo su un piccolo gruppo di macchine virtuali per la versione dell'hypervisor attualmente in uso nell'organizzazione.

Utilizzo di Network Agent per Windows, macOS e Linux a confronto

Network Agent per macOS e Linux presenta diverse limitazioni funzionali rispetto a Network Agent per Windows. Anche le impostazioni del criterio e del pacchetto di installazione di Network Agent variano a seconda del sistema operativo. La tabella seguente mette a confronto le funzionalità di Network Agent e gli scenari di utilizzo disponibili per i sistemi operativi Windows, macOS e Linux.

Confronto fra le funzionalità di Network Agent

Funzionalità di Network Agent	Windows	Linux	macOS
Installazione			
Installazione automatica di aggiornamenti e patch per Network Agent	✓	–	–
Distribuzione automatica di una chiave	✓	✓	✓
Installazione manuale, eseguendo i programmi di	✓	✓	✓

installazione delle applicazioni nei dispositivi			
Sincronizzazione forzata	✓	✓	✓
Punto di distribuzione			
Polling della rete	✓ • Polling intervallo IP • Polling della rete Windows • Polling del controller di dominio (Microsoft Active Directory)	✓ • Polling intervallo IP • Polling del controller di dominio (Microsoft Active Directory, Samba come Active Directory)	–
Esecuzione del servizio proxy KSN da parte di un punto di distribuzione	✓	–	–
Download degli aggiornamenti tramite i server degli aggiornamenti Kaspersky nei repository dei punti di distribuzione che distribuiscono gli aggiornamenti ai dispositivi gestiti	✓	✓	– I dispositivi dei punti di distribuzione che eseguono macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky. Se uno o più dispositivi che eseguono macOS rientrano nell'ambito dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'attività viene completata con lo stato *Non riuscito*, anche se è stata completata correttamente in tutti i dispositivi Windows.
Installazione push delle applicazioni	✓	Limitata: non è possibile eseguire l'installazione push su dispositivi Linux utilizzando i punti di distribuzione macOS.	
Gestione delle applicazioni di terzi			
Installazione remota delle applicazioni nei dispositivi	✓	–	–

Aggiornamenti software	✓	–	–
Configurazione degli aggiornamenti del sistema operativo in un criterio di Network Agent	✓	–	–
Visualizzazione delle informazioni sulle vulnerabilità del software	✓	–	–
Scansione delle applicazioni per rilevare la presenza di vulnerabilità	✓	–	–
Inventario del software installato nei dispositivi	✓	–	–
Macchine virtuali			
Installazione di Network Agent in una macchina virtuale	✓	✓	✓
Ottimizzazione delle impostazioni per VDI (Virtual Desktop Infrastructure)	✓	✓	✓
Supporto delle macchine virtuali dinamiche	✓	✓	✓
Altro			
Azioni di controllo in un dispositivo client remoto utilizzando Condivisione desktop Windows	✓	–	–
Gestione dei riavvii dei dispositivi	✓	–	–
Gestione connessioni	✓	✓	✓
Connessione remota al desktop di un dispositivo client	✓	–	–

Le seguenti sezioni vengono visualizzate nelle proprietà del punto di distribuzione, ma le funzionalità corrispondenti non sono supportate da Network Agent per macOS:

- Sorgente degli aggiornamenti
- Server proxy KSN
- Domini Windows
- Active Directory
- Intervalli IP
- Avanzate

- Statistiche

Definizione delle impostazioni per l'installazione remota nei dispositivi Unix

Quando si installa un'applicazione in un dispositivo Unix utilizzando un'attività di installazione remota, è possibile specificare le impostazioni specifiche per Unix per l'attività. Queste impostazioni sono disponibili nelle proprietà dell'attività dopo la creazione dell'attività.

Per specificare le impostazioni specifiche per Unix per un'attività di installazione remota:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul nome dell'attività di installazione remota per la quale si desidera specificare le impostazioni specifiche per Unix.

   Verrà visualizzata la finestra delle proprietà dell'attività.
3. Accedere a **Impostazioni applicazione** → **Impostazioni specifiche per Unix**.
4. Specificare le seguenti impostazioni:

   - Imposta una password per l'account radice (solo per la distribuzione tramite SSH)

     Se il comando `sudo` non può essere utilizzato nel dispositivo di destinazione senza specificare la password, selezionare questa opzione, quindi specificare la password per l'account radice. Kaspersky Security Center Cloud Console trasmette la password in formato criptato al dispositivo di destinazione, decripta la password e avvia la procedura di installazione per conto dell'account radice con la password specificata.

     Kaspersky Security Center Cloud Console non utilizza l'account o la password specificata per creare una connessione SSH.

   - Specifica il percorso di una cartella temporanea con autorizzazioni Esecuzione nel dispositivo di destinazione (solo per la distribuzione tramite SSH)

     Se la directory /tmp nel dispositivo di destinazione non dispone dell'autorizzazione di esecuzione, selezionare questa opzione e specificare il percorso della directory con l'autorizzazione di esecuzione. Kaspersky Security Center Cloud Console utilizza la directory specificata come directory temporanea per accedere tramite SSH. L'applicazione inserisce il pacchetto di installazione nella directory ed esegue la procedura di installazione.
5. Fare clic sul pulsante **Salva**.

Le impostazioni dell'attività specificata vengono salvate.

Sostituzione di applicazioni di protezione di terzi

L'Installazione delle applicazioni di protezione Kaspersky tramite Kaspersky Security Center Cloud Console può richiedere la rimozione di software di terze parti incompatibile con l'applicazione da installare. Kaspersky Security Center Cloud Console offre diversi modi di rimuovere le applicazioni di terze parti.

Rimozione delle applicazioni incompatibili durante la configurazione dell'installazione remota di un'applicazione

È possibile abilitare l'opzione **Disinstalla automaticamente le applicazioni incompatibili** quando si configura l'installazione remota di un'applicazione di protezione. Questa opzione è disponibile nella Distribuzione guidata della protezione. Quando questa opzione è abilitata, Kaspersky Security Center Cloud Console consente di rimuovere le applicazioni incompatibili prima di installare un'applicazione di protezione in un dispositivo gestito.

Rimozione delle applicazioni incompatibili tramite un'attività dedicata

Per rimuovere le applicazioni incompatibili tramite un'attività, utilizzare l'attività **Disinstalla l'applicazione in remoto**. Questa attività deve essere eseguita nei dispositivi prima dell'attività di installazione dell'applicazione di protezione. Ad esempio, nell'attività di installazione è possibile selezionare il tipo di pianificazione **Al completamento di un'altra attività**, dove l'altra attività è **Disinstalla l'applicazione in remoto**.

Questo metodo di disinstallazione è consigliabile quando il programma di installazione dell'applicazione di protezione non è in grado di rimuovere correttamente un'applicazione incompatibile.

Opzioni per l'installazione manuale delle applicazioni

È possibile installare Network Agent nei dispositivi in locale senza coinvolgere Kaspersky Security Center Cloud Console. A tale scopo, creare un pacchetto di installazione indipendente autonomo per Network Agent come descritto nell'argomento seguente: Creazione di pacchetti di installazione indipendenti. Trasferire il pacchetto nel dispositivo client e installarlo. Una volta completata l'installazione di Network Agent, è possibile utilizzare il dispositivo come punto di distribuzione.

Distribuzione guidata della protezione

Per installare le applicazioni Kaspersky, è possibile utilizzare la Distribuzione guidata della protezione. La Distribuzione guidata della protezione consente l'installazione remota delle applicazioni con pacchetti di installazione creati appositamente o direttamente da un pacchetto di distribuzione.

La Distribuzione guidata della protezione esegue le seguenti operazioni:

- Download di un pacchetto di installazione per l'installazione dell'applicazione (se non è già stato creato). Il pacchetto di installazione è disponibile in **Individuazione e distribuzione → Distribuzione e assegnazione → Pacchetti di installazione**. È possibile utilizzare questo pacchetto di installazione per l'installazione dell'applicazione in futuro.

- Creazione ed esecuzione di un'attività di installazione remota per dispositivi specifici o per un gruppo di amministrazione. La nuova attività di installazione remota creata viene archiviata nella sezione **Attività**. È possibile avviare manualmente questa attività in un secondo momento. Il tipo di attività è **Installa l'applicazione in remoto**.

Avvio della Distribuzione guidata della protezione

Per avviare manualmente la Distribuzione guidata della protezione:

Nella finestra principale dell'applicazione, passare a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Distribuzione guidata della protezione**.

Verrà avviata la Distribuzione guidata della protezione. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

Passaggio 1. Selezione del pacchetto di installazione

Selezionare il pacchetto di installazione dell'applicazione che si desidera installare.

Se il pacchetto di installazione dell'applicazione desiderata non è elencato, fare clic sul pulsante **Aggiungi** e quindi selezionare l'applicazione dall'elenco.

Passaggio 2. Selezione della versione di Network Agent

Se è stato selezionato il pacchetto di installazione di un'applicazione diversa da Network Agent, è necessario installare anche Network Agent, che connette l'applicazione con Kaspersky Security Center Administration Server.

Selezionare la versione più recente di Network Agent.

Passaggio 3. Selezione dei dispositivi

Specificare un elenco di dispositivi in cui verrà installata l'applicazione:

- **Installa nei dispositivi gestiti**

  Se questa opzione è selezionata, l'attività di installazione remota viene creata per un gruppo di dispositivi.

- **Selezionare i dispositivi per l'installazione**

  L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

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

Nella pagina **Impostazioni attività "Installazione remota"** specificare le impostazioni per l'installazione remota dell'applicazione.

Nel gruppo di impostazioni **Forza il download del pacchetto di installazione** specificare la modalità di distribuzione dei file necessari per l'installazione dell'applicazione ai dispositivi client:

- **Utilizzando Network Agent**

  Se questa opzione è abilitata, i pacchetti di installazione vengono distribuiti ai dispositivi client da Network Agent installato nei dispositivi client.

  Se questa opzione è disabilitata, i pacchetti di installazione vengono distribuiti utilizzando gli strumenti del sistema operativo dei dispositivi client.

  È consigliabile abilitare questa opzione se l'attività è stata assegnata a dispositivi in cui sono installati Network Agent.

  Per impostazione predefinita, questa opzione è abilitata.

- **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**

  Se questa opzione è abilitata, i pacchetti di installazione verranno trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo tramite i punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete.

  Se l'opzione **Utilizzo di Network Agent** è abilitata, i file vengono inviati tramite gli strumenti del sistema operativo solo se gli strumenti di Network Agent non sono disponibili.

  Per impostazione predefinita, questa opzione è abilitata per le attività di installazione remota create in un Administration Server virtuale.

Definire l'impostazione aggiuntiva:

Non reinstallare l'applicazione se è già installata

Se questa opzione è abilitata, l'applicazione selezionata non verrà reinstallata se è già stata installata nel dispositivo client.

Se questa opzione è disabilitata, l'applicazione verrà installata in ogni caso.

Per impostazione predefinita, questa opzione è abilitata.

Passaggio 5. Gestione riavvio

Specificare l'azione da eseguire se il sistema operativo deve essere riavviato durante l'installazione dell'applicazione:

- **Non riavviare il dispositivo**

I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

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

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

  L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

  Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

  Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

  Per impostazione predefinita, questa opzione è disabilitata.

Passaggio 6. Rimozione delle applicazioni incompatibili prima dell'installazione

Questo passaggio è presente solo se l'applicazione da distribuire risulta incompatibile con alcune altre applicazioni.

Selezionare l'opzione se si desidera che Kaspersky Security Center Cloud Console rimuova automaticamente le applicazioni incompatibili con l'applicazione distribuita.

Viene visualizzato anche l'elenco delle applicazioni incompatibili.

Se non si seleziona questa opzione, l'applicazione verrà installata solo nei dispositivi in cui non sono presenti applicazioni incompatibili.

Passaggio 7. Spostamento dei dispositivi in Dispositivi gestiti

Specificare se i dispositivi devono essere spostati in un gruppo di amministrazione dopo l'installazione di Network Agent.

- **Non spostare i dispositivi**

  I dispositivi rimangono nei gruppi in cui si trovano attualmente. I dispositivi che non sono stati inseriti in alcun gruppo rimangono non assegnati.

- **Sposta i dispositivi non assegnati nel gruppo**

  I dispositivi vengono spostati nel gruppo di amministrazione selezionato.

L'opzione **Non spostare i dispositivi** è selezionata per impostazione predefinita. Per motivi di sicurezza, è consigliabile spostare i dispositivi manualmente.

Passaggio 8. Selezione degli account per l'accesso ai dispositivi

Se necessario, aggiungere gli account che verranno utilizzati per avviare l'attività di installazione remota:

- **Nessun account richiesto (Network Agent installato)**

  Se questa opzione è selezionata, non è necessario specificare un account con cui verrà eseguito il programma di installazione dell'applicazione. L'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

  Se Network Agent non è stato installato nei dispositivi client, questa opzione non è disponibile.

- **Account richiesto (Network Agent non utilizzato)**

Selezionare questa opzione se Network Agent non è installato nei dispositivi a cui si assegna l'attività di installazione remota. In questo caso, è possibile specificare un account utente per installare l'applicazione.

Per specificare l'account utente con cui verrà eseguito il programma di installazione dell'applicazione, fare clic sul pulsante **Aggiungi**, selezionare **Account locale** e quindi specificare le credenziali dell'account utente.

È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi per cui si assegna l'attività. In questo caso, tutti gli account aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

Passaggio 9. Avvio dell'installazione

Questo è il passaggio finale della procedura guidata. A questo punto, l'**Attività di installazione remota** è stata creata e configurata correttamente.

Per impostazione predefinita, l'opzione **Esegui l'attività al termine della procedura guidata** non è selezionata. Se si seleziona questa opzione, l'**Attività di installazione remota** verrà avviata immediatamente dopo il completamento della procedura guidata. Se non si seleziona questa opzione, l'**Attività di installazione remota** non verrà avviata. È possibile avviare manualmente questa attività in un secondo momento.

Fare clic su **OK** per completare il passaggio finale della Distribuzione guidata della protezione.

Impostazioni di rete per l'interazione con servizi esterni

Kaspersky Security Center Cloud Console utilizza le seguenti impostazioni di rete per l'interazione con i servizi esterni.

Impostazioni di rete

Impostazioni di rete	Indirizzo	Descrizione
Porta: 443 Protocollo: HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	Attivazione dell'applicazione.
Porta: 443 Protocollo: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com	Aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky.

	https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	
Porta: 443 Protocollo: HTTPS	https://downloads.upd.kaspersky.com	• Aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky. • Verifica dell'accessibilità dei server Kaspersky. Prima di scaricare i database e i moduli software di Kaspersky, Kaspersky Security Center Cloud Console verifica se i server Kaspersky sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici.
Porta: 80 Protocollo: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com	Aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky.

	http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	
Porta: 443 Protocollo: HTTPS	ds.kaspersky.com	Utilizzo di Kaspersky Security Network.
Porto: 443, 1443 Protocollo: HTTPS	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	Utilizzo di Kaspersky Security Network.
Protocollo: HTTPS	click.kaspersky.com redirect.kaspersky.com	Visita dei collegamenti sull'interfaccia.
Porta: 80 Protocollo: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Public Key Infrastructure (PKI).
Porta: 443 Protocollo: HTTPS	https://ipm-klca.kaspersky.com	Annunci di marketing.

Preparazione di un dispositivo in cui viene eseguito Astra Linux in modalità ambiente software chiuso per l'installazione di Network Agent

Prima di installare Network Agent in un dispositivo in cui viene esegue Astrito Linux in modalità ambiente software chiuso, è necessario eseguire due procedure di preparazione: quella nelle istruzioni riportate di seguito e i passaggi generali di preparazione per qualsiasi dispositivo Linux.

Prima di iniziare:

- Verificare che il dispositivo in cui si desidera installare Network Agent for Linux esegua una delle distribuzioni Linux supportate.
- Scaricare il file di installazione di Network Agent necessario dal sito Web di Kaspersky.

Eseguire i comandi presenti in questa istruzione con un account con privilegi di root.

Per preparare un dispositivo in cui viene eseguito Astra Linux in modalità ambiente software chiuso per l'installazione di Network Agent:

1. Aprire il file /etc/digsig/digsig_initramfs.conf, quindi specificare la seguente impostazione:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Nella riga di comando, eseguire il seguente comando per installare il pacchetto di compatibilità:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Creare una directory per la chiave dell'applicazione:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Posizionare la chiave dell'applicazione /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg nella directory creata nel passaggio precedente:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Se il kit di distribuzione di Kaspersky Security Center Cloud Console non include la chiave dell'applicazione kaspersky_astra_pub_key.gpg, è possibile scaricarla facendo clic sul collegamento: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Aggiornare i dischi RAM:

   ```
   update-initramfs -u -k all
   ```

   Riavviare il sistema.

6. Eseguire i passaggi di preparazione comuni per qualsiasi dispositivo Linux.

Il dispositivo è preparato. È ora possibile procedere all'installazione di Network Agent.

Preparazione di un dispositivo Linux e installazione di Network Agent in un dispositivo Linux da remoto

L'installazione di Network Agent comprende due passaggi:

- Una preparazione per il dispositivo Linux
- Installazione remota di Network Agent

Una preparazione per il dispositivo Linux

Per preparare un dispositivo Linux per l'installazione remota di Network Agent:

1. Accertarsi che il seguente software sia installato nel dispositivo Linux di destinazione.

   - Sudo
   - Interprete del linguaggio Perl versione 5.10 o successiva

2. Testare la configurazione del dispositivo:

   a. Verificare se è possibile connettersi al dispositivo tramite un client SSH (ad esempio, PuTTY).

      Se non è possibile connettersi al dispositivo, aprire il file /etc/ssh/sshd_config e verificare che per le seguenti impostazioni siano specificati i valori elencati:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > Non modificare il file /etc/ssh/sshd_config se è possibile connettersi al dispositivo senza problemi; in caso contrario, è possibile che si verifichi un errore di autenticazione SSH durante l'esecuzione di un'attività di installazione remota.

      Salvare il file (se necessario) e riavviare il servizio SSH utilizzando il comando `sudo service ssh restart`.

   b. Disabilitare la password sudo per l'account utente con cui deve essere eseguita la connessione del dispositivo.

   c. Utilizzare il comando `visudo` in sudo per aprire il file di configurazione sudoers.

      Nel file aperto, trovare la riga che inizia con `%sudo` (o con `%wheel` se si utilizza il sistema operativo CentOS). Sotto questa riga, specificare quanto segue: `<username> ALL = (ALL) NOPASSWD: ALL`. In questo caso, `<username>` è l'account utente che deve essere utilizzato per la connessione del dispositivo tramite SSH. Se si utilizza il sistema operativo Astra Linux, nel file /etc/sudoers aggiungere l'ultima riga con il seguente testo: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Salvare e chiudere il file sudoers.

   e. Eseguire di nuovo la connessione al dispositivo tramite SSH e verificare che il servizio Sudo non richieda l'immissione di una password. A tale scopo, utilizzare il comando `sudo whoami`.

3. Aprire il file /etc/systemd/logind.conf, quindi eseguire una delle seguenti operazioni:

   - Specificare "no" come valore per l'impostazione KillUserProcesses: `KillUserProcesses=no`.
   - Per l'impostazione KillExcludeUsers digitare il nome utente dell'account con il quale deve essere eseguita l'installazione remota, ad esempio, `KillExcludeUsers=root`.

   Se nel dispositivo di destinazione viene eseguito Astra Linux, aggiungere la stringa `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` nel file `/home/<nome utente>/.bashrc`, dove `<nome utente>` è l'account utente da utilizzare per la connessione del dispositivo tramite SSH.

   Per applicare l'impostazione modificata, riavviare il dispositivo Linux o eseguire il seguente comando:

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

4. Se si desidera installare Network Agent nei dispositivi con sistema operativo SUSE Linux Enterprise Server 15, installare il pacchetto insserv-compat prima di configurare Network Agent.

5. Se si desidera installare Network Agent nei dispositivi con il sistema operativo Astra Linux in esecuzione in modalità ambiente software chiuso, eseguire passaggi aggiuntivi per preparare i dispositivi Astra Linux.

Installazione remota di Network Agent

Per installare Network Agent nei dispositivi Linux da remoto:

1. Scaricare e creare un pacchetto di installazione:

   a. Prima di installare il pacchetto nel dispositivo, verificare di avere già installato tutte le dipendenze (programmi e librerie) per questo pacchetto.

   È possibile visualizzare le dipendenze per ciascun pacchetto autonomamente, utilizzando le utilità specifiche per la distribuzione Linux in cui deve essere installato il pacchetto. Per informazioni dettagliate sulle utilità, fare riferimento alla documentazione del sistema operativo.

   b. Scaricare il pacchetto di installazione di Network Agent utilizzando l'interfaccia dell'applicazione o dal sito Web di Kaspersky.

   c. Per creare un pacchetto di installazione remota, utilizzare i seguenti file:

   - klnagent.kpd
   - akinstall.sh
   - Pacchetto .deb o .rpm di Network Agent

2. Crea un'attività di installazione remota con le seguenti impostazioni:

   - Nella pagina **Impostazioni** della Creazione guidata nuova attività, selezionare la casella di controllo **Utilizzo delle risorse del sistema operativo tramite Administration Server**. Deselezionare tutte le altre caselle di controllo.
   - Nella pagina **Selezione di un account per l'esecuzione dell'attività**, specificare le impostazioni dell'account utente utilizzato per la connessione del dispositivo tramite SSH.

3. Eseguire l'attività di installazione remota. Utilizzare l'opzione per il comando `su` per preservare l'ambiente: `-m, -p, --preserve-environment`.

Se si installa Network Agent con SSH in dispositivi che eseguono versioni di Fedora precedenti alla 20, è possibile che venga restituito un errore. In questo caso, per la corretta installazione di Network Agent impostare come commento l'opzione Defaults requiretty (includerla nella sintassi del commento per rimuoverla dal codice analizzato) nel file /etc/sudoers. Per una descrizione dettagliata della condizione dell'opzione Defaults requiretty che può causare problemi durante la connessione SSH, fare riferimento al sito Web del bugtracker Bugzilla.

Mobile Device Management

La gestione della protezione per i dispositivi mobili tramite Kaspersky Security Center Cloud Console viene eseguita utilizzando la funzionalità Mobile Device Management. Per gestire i dispositivi mobili appartenenti ai dipendenti dell'organizzazione, abilitare e configurare Mobile Device Management.

Mobile Device Management consente di gestire i dispositivi Android dei dipendenti. La protezione è garantita dall'app mobile Kaspersky Security for Mobile installata nei dispositivi. Questa app mobile garantisce la protezione dei dispositivi mobili da minacce Web, virus e altri programmi che costituiscono una minaccia.

Per informazioni sulla gestione e sulla distribuzione della protezione dei dispositivi mobili, vedere la Guida di Kaspersky Security for Mobile.

Funzionalità di rilevamento e risposta

Questa sezione contiene informazioni sulle soluzioni Kaspersky che possono essere integrate in Kaspersky Security Center Cloud Console per aggiungere le funzionalità di rilevamento e risposta alla console.

Informazioni sulle funzionalità di rilevamento e risposta

Kaspersky Security Center Cloud Console può integrare le funzionalità di altre soluzioni Kaspersky nell'interfaccia della console. È ad esempio possibile aggiungere le funzionalità di rilevamento e risposta alla funzionalità di Kaspersky Security Center Cloud Console.

Le soluzioni di rilevamento e risposta sono progettate per proteggere l'infrastruttura IT di un'organizzazione da minacce informatiche complesse. La funzionalità delle soluzioni combina il rilevamento automatico delle minacce con la capacità di rispondere a queste minacce per resistere ad attacchi complessi, inclusi nuovi exploit, ransomware, attacchi senza file e metodi che utilizzano strumenti di sistema legittimi.

È possibile integrare le seguenti soluzioni:

- Kaspersky Endpoint Detection and Response Optimum

  Dopo che un'applicazione Kaspersky Endpoint Protection Platform (nota anche come EPP) rileva una minaccia, Kaspersky Security Center Cloud Console aggiunge un nuovo avviso all'elenco degli avvisi. Un avviso contiene informazioni dettagliate sulla minaccia rilevata e consente di analizzare e indagare sulla minaccia. È inoltre possibile visualizzare la minaccia creando un grafico della catena di sviluppo delle minacce. Il grafico descrive le fasi di distribuzione dell'attacco rilevato nel tempo.

  Come risposta, è possibile scegliere una delle azioni di risposta predefinite, ad esempio l'isolamento di un oggetto non attendibile, l'isolamento di un dispositivo compromesso dalla rete o la creazione di una regola di prevenzione dell'esecuzione per un oggetto non attendibile.

  Per informazioni sull'attivazione della soluzione, vedere la documentazione di Kaspersky Endpoint Detection and Response Optimum.

- Kaspersky Managed Detection and Response

  Dopo che un'applicazione Kaspersky EPP rileva una minaccia, Kaspersky Security Center Cloud Console aggiunge un nuovo incidente all'elenco degli incidenti. Un incidente contiene informazioni dettagliate sulla minaccia rilevata. Gli analisti MDR SOC (Security Operation Center) di Kaspersky o di un'azienda di terze parti indagano sugli incidenti e offrono risposte per risolverli. È possibile accettare o rifiutare le misure offerte manualmente o abilitare l'opzione per l'accettazione automatica di tutte le risposte.

  Per informazioni sull'attivazione della soluzione, vedere la documentazione di Kaspersky Managed Detection and Response.

- Kaspersky Endpoint Detection and Response Expert

  Si tratta di una soluzione per le organizzazioni che dispongono di un team di analisti SOC. Le minacce rilevate vengono registrate come avvisi o incidenti che possono essere assegnati agli analisti SOC per l'analisi. Kaspersky Endpoint Detection and Response Expert fornisce informazioni dettagliate su ciascun avviso o incidente, nonché gli strumenti per la gestione degli avvisi e degli incidenti, la ricerca delle minacce e lo sviluppo di regole personalizzate. Gli analisti SOC o i security officer possono selezionare manualmente le azioni di risposta oppure è possibile adottare le misure di risposta automatizzate predefinite.

  Per informazioni sull'attivazione della soluzione, vedere la documentazione di Kaspersky Endpoint Detection and Response Expert.

L'interfaccia cambia dopo l'integrazione delle funzionalità di rilevamento e risposta

Le seguenti soluzioni Kaspersky offrono funzionalità di rilevamento e risposta che possono essere integrate nell'interfaccia di Kaspersky Security Center Cloud Console:

- Kaspersky Endpoint Detection and Response (EDR) Optimum
- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response (EDR) Expert

La seguente tabella elenca le modifiche apportate dalle soluzioni nell'interfaccia di Kaspersky Security Center Cloud Console dopo l'integrazione.

Modifiche all'interfaccia apportate dalle soluzioni Kaspersky integrate

Soluzione	Modifiche in Kaspersky Security Center Cloud Console
Kaspersky EDR Optimum	Aggiunge i seguenti elementi: • Sezione **Alerts** (**Monitoraggio e generazione dei rapporti** → **Alerts**). Gli avvisi rilevati da questa soluzione vengono elencati nella scheda **Optimum**. • Un widget in **Dashboard** (**Monitoraggio e generazione dei rapporti** → **Dashboard**).
Kaspersky MDR	Aggiunge i seguenti elementi: • Sezione **MDR** (**Monitoraggio e generazione dei rapporti** → **MDR**). • L'opzione **Mostra funzionalità MDR** (**Impostazioni** → **Opzioni di interfaccia** → **Mostra funzionalità MDR**). • Un widget in **Dashboard** (**Monitoraggio e generazione dei rapporti** → **Dashboard**).
Kaspersky EDR Expert	Aggiunge i seguenti elementi: • Sezione **Alerts** (**Monitoraggio e generazione dei rapporti** → **Alerts**). Gli avvisi rilevati da questa soluzione vengono elencati nella scheda **Expert**. • Sezione **Incidents** (**Monitoraggio e generazione dei rapporti** → **Incidents**). • Sezione **Threat hunting** (**Monitoraggio e generazione dei rapporti** → **Threat hunting**). • Sezione **Custom rules** (**Monitoraggio e generazione dei rapporti** → **Custom rules**). • Impostazioni generali di Kaspersky EDR Expert (**Impostazioni** → **Integrazione** → **Kaspersky EDR Expert**). • Widget in **Dashboard** (**Monitoraggio e generazione dei rapporti** → **Dashboard**).

Individuazione dei dispositivi nella rete e creazione di gruppi di amministrazione

Questa sezione descrive la ricerca e l'individuazione dei dispositivi nella rete, nonché la creazione di gruppi di amministrazione per tali dispositivi.

Kaspersky Security Center Cloud Console consente di individuare i dispositivi sulla base dei criteri specificati. È possibile salvare i risultati della ricerca in un file di testo.

La funzionalità di ricerca e individuazione consente di trovare i seguenti dispositivi:

- I dispositivi gestiti nei gruppi di amministrazione dell'Administration Server di Kaspersky Security Center Cloud Console e nei relativi Administration Server secondari.
- I dispositivi non assegnati gestiti dall'Administration Server di Kaspersky Security Center Cloud Console e dai relativi Administration Server secondari.

Scenario: Individuazione dei dispositivi nella rete

È necessario eseguire l'individuazione dispositivi prima della distribuzione iniziale delle applicazioni di protezione. Quando vengono individuati tutti i dispositivi della rete, è possibile ottenere informazioni in merito e gestirli tramite i criteri. Il polling periodico della rete è necessario per scoprire se sono presenti nuovi dispositivi e se i dispositivi individuati in precedenza sono ancora in rete.

Una volta completato lo scenario, verrà configurata l'individuazione dispositivi che verrà eseguita in base alla pianificazione specificata.

Prerequisiti

In Kaspersky Security Center Cloud Console l'individuazione dispositivi viene eseguita dai punti di distribuzione. Prima di iniziare, procedere come segue:

- Decidere quali dispositivi fungeranno da punti di distribuzione.
- Installare i Network Agent nei dispositivi selezionati.
- Assegnare manualmente ai dispositivo il ruolo di punto di distribuzione.

Passaggi

Lo scenario procede per fasi:

1. **Scelta dei tipi di individuazione**

   Decidere quali tipi di individuazione si desidera utilizzare regolarmente.

2. **Configurazione dei polling**

   Nelle proprietà di ogni punto di distribuzione abilitare e configurare i tipi di polling della rete selezionati: polling della rete Windows, polling del controller di dominio o polling degli intervalli IP. Verificare che la pianificazione del polling soddisfi le esigenze dell'organizzazione.

Se i dispositivi in rete sono inclusi in un dominio, è consigliabile utilizzare il polling del controller di dominio.

3. **Configurazione delle regole per l'aggiunta dei dispositivi individuati nei gruppi di amministrazione (opzione facoltativa)**

   Se vengono visualizzati nuovi dispositivi nella rete, questi vengono individuati durante il polling periodico e vengono automaticamente inclusi nel gruppo **Dispositivi non assegnati**. Se si desidera, è possibile configurare le regole per lo spostamento automatico di questi dispositivi nel gruppo **Dispositivi gestiti**. È inoltre possibile definire le regole di conservazione.

   Se si ignora questo passaggio di configurazione delle regole, tutti i dispositivi individuati passano al gruppo **Dispositivi non assegnati** e rimangono in tale gruppo. Se si desidera, è possibile spostare questi dispositivi nel gruppo **Dispositivi gestiti** manualmente. Se si spostano manualmente i dispositivi nel gruppo **Dispositivi gestiti**, è possibile analizzare le informazioni su ciascun dispositivo, decidere se spostarlo in un gruppo di amministrazione e, in tal caso, in quale gruppo.

Al termine di un'operazione di polling della rete, verificare che i nuovi dispositivi individuati siano disposti in base alle regole configurate. Se non è configurata alcuna regola, i dispositivi rimangono nel gruppo **Dispositivi non assegnati**.

Polling della rete

Le informazioni sulla struttura della rete e i dispositivi al suo interno vengono ricevute da Kaspersky Security Center Cloud Consone tramite il polling periodico della rete Windows, degli intervalli IP, del controller di dominio Microsoft di Active Directory e un controller di dominio di Samba. Per un controller di dominio Samba, Samba 4 viene utilizzato come controller di dominio Active Directory. Il polling della rete può essere avviato manualmente o automaticamente in base a una pianificazione.

Sulla base dei risultati di questo polling, Kaspersky Security Center Cloud Console aggiorna l'elenco dei dispositivi non assegnati. È inoltre possibile configurare le regole per i nuovi dispositivi individuati da spostare automaticamente nei gruppi di amministrazione.

Kaspersky Security Center Cloud Console utilizza i seguenti metodi di polling della rete:

- *Polling intervallo IP*. Kaspersky Security Center Cloud Console esegue il polling degli intervalli IP specificati utilizzando pacchetti ICMP (Internet Control Message Protocol) e compila un set completo di dati sui dispositivi all'interno degli intervalli IP.

- *Polling della rete Windows*. È possibile eseguire due tipi di polling della rete Windows: veloce o completo. Durante un polling veloce Kaspersky Security Center Cloud Console recupera informazioni solo dall'elenco dei nomi dei dispositivi NetBIOS in tutti i domini di rete e i gruppi di lavoro. Durante un polling completo vengono richieste le seguenti informazioni da ogni dispositivo: nome del sistema operativo, indirizzo IP, nome DNS e nome NetBIOS.

- *Polling dei controller di dominio*. Le informazioni sulla struttura delle unità Active Directory e sui nomi DNS dei dispositivi dai gruppi Active Directory sono registrate nel database di Kaspersky Security Center Cloud Console.

I risultati del polling sono mostrati nella sezione **Individuazione e distribuzione** → **Individuazione** separatamente per i metodi di *polling di rete di Windows* e *polling dei controller di dominio*.

I risultati del polling per il metodo *di polling dell'intervallo IP* sono visualizzati nella sezione **Individuazione e distribuzione** → **Dispositivi non assegnati**.

È possibile visualizzare un dispositivo in più di un'area di rilevamento. Se viene rilevato un dispositivo nel dominio HQ e il suo indirizzo è 192.168.0.1, il dispositivo verrà visualizzato sia nella sezione **Domini Windows** che nella nella sezione **Dispositivi non assegnati**. È possibile modificare le impostazioni di polling della rete per ciascun metodo di polling. È ad esempio possibile modificare la pianificazione del polling o impostare l'esecuzione del polling solo di un dominio specifico o dell'intera foresta Active Directory.

Polling della rete Windows

Informazioni sul polling della rete Windows

Durante un polling rapido Administration Server recupera informazioni solo dall'elenco dei nomi di dispositivi NetBIOS in tutti i domini di rete e i gruppi di lavoro. Durante un polling completo sono richieste le seguenti informazioni da ogni dispositivo client:

- Nome del sistema operativo
- Indirizzo IP
- Nome DNS
- Nome NetBIOS

Sia il polling rapido che quello completo richiedono le seguenti operazioni:

- Le porte UDP 137/138, TCP 139 devono essere disponibili nella rete.
- È necessario utilizzare il servizio Microsoft Computer Browser e il computer del browser principale deve essere abilitato nel punto di distribuzione.
- È necessario utilizzare il servizio Microsoft Computer Browser e il computer del browser primario deve essere abilitato nei dispositivi client:
  - In almeno un dispositivo, se il numero di dispositivi della rete non è superiore a 32.
  - In almeno un dispositivo ogni 32 dispositivi della rete.

Il polling completo può essere eseguito solo se il polling rapido è stato eseguito almeno una volta.

Visualizzazione e modifica delle impostazioni per il polling della rete Windows

Per modificare le proprietà del polling della rete Windows:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Fare clic sul nome del punto di distribuzione che si desidera utilizzare per eseguire il polling della rete.

   Verrà visualizzata la finestra delle proprietà del punto di distribuzione.

4. Seleziona la sezione **Polling domini Windows**.

5. Abilitare o disabilitare il polling della rete Windows utilizzando l'interruttore **Consenti il polling della rete**.

6. Configurare la pianificazione per il polling rapido e il polling completo.

7. Fare clic sul pulsante **OK**.

Le proprietà verranno salvate e applicate a tutti i domini e i gruppi di lavoro di Windows rilevati.

Polling del controller di dominio

Kaspersky Security Center Cloud Console supporta il polling di un controller di dominio Microsoft Active Directory e di un controller di dominio Samba. Per un controller di dominio Samba, Samba 4 viene utilizzato come controller di dominio Active Directory. Quando si esegue il polling di un controller di dominio o un punto di distribuzione recupera le informazioni sulla struttura del dominio, sugli account utente, sui gruppi di protezione e sui nomi DNS dei dispositivi inclusi nel dominio. Il polling del controller di dominio viene eseguito in base a una pianificazione impostata.

Prerequisiti

Prima di eseguire il polling di un controller di dominio, assicurarsi che i seguenti protocolli siano abilitati:

- Simple Authentication and Security Layer (SASL)
- Lightweight Directory Access Protocol (LDAP)

Verificare che le seguenti porte siano disponibili nel dispositivo del controller di dominio:

- 389 per SASL
- 636 per TLS

Polling del controller di dominio utilizzando un punto di distribuzione

È inoltre possibile eseguire il polling di un controller di dominio utilizzando un punto di distribuzione. Un dispositivo gestito basato su Windows o Linux può fungere da punto di distribuzione.

Per un punto di distribuzione Linux, sono supportati il polling di un controller di dominio Microsoft Active Directory e di un controller di dominio Samba.
Per un punto di distribuzione Windows, è supportato solo il polling di un controller di dominio Microsoft Active Directory.
Il polling con un punto di distribuzione Mac non è supportato.

Per configurare il polling del controller di dominio utilizzando il punto di distribuzione:

1. Aprire le proprietà del punto di distribuzione.

2. Selezionare la sezione **Polling del controller di dominio**.

3. Selezionare l'opzione **Abilita polling controller di dominio**.

4. Selezionare il controller di dominio di cui si desidera eseguire il polling.

   Se si utilizza un punto di distribuzione Linux, nella sezione **Esegui polling di domini specifici**, fare clic su **Aggiungi**, quindi specificare l'indirizzo e le credenziali utente del controller di dominio.

   Se si utilizza un punto di distribuzione Windows, è possibile selezionare una delle seguenti opzioni:

   - **Esegui polling dominio corrente**
   - **Esegui polling di tutta la foresta di dominio**
   - **Esegui polling di domini specifici**

5. Fare clic sul pulsante **Imposta pianificazione di polling** per specificare le opzioni di pianificazione del polling, se necessario.

   Il polling viene avviato solo in base alla pianificazione specificata. L'avvio manuale del polling non è disponibile.

Al termine del polling, la struttura del dominio verrà visualizzata nella sezione **Controller di dominio**.

Se sono installate e attivate le regole di spostamento dei dispositivi, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi gestiti**. Se non sono state abilitate regole di spostamento, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi non assegnati**.

Gli account utente rilevati possono essere utilizzati per l'autenticazione del dominio in Kaspersky Security Center Cloud Console.

Visualizzazione dei risultati del polling del controller di dominio

Per visualizzare i risultati del polling del controller di dominio:

1. Nel menu principale, passare a **Individuazione e distribuzione** → **Individuazione** → **Controller di dominio**.

   Verrà visualizzato l'elenco delle unità organizzative rilevate.

2. Selezionare un'unità organizzativa, quindi fare clic sul pulsante **Dispositivi**.

   Verrà visualizzato l'elenco dei dispositivi nell'unità organizzativa.

È possibile eseguire ricerche nell'elenco e filtrare i risultati.

Polling intervallo IP

Kaspersky Security Center Cloud Console tenta di eseguire la risoluzione inversa dei nomi per ogni indirizzo nell'intervallo specificato a un nome DNS utilizzando richieste DNS standard. Se questa operazione riesce, il server invia un messaggio `ICMP ECHO REQUEST` (equivalente al comando ping) al nome ricevuto. Se il dispositivo risponde, le informazioni su di esso vengono aggiunte al database di Kaspersky Security Center Cloud Console. La risoluzione inversa dei nomi è necessaria per escludere i dispositivi di rete che possono avere un indirizzo IP ma che non sono computer, ad esempio stampanti o router di rete.

Questo metodo di polling si basa su un servizio DNS locale configurato correttamente. Deve essere presente una zona di ricerca inversa. Se questa zona non è configurata, il polling della subnet IP non produrrà risultati. Nelle reti in cui è utilizzato Active Directory tale zona viene mantenuta automaticamente. In queste reti, tuttavia, il polling della subnet IP non fornisce più informazioni del polling di Active Directory. Inoltre, gli amministratori delle reti di piccole dimensioni spesso non configurano la zona di ricerca inversa perché non è necessaria per il lavoro di molti servizi di rete. Per tali motivi, il polling della subnet IP è disabilitato per impostazione predefinita.

Inizialmente Kaspersky Security Center Cloud Console ottiene gli intervalli IP per il polling dalle impostazioni di rete del dispositivo del punto di distribuzione utilizzato per il polling della rete. Se l'indirizzo del dispositivo è 192.168.0.1 e la subnet mask è 255.255.255.0, Kaspersky Security Center Cloud Console include automaticamente la rete 192.168.0.0/24 nell'elenco degli indirizzi di polling. Kaspersky Security Center Cloud Console esegue il polling di tutti gli indirizzi da 192.168.0.1 a 192.168.0.254.

Non è consigliabile utilizzare il polling degli intervalli IP se si utilizza il polling di rete Windows e/o il polling di Active Directory.

Visualizzazione e modifica delle impostazioni per il polling degli intervalli IP

Per visualizzare e modificare le proprietà per il polling degli intervalli IP:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Fare clic sul nome del punto di distribuzione che si desidera utilizzare per eseguire il polling della rete.

   Verrà visualizzata la finestra delle proprietà del punto di distribuzione.

4. Selezionare la sezione **Polling intervalli IP**.

5. Abilitare o disabilitare il polling IP utilizzando l'interruttore **Abilita polling intervalli**.

6. Configurare la pianificazione del polling. Per impostazione predefinita, il polling IP viene eseguito ogni 420 minuti (sette ore).

7. Se necessario, modificare gli intervalli IP di cui eseguire il polling.

   Quando si specifica l'intervallo di polling, verificare che questa impostazione non superi il valore del parametro di durata dell'indirizzo IP. Se un indirizzo IP non viene verificato tramite il polling durante la durata dell'indirizzo IP, tale indirizzo IP viene automaticamente rimosso dai risultati del polling. Per impostazione predefinita, la durata dei risultati del polling è di 24 ore, poiché gli indirizzi IP dinamici, ovvero assegnati tramite il protocollo DHCP (Dynamic Host Configuration Protocol), cambiano ogni 24 ore.

8. Fare clic sul pulsante **OK**.

Le proprietà verranno salvate e applicate a tutti gli intervalli IP.

Configurazione di un controller di dominio Samba

Kaspersky Security Center Cloud Console supporta un controller di dominio Linux in esecuzione solo su Samba 4.

Un controller di dominio Samba supporta le stesse estensioni dello schema di un controller di dominio Microsoft Active Directory. È possibile abilitare la piena compatibilità di un controller di dominio Samba con un controller di dominio Microsoft Active Directory utilizzando l'estensione dello schema Samba 4. Questa è un'azione facoltativa.

Si consiglia di abilitare la piena compatibilità di un controller di dominio Samba con un controller di dominio Microsoft Active Directory. In questo modo, si assicurerà la corretta interazione tra Kaspersky Security Center Cloud Console e il controller di dominio Samba.

Per abilitare la piena compatibilità di un controller di dominio Samba con un controller di dominio Microsoft Active Directory:

1. Eseguire il seguente comando per utilizzare l'estensione dello schema RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Abilitare l'aggiornamento dello schema in un controller di dominio Samba. A tale scopo, aggiungere la seguente riga al file /etc/samba/smb.conf:

   ```
   dsdb:schema update allowed = true
   ```

   Se l'aggiornamento dello schema viene completato con un errore, è necessario eseguire un ripristino completo del controller di dominio che funge da master dello schema.

Se si desidera eseguire correttamente il polling di un controller di dominio Samba, è necessario specificare il `netbios name` e i parametri del `workgroup` nel file /etc/samba/smb.conf.

Aggiunta e modifica di un intervallo IP

Inizialmente Kaspersky Security Center Cloud Console ottiene gli intervalli IP per il polling dalle impostazioni di rete del dispositivo del punto di distribuzione utilizzato per il polling della rete. Se l'indirizzo del dispositivo è 192.168.0.1 e la subnet mask è 255.255.255.0, Kaspersky Security Center Cloud Console include automaticamente la rete 192.168.0.0/24 nell'elenco degli indirizzi di polling. Kaspersky Security Center Cloud Console esegue il polling di tutti gli indirizzi da 192.168.0.1 a 192.168.0.254. È possibile modificare gli intervalli IP definiti automaticamente o aggiungere intervalli IP personalizzati.

Per aggiungere un nuovo intervallo IP:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Fare clic sul nome del punto di distribuzione che si desidera utilizzare per eseguire il polling della rete.

   Verrà visualizzata la finestra delle proprietà del punto di distribuzione.

4. Selezionare la sezione **Polling intervalli IP**.

5. Per aggiungere un nuovo intervallo IP, fare clic sul pulsante **Aggiungi**.

6. Nella finestra visualizzata specificare le seguenti impostazioni:

- **Nome**

  Nome dell'intervallo IP. È possibile specificare l'intervallo IP stesso come nome, ad esempio "192.168.0.0/24".

- **Intervallo IP o indirizzo subnet e subnet mask**

  Impostare l'intervallo IP specificando gli indirizzi IP iniziale e finale o l'indirizzo subnet e la subnet mask. È possibile aggiungere tutte le subnet necessarie. Gli intervalli IP denominati non possono sovrapporsi, ma le subnet non denominate all'interno di un intervallo IP non presentano tali restrizioni.

- **Durata dell'indirizzo IP (ore)**

  Quando si specifica questo parametro, assicurarsi che superi l'intervallo di polling impostato nella pianificazione del polling. Se un indirizzo IP non viene verificato tramite il polling durante la durata dell'indirizzo IP, tale indirizzo IP viene automaticamente rimosso dai risultati del polling. Per impostazione predefinita, la durata dei risultati del polling è di 24 ore, poiché gli indirizzi IP dinamici, ovvero assegnati tramite il protocollo DHCP (Dynamic Host Configuration Protocol), cambiano ogni 24 ore.

7. Fare clic sul pulsante **OK**.

Il nuovo intervallo IP verrà aggiunto all'elenco degli intervalli IP.

Al termine del polling, è possibile visualizzare l'elenco dei dispositivi rilevati utilizzando il pulsante **Dispositivi**. Per impostazione predefinita, la durata dei risultati del polling è di 24 ore ed è uguale all'impostazione per la durata dell'indirizzo IP.

Regolazione di punti di distribuzione e gateway di connessione

Una struttura di gruppi di amministrazione in Kaspersky Security Center Cloud Console esegue le seguenti funzioni:

- Imposta l'ambito dei criteri

  È disponibile un metodo alternativo per l'applicazione delle impostazioni appropriate nei dispositivi, utilizzando i *profili criterio*. In questo caso, l'ambito dei criteri viene definito con tag, posizioni dei dispositivi nelle unità organizzative di Active Directory, appartenenza a gruppi di protezione di Active Directory e così via.

- Imposta l'ambito delle attività di gruppo

  Esiste un approccio alla definizione dell'ambito delle attività di gruppo che non è basato su una gerarchia di gruppi di amministrazione: l'utilizzo di attività per selezioni dispositivi e di attività per dispositivi specifici.

- Imposta i diritti di accesso a dispositivi e Administration Server secondari

- Assegna i punti di distribuzione

Al momento della creazione della struttura dei gruppi di amministrazione, è necessario tenere conto della topologia della rete dell'organizzazione per l'assegnazione ottimale dei punti di distribuzione. La distribuzione ottimale dei punti di distribuzione consente di ridurre il traffico nella rete dell'organizzazione.

A seconda dello schema dell'organizzazione e della topologia di rete, le seguenti configurazioni standard possono essere applicate alla struttura dei gruppi di amministrazione:

- Singola sede
- Più sedi remote di piccole dimensioni

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Calcolo del numero e configurazione dei punti di distribuzione

Più dispositivi client contiene una rete, maggiore è il numero dei punti di distribuzione richiesti. Utilizzare le seguenti tabelle per calcolare il numero di punti di distribuzione richiesti per la rete in uso.

Verificare che i dispositivi che si prevede di utilizzare come punti di distribuzione dispongano di un volume sufficiente di spazio libero su disco, che non vengano arrestati regolarmente e che la modalità di sospensione sia disabilitata.

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–100	1
Più di 100	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Utilizzo di dispositivi client standard (workstation) come punti di distribuzione

Se si prevede di utilizzare dispositivi client standard (ovvero, workstation) come punti di distribuzione, è consigliabile assegnare i punti di distribuzione come indicato nelle tabelle seguenti per evitare un carico eccessivo sui canali di comunicazione e su Administration Server:

Numero di workstation che operano come punti di distribuzione in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Numero di workstation che operano come punti di distribuzione in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)

10–30	1
31–300	2
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Se non è disponibile un punto di distribuzione, valutare se aggiornare i database, i moduli software e le applicazioni Kaspersky manualmente o direttamente dai server di aggiornamento Kaspersky.

Configurazione standard dei punti di distribuzione: singola sede

In una configurazione standard con una singola sede, tutti i dispositivi si trovano nella rete dell'organizzazione e sono visibili reciprocamente. La rete dell'organizzazione può comprendere diversi componenti (reti o segmenti di rete) connessi tramite canali con larghezza di banda ridotta.

Sono disponibili i seguenti metodi per creare la struttura dei gruppi di amministrazione:

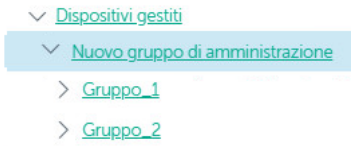
- Creazione della struttura dei gruppi di amministrazione tenendo conto della topologia di rete. La struttura dei gruppi di amministrazione potrebbe non riflettere la topologia di rete alla perfezione. Una corrispondenza tra i diversi componenti della rete e alcuni gruppi di amministrazione può essere sufficiente.

- Creazione della struttura dei gruppi di amministrazione senza tenere conto della topologia di rete. In questo caso è necessario assegnare a uno o più dispositivi il ruolo di punti di distribuzione per un gruppo di amministrazione radice in ciascun componente della rete, ad esempio per il gruppo **Dispositivi gestiti**. Tutti i punti di distribuzione saranno allo stesso livello e avranno lo stesso ambito che comprende tutti i dispositivi della rete dell'organizzazione. In questo caso, tutti i Network Agent si connetteranno al punto di distribuzione con il percorso più vicino. Il percorso di un punto di distribuzione è monitorabile con l'utilità tracert.

Configurazione standard dei punti di distribuzione: più sedi remote di piccole dimensioni

Questa configurazione standard prevede la presenza di diverse sedi remote, che possono comunicare con la sede centrale via Internet. Ogni sede remota è situata dietro il NAT, ovvero la connessione da una sede remota all'altra non è possibile perché le sedi sono isolate tra loro.

La configurazione deve essere riflessa nella struttura dei gruppi di amministrazione: è necessario creare un gruppo di amministrazione distinto per ogni sede remota (i gruppi **Sede 1** e **Sede 2** nella figura seguente).



Le sedi remote sono incluse nella struttura dei gruppi di amministrazione

È necessario assegnare uno o più punti di distribuzione a ogni gruppo di amministrazione che corrisponde a una sede. I punti di distribuzione devono essere dispositivi nella sede remota con una quantità sufficiente di spazio libero su disco. I dispositivi distribuiti nel gruppo **Sede 1**, ad esempio, accederanno ai punti di distribuzione assegnati al gruppo di amministrazione **Sede 1**.

Se alcuni utenti si spostano fisicamente tra le sedi con i loro computer portatili, è necessario selezionare due o più dispositivi (oltre ai punti di distribuzione esistenti) in ogni sede remota e assegnare loro il ruolo di punti di distribuzione per un gruppo di amministrazione di primo livello (**Gruppo radice per le sedi** nella figura precedente).

Esempio: un computer portatile è distribuito nel gruppo di amministrazione **Sede 1** e quindi viene spostato fisicamente nella sede che corrisponde al gruppo di amministrazione **Sede 2**. Dopo lo spostamento del portatile, Network Agent tenta di accedere ai punti di distribuzione assegnati al gruppo **Sede 1**, ma tali punti di distribuzione non sono disponibili. Network Agent inizia quindi a tentare di accedere ai punti di distribuzione che sono stati assegnati al **Gruppo radice per le sedi**. Poiché le sedi remote sono isolate tra loro, i tentativi di accedere ai punti di distribuzione assegnati al gruppo di amministrazione **Gruppo radice per le sedi** avranno esito positivo solo quando Network Agent tenta di accedere ai punti di distribuzione nel gruppo **Sede 2**. In altre parole, il computer portatile rimarrà nel gruppo di amministrazione che corrisponde alla sede iniziale, ma utilizzerà il punto di distribuzione della sede in cui si trova fisicamente al momento.

Assegnazione manuale di punti di distribuzione

Kaspersky Security Center Cloud Console consente di assegnare manualmente ai dispositivi il ruolo di punti di distribuzione. È consigliabile calcolare il numero e la configurazione dei punti di distribuzione richiesti per la rete.

I dispositivi dei punti di distribuzione che eseguono macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky.

Se uno o più dispositivi che eseguono macOS rientrano nell'ambito dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'attività viene completata con lo stato *Non riuscito*, anche se è stata completata correttamente in tutti i dispositivi Windows.

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Per assegnare manualmente a un dispositivo il ruolo di punto di distribuzione:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Fare clic sul pulsante **Assegna**.

4. Selezionare il dispositivo che si desidera rendere un punto di distribuzione.

   Quando si seleziona un dispositivo, tenere presenti le funzionalità operative dei punti di distribuzione e i requisiti definiti per il dispositivo che opera come punto di distribuzione.

5. Selezionare il gruppo di amministrazione da includere nell'ambito del punto di distribuzione selezionato.

6. Fare clic sul pulsante **Aggiungi**.

   Il punto di distribuzione aggiunto sarà visualizzato nell'elenco dei punti di distribuzione, nella sezione **Punti di distribuzione**.

7. Selezionare il nuovo punto di distribuzione aggiunto nell'elenco per aprire la relativa finestra delle proprietà.

8. Configurare il punto di distribuzione nella finestra delle proprietà:

- La sezione **Generale** contiene le impostazioni per l'interazione tra il punto di distribuzione e i dispositivi client:

  - **Porta SSL**

    Numero della porta SSL per la connessione criptata tra i dispositivi client e il punto di distribuzione tramite SSL.

    Per impostazione predefinita, viene utilizzata la porta 13000.

  - **Usa multicast**

    Se questa opzione è abilitata, verrà utilizzata la modalità IP multicast per la distribuzione automatica dei pacchetti di installazione ai dispositivi client del gruppo.

    Il multicast IP riduce il tempo necessario per installare un'applicazione da un pacchetto di installazione in un gruppo di dispositivi client, ma aumenta il tempo di installazione quando si installa un'applicazione in un singolo dispositivo client.

  - **Indirizzo IP multicast**

    Indirizzo IP che verrà utilizzato per la modalità multicast. È possibile definire un indirizzo IP nell'intervallo da 224.0.0.0 a 239.255.255.255

    Per impostazione predefinita Kaspersky Security Center Cloud Console assegna automaticamente un indirizzo IP multicast univoco all'interno dell'intervallo specificato.

  - **Numero di porta IP multicast**

    Numero di porta per la modalità IP multicast.

    Il numero di porta predefinito è 15001. Se il dispositivo in cui è installato Administration Server è specificato come punto di distribuzione, per impostazione predefinita viene utilizzata la porta 13001 per la connessione SSL.

  - **Distribuisci aggiornamenti**

    Gli aggiornamenti vengono distribuiti ai dispositivi gestiti dalle seguenti sorgenti:

    - Questo punto di distribuzione se l'opzione è abilitata.
    - Altri punti di distribuzione, Administration Server o server degli aggiornamenti Kaspersky se l'opzione è disabilitata.

    Se si utilizzano i punti di distribuzione per distribuire gli aggiornamenti, è possibile risparmiare traffico riducendo il numero di download. È inoltre possibile alleggerire il carico su Administration Server e ridistribuirlo tra i punti di distribuzione. È possibile calcolare il numero di punti di distribuzione per la propria rete in modo da ottimizzare il traffico e il carico.

    Se si disabilita questa opzione, il numero di download degli aggiornamenti e il carico su Administration Server potrebbero aumentare. Per impostazione predefinita, questa opzione è abilitata.

  - **Distribuisci pacchetti di installazione**

I pacchetti di installazione vengono distribuiti ai dispositivi gestiti dalle seguenti sorgenti:

- Questo punto di distribuzione se l'opzione è abilitata.
- Altri punti di distribuzione, Administration Server o server degli aggiornamenti Kaspersky se l'opzione è disabilitata.

Se si utilizzano i punti di distribuzione per distribuire i pacchetti di installazione, è possibile risparmiare traffico riducendo il numero di download. È inoltre possibile alleggerire il carico su Administration Server e ridistribuirlo tra i punti di distribuzione. È possibile calcolare il numero di punti di distribuzione per la propria rete in modo da ottimizzare il traffico e il carico.

Se si disabilita questa opzione, il numero di download dei pacchetti di installazione e il carico su Administration Server potrebbero aumentare. Per impostazione predefinita, questa opzione è abilitata.

- **Esegui server push**

  In Kaspersky Security Center Cloud Console, un punto di distribuzione può fungere da server push per i dispositivi basati su Windows e Linux gestiti da Network Agent. Un server push ha lo stesso ambito dei dispositivi gestiti del punto di distribuzione in cui è abilitato il server push. Se sono stati assegnati più punti di distribuzione per lo stesso gruppo di amministrazione, è possibile abilitare il server push in ciascuno dei punti di distribuzione. In questo caso, Administration Server bilancia il carico tra i punti di distribuzione.

- **Porta server push**

  Il numero di porta per il server push. È possibile specificare il numero di qualsiasi porta non occupata.

- Nella sezione **Ambito** specificare l'ambito in cui il punto di distribuzione distribuirà gli aggiornamenti (gruppi di amministrazione e/o percorso di rete).

  Solo i dispositivi con un sistema operativo Windows possono determinare il percorso di rete. Non è possibile determinare il percorso di rete per i dispositivi che eseguono altri sistemi operativi.

- Nella sezione **Proxy KSN** è possibile configurare l'applicazione per l'utilizzo del punto di distribuzione per l'inoltro delle richieste KSN dai dispositivi gestiti:

  Abilita proxy KSN da parte del punto di distribuzione

Il servizio proxy KSN viene eseguito nel dispositivo utilizzato come punto di distribuzione. Utilizzare questa funzionalità per ridistribuire e ottimizzare il traffico nella rete.

Questa funzionalità non è supportata dai dispositivi dei punti di distribuzione che eseguono Linux o macOS.

Il punto di distribuzione invia le statistiche KSN, elencate nell'informativa di Kaspersky Security Network, a Kaspersky. Per impostazione predefinita, l'informativa KSN è disponibile in %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Per impostazione predefinita, questa opzione è disabilitata. L'attivazione di questa opzione ha effetto solo se l'opzione **Accetto di utilizzare Kaspersky Security Network** è abilitata nella finestra delle proprietà di Administration Server.

È possibile assegnare il nodo di un cluster attivo-passivo a un punto di distribuzione e abilitare il proxy KSN in tale nodo.

- Configurare il polling dei domini Windows, di Active Directory e degli intervalli IP da parte del punto di distribuzione:
  - Polling domini Windows

    È possibile abilitare la device discovery per i domini Windows e impostare la pianificazione per l'individuazione.

  - Active Directory

    È possibile abilitare il polling della rete per Active Directory e impostare la pianificazione per il polling.

    Se si utilizza un punto di distribuzione Windows, è possibile selezionare una delle seguenti opzioni:

    - **Esegui il polling del dominio Active Directory corrente**.
    - **Esegui il polling della foresta di dominio Active Directory**.
    - **Esegui il polling dei domini Active Directory selezionati**. Se si seleziona questa opzione, aggiungere uno o più domini Active Directory all'elenco.

    Se si utilizza un punto di distribuzione Linux con Network Agent versione 15 installato, è possibile eseguire il polling solo dei domini Active Directory per i quali si specificano l'indirizzo e le credenziali utente. Il polling del dominio Active Directory corrente e della foresta di domini Active Directory non è disponibile.

  - Polling intervalli IP

Adesso è possibile abilitare Device discovery per gli intervalli IPv4 e le reti IPv6.

Se si abilita l'opzione **Abilita polling intervalli**, è possibile aggiungere gli intervalli esaminati e impostare la relativa pianificazione. È possibile aggiungere intervalli IP all'elenco degli intervalli esaminati.

Se si abilita l'opzione **Usa Zeroconf per il polling delle reti IPv6**, il punto di distribuzione esegue automaticamente il polling della rete IPv6 utilizzando le reti zero-configuration (definite anche *Zeroconf*). In questo caso, gli intervalli IP specificati vengono ignorati perché il punto di distribuzione esegue il polling dell'intera rete. L'opzione **Usa Zeroconf per il polling delle reti IPv6** è disponibile se nel punto di distribuzione viene eseguito Linux. Per utilizzare il polling ipv6 Zeroconf, è necessario installare l'utilità avahi-browse nel punto di distribuzione.

- Nella sezione **Avanzate** specificare la cartella che il punto di distribuzione deve utilizzare per archiviare i dati distribuiti:
  - **Usa cartella predefinita**

    Se questa opzione è selezionata, l'applicazione utilizza la cartella di installazione di Network Agent nel punto di distribuzione.

  - **Usa cartella specificata**

    Se questa opzione è selezionata, nel campo sottostante è possibile specificare il percorso della cartella. È possibile specificare una cartella locale nel punto di distribuzione oppure una cartella in qualsiasi dispositivo nella rete aziendale.

    L'account utente utilizzato nel punto di distribuzione per eseguire Network Agent deve disporre di accesso in lettura e scrittura alla cartella specificata.

9. Fare clic sul pulsante **OK**.

I dispositivi selezionati opereranno come punti di distribuzione.

Modifica dell'elenco dei punti di distribuzione per un gruppo di amministrazione

È possibile visualizzare l'elenco dei punti di distribuzione assegnati a un gruppo di amministrazione specifico e modificare l'elenco aggiungendo o rimuovendo punti di distribuzione.

Per visualizzare e modificare l'elenco dei punti di distribuzione assegnati a un gruppo di amministrazione:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Gruppi**.
2. Nella struttura dei gruppi di amministrazione selezionare il gruppo di amministrazione per cui si desidera visualizzare i punti di distribuzione assegnati.
3. Fare clic sulla scheda **Punti di distribuzione**.
4. Aggiungere nuovi punti di distribuzione per il gruppo di amministrazione utilizzando il pulsante **Assegna** o rimuovere i punti di distribuzione assegnati utilizzando il pulsante **Annulla assegnazione**.

A seconda delle modifiche, i nuovi punti di distribuzione verranno aggiunti all'elenco o i punti di distribuzione esistenti verranno rimossi dall'elenco.

Utilizzo di un punto di distribuzione come server push

In Kaspersky Security Center Cloud Console, un punto di distribuzione può fungere da server push per i dispositivi basati su Windows e Linux gestiti da Network Agent. Un server push ha lo stesso ambito dei dispositivi gestiti del punto di distribuzione in cui è abilitato il server push. Se sono stati assegnati più punti di distribuzione per lo stesso gruppo di amministrazione, è possibile abilitare il server push in ciascuno dei punti di distribuzione. In questo caso, Administration Server bilancia il carico tra i punti di distribuzione.

È possibile utilizzare i punti di distribuzione come server push per garantire la connettività continua tra un dispositivo gestito e Administration Server. La continuità della connessione è necessaria per alcune operazioni, come l'esecuzione e l'arresto di attività locali, la ricezione di statistiche per un'applicazione gestita o la creazione di un tunnel. Se si utilizza un punto di distribuzione come server push, non è necessario inviare pacchetti alla porta UDP di Network Agent.

Per utilizzare un punto di distribuzione come server push:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Fare clic sul punto di distribuzione che si desidera utilizzare come server push.

4. Nell'elenco delle proprietà del punto di distribuzione selezionato, passare alla sezione **Generale**, quindi abilitare l'opzione **Esegui server push**.

   Il campo di immissione **Porta server push** diventa disponibile.

5. Nel campo di immissione **Porta server push**, specificare la porta nel punto di distribuzione che i dispositivi client utilizzeranno per la connessione. Per impostazione predefinita, viene utilizzata la porta 13295.

   > Per stabilire una connessione tra il punto di distribuzione che funge da server push e un dispositivo gestito, è necessario aggiungere manualmente la porta del server push specificata all'elenco di esclusioni di Microsoft Windows Firewall.

6. Fare clic su **OK** per chiudere la finestra delle proprietà del punto di distribuzione, quindi fare clic su **Salva** per applicare le modifiche.

   Dopo aver abilitato l'opzione **Esegui server push**, l'opzione **Non eseguire la disconnessione da Administration Server** viene abilitata automaticamente nel punto di distribuzione che funge da server push. Questa opzione fornisce una connessione anticipata tra Network Agent e Administration Server.

7. Aprire la finestra delle impostazioni del criterio di Network Agent.

8. Passare a **Connettività** → **Rete** e quindi abilitare l'opzione **Usa punto di distribuzione per forzare la connessione ad Administration Server**. Chiudere il lucchetto di questa opzione.

9. Anche nella sottosezione **Rete** è possibile disabilitare l'opzione **Usa porta UDP**. Il server push configurato fornirà connettività continua tra un dispositivo gestito e l'Administration Server anziché inviare pacchetti tramite la porta UDP.

10. Fare clic su **OK** per chiudere la finestra.

Il punto di distribuzione inizia a operare come server push. Adesso può inviare notifiche push ai dispositivi client.

Utilizzo dell'opzione "Non eseguire la disconnessione da Administration Server" per garantire connettività continua tra un dispositivo gestito e Administration Server

Se non si utilizzano server push, Kaspersky Security Center Cloud Console non garantirà la connettività continua tra i dispositivi gestiti e Administration Server. I Network Agent nei dispositivi gestiti stabiliscono periodicamente connessioni ed eseguono la sincronizzazione con l'Administration Server. L'intervallo tra queste sessioni di sincronizzazione è definito in un criterio di Network Agent. Se è necessaria una sincronizzazione anticipata, Administration Server (o un punto di distribuzione, se in uso) invia un pacchetto di rete firmato tramite una rete IPv4 o IPv6 alla porta UDP di Network Agent. Il numero di porta predefinito è 15000. Se non è possibile stabilire la connessione tramite UDP tra Administration Server e un dispositivo gestito, la sincronizzazione verrà eseguita alla successiva connessione periodica di Network Agent ad Administration Server entro l'intervallo di sincronizzazione.

Alcune operazioni non possono essere eseguite senza una connessione preventiva tra Network Agent e Administration Server, come l'esecuzione e l'arresto di attività locali, la ricezione di statistiche per un'applicazione gestita o la creazione di un tunnel. Per risolvere il problema, se non si utilizzano server push è possibile utilizzare l'opzione **Non eseguire la disconnessione da Administration Server** per assicurarsi che vi sia connettività continua tra un dispositivo gestito e Administration Server.

Per garantire connettività continua tra un dispositivo gestito e Administration Server:

1. Eseguire una delle seguenti operazioni:

   - Se il dispositivo gestito accede direttamente ad Administration Server (quindi non tramite un punto di distribuzione):

     a. Nel menu principale accedere a **Dispositivi** → **Dispositivi gestiti**.

     b. Fare clic sul nome del dispositivo a cui si desidera fornire una connettività continua.

     Verrà visualizzata la finestra delle proprietà del dispositivo gestito.

   - Se il dispositivo gestito accede ad Administration Server tramite un punto di distribuzione in esecuzione in modalità gateway, non direttamente:

     a. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome dell'Administration Server richiesto.

     Verrà visualizzata la finestra delle proprietà di Administration Server.

     b. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

     c. Nell'elenco dei punti di distribuzione, fare clic sul nome del punto di distribuzione richiesto.

     Verrà visualizzata la finestra delle proprietà del punto di distribuzione selezionato.

2. Nella sezione **Generale** della finestra delle proprietà aperta, selezionare l'opzione **Non eseguire la disconnessione da Administration Server**.

Viene stabilita la connettività continua tra il dispositivo gestito e Administration Server.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Creazione dei gruppi di amministrazione

Inizialmente, la gerarchia dei gruppi di amministrazione contiene il solo gruppo di amministrazione denominato **Dispositivi gestiti**. Durante la creazione di una gerarchia di gruppi di amministrazione, è possibile aggiungere dispositivi e macchine virtuali al gruppo **Dispositivi gestiti**, nonché aggiungere sottogruppi. Per ciascun gruppo di amministrazione, la finestra delle proprietà contiene informazioni su criteri, attività e dispositivi correlati al gruppo.

Per creare un gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Selezionare la casella di controllo accanto al gruppo di amministrazione per cui si desidera creare un nuovo sottogruppo.
3. Fare clic sul pulsante **Aggiungi**.
4. Digitare un nome per il nuovo gruppo di amministrazione.
5. Fare clic sul pulsante **Aggiungi**.

   Un nuovo gruppo di amministrazione con il nome specificato viene visualizzato nella gerarchia dei gruppi di amministrazione.

L'applicazione consente di creare una gerarchia di gruppi di amministrazione basata sulla struttura di Active Directory o sulla struttura della rete di dominio. È inoltre possibile creare una struttura di gruppi a partire da un file di testo.

Per creare una struttura di gruppi di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Fare clic sul pulsante **Importa**.

   Verrà avviata la Creazione guidata nuova struttura dei gruppi di amministrazione. Seguire le istruzioni della procedura guidata.

Creazione delle regole di spostamento dei dispositivi

È possibile impostare regole di spostamento dei dispositivi, ovvero regole che allocano automaticamente i dispositivi ai gruppi di amministrazione.

Per creare una regola di spostamento:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Regole di spostamento**.
2. Fare clic su **Aggiungi**.

3. Nella finestra visualizzata specificare le seguenti impostazioni nella scheda **Generale**:

- Nome regola

  Immettere un nome per la nuova regola.

  Se si sta copiando una regola, alla nuova regola è assegnato lo stesso nome della regola di origine, ma al nome viene aggiunto un indice in formato (), ad esempio: (1).

- Gruppo di amministrazione

  Selezionare il gruppo di amministrazione in cui devono essere spostati automaticamente i dispositivi.

- Regola attiva

  Se questa opzione è abilitata, la regola è abilitata e inizia a funzionare dopo il salvataggio.

  Se questa opzione è disabilitata, la regola viene creata, ma non abilitata. Non funzionerà finché non si abilita questa opzione.

- Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione

  Se questa opzione è abilitata, solo i dispositivi non assegnati verranno spostati nel gruppo selezionato.

  Se questa opzione è disabilitata, i dispositivi che appartengono già ad altri gruppi di amministrazione, nonché i dispositivi non assegnati, verranno spostati nel gruppo selezionato.

- Applica regola

  È possibile selezionare una delle seguenti opzioni:

  - **Esegui una volta per ciascun dispositivo**

    La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri.

  - **Esegui una volta per ciascun dispositivo, quindi a ogni reinstallazione di Network Agent**

    La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri, quindi solo quando Network Agent viene reinstallato in questi dispositivi.

  - **Applica regola in modo continuativo**

    La regola viene applicata in base alla pianificazione impostata automaticamente da Administration Server (in genere, con una frequenza di alcune ore).

4. Nella scheda **Condizioni delle regole**, specificare almeno un criterio in base al quale i dispositivi vengono spostati in un gruppo di amministrazione.

5. Fare clic su **Salva**.

Verrà creata la regola di spostamento. La regola è visualizzata nell'elenco delle regole di spostamento.

Maggiore è la posizione nell'elenco, maggiore sarà la priorità della regola. Per aumentare o diminuire la priorità di una regola di spostamento, spostare la regola rispettivamente in alto o in basso nell'elenco utilizzando il mouse.

Se gli attributi del dispositivo soddisfano le condizioni di più regole, il dispositivo viene spostato nel gruppo di destinazione della regola con la priorità più alta (al livello più alto nell'elenco delle regole).

Copia delle regole di spostamento dei dispositivi

È possibile copiare le regole di spostamento, ad esempio se si desidera disporre di più regole identiche per diversi gruppi di amministrazione di destinazione.

Per copiare una regola di spostamento esistente:

1. Eseguire una delle seguenti operazioni:
   - Nel menu principale accedere a **Risorse (dispositivi)** → **Regole di spostamento**.
   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Regole di spostamento**.

   Verrà visualizzato l'elenco delle regole di spostamento.
2. Selezionare la casella di controllo accanto alla regola da copiare.
3. Fare clic su **Copia**.
4. Nella finestra visualizzata modificare le seguenti informazioni nella scheda **Generale** (o non apportare modifiche se si desidera solo copiare la regola senza modificarne le impostazioni):
   - Nome regola

     Immettere un nome per la nuova regola.

     Se si sta copiando una regola, alla nuova regola è assegnato lo stesso nome della regola di origine, ma al nome viene aggiunto un indice in formato (), ad esempio: (1).
   - Gruppo di amministrazione

     Selezionare il gruppo di amministrazione in cui devono essere spostati automaticamente i dispositivi.
   - Regola attiva

     Se questa opzione è abilitata, la regola è abilitata e inizia a funzionare dopo il salvataggio.

     Se questa opzione è disabilitata, la regola viene creata, ma non abilitata. Non funzionerà finché non si abilita questa opzione.
   - Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione

     Se questa opzione è abilitata, solo i dispositivi non assegnati verranno spostati nel gruppo selezionato.

     Se questa opzione è disabilitata, i dispositivi che appartengono già ad altri gruppi di amministrazione, nonché i dispositivi non assegnati, verranno spostati nel gruppo selezionato.

- Applica regola

  È possibile selezionare una delle seguenti opzioni:

  - **Esegui una volta per ciascun dispositivo**

    La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri.

  - **Esegui una volta per ciascun dispositivo, quindi a ogni reinstallazione di Network Agent**

    La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri, quindi solo quando Network Agent viene reinstallato in questi dispositivi.

  - **Applica regola in modo continuativo**

    La regola viene applicata in base alla pianificazione impostata automaticamente da Administration Server (in genere, con una frequenza di alcune ore).

5. Nella scheda **Condizioni delle regole**, specificare almeno un criterio per i dispositivi che si desidera spostare automaticamente.

6. Fare clic su **Salva**.

Verrà creata la nuova regola di spostamento. La regola è visualizzata nell'elenco delle regole di spostamento.

Aggiunta manuale dei dispositivi a un gruppo di amministrazione

È possibile spostare automaticamente i dispositivi nei gruppi di amministrazione creando regole di spostamento dei dispositivi o manualmente spostando i dispositivi da un gruppo di amministrazione a un altro oppure aggiungendo dispositivi a un gruppo di amministrazione selezionato. Questa sezione descrive come aggiungere manualmente i dispositivi a un gruppo di amministrazione.

Per aggiungere manualmente uno o più dispositivi a un gruppo di amministrazione selezionato:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

2. Fare clic sul collegamento **Percorso corrente:** `<percorso corrente>` sopra l'elenco.

3. Nella finestra visualizzata selezionare il gruppo di amministrazione al quale si desidera aggiungere i dispositivi.

4. Fare clic sul pulsante **Aggiungi dispositivi**.

   Verrà avviato lo Spostamento guidato dispositivi.

5. Creare un elenco dei dispositivi che si desidera aggiungere al gruppo di amministrazione.

   È possibile aggiungere solo i dispositivi per cui sono già state aggiunte informazioni al database di Administration Server durante la connessione del dispositivo o dopo la device discovery.

   Selezionare il modo in cui aggiungere dispositivi all'elenco:

   - Fare clic sul pulsante **Aggiungi dispositivi** e specificare i dispositivi in uno dei seguenti modi:

     - Selezionare i dispositivi dall'elenco dei dispositivi rilevati da Administration Server.

- Specificare l'indirizzo IP o l'intervallo IP di un dispositivo.
- Specificare il nome NetBIOS o il nome DNS di un dispositivo.

Il campo relativo al nome del dispositivo non deve contenere né spazi né i seguenti caratteri proibiti: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Fare clic sul pulsante **Importa dispositivi da file** per importare un elenco di dispositivi da un file .txt. È necessario specificare il nome o l'indirizzo di ciascun dispositivo in una riga separata.

Il file non deve contenere né spazi né i seguenti caratteri proibiti: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

6. Visualizzare l'elenco dei dispositivi da aggiungere al gruppo di amministrazione. È possibile modificare l'elenco aggiungendo o rimuovendo i dispositivi.
7. Dopo essersi accertati che l'elenco è corretto, fare clic sul pulsante **Avanti**.

La procedura guidata elabora l'elenco dei dispositivi e visualizza il risultato. I dispositivi elaborati correttamente vengono aggiunti al gruppo di amministrazione e visualizzati nell'elenco dei dispositivi con i nomi generati da Administration Server.

Spostamento manuale dei dispositivi o dei cluster in un gruppo di amministrazione

È possibile spostare i dispositivi da un gruppo di amministrazione a un altro o dal gruppo dei dispositivi non assegnati a un gruppo di amministrazione.

È anche possibile spostare cluster o array di server da un gruppo di amministrazione all'altro. Quando si sposta un cluster o un array di server in un altro gruppo, tutti i suoi nodi vengono spostati con esso, perché un cluster e uno qualsiasi dei suoi nodi appartengono sempre allo stesso gruppo di amministrazione. Quando si seleziona un singolo nodo del cluster nella scheda **Dispositivi**, il pulsante **Sposta nel gruppo** diventa non disponibile.

Per spostare uno o più dispositivi o cluster in un gruppo di amministrazione selezionato:

1. Aprire il gruppo di amministrazione da cui si desidera spostare i dispositivi. A tale scopo, eseguire una delle operazioni seguenti:
   - Per aprire un gruppo di amministrazione, nel menu principale passare a **Risorse (dispositivi)** → **Gruppi** → **<group name>** → **Dispositivi gestiti**.
   - Per aprire il gruppo **Dispositivi non assegnati**, nel menu principale passare a **Individuazione e distribuzione** → **Dispositivi non assegnati**.
2. Se il gruppo di amministrazione contiene cluster o array di server, la sezione **Dispositivi gestiti** è divisa in due schede: la scheda **Dispositivi** e la scheda **Cluster e array di server**. Aprire la scheda dell'oggetto che si desidera spostare.
3. Selezionare le caselle di controllo accanto ai dispositivi o ai cluster che si desidera spostare in un altro gruppo.

4. Fare clic sul pulsante **Sposta nel gruppo**.

5. Nella gerarchia dei gruppi di amministrazione, selezionare la casella di controllo accanto al gruppo di amministrazione in cui si desidera spostare i dispositivi o i cluster selezionati.

6. Fare clic sul pulsante **Sposta**.

I dispositivi o i cluster selezionati verranno spostati nel gruppo di amministrazione selezionato.

Configurazione delle regole di conservazione per i dispositivi non assegnati

Al termine del polling della rete Windows, i dispositivi trovati vengono inseriti nei sottogruppi del gruppo di amministrazione Dispositivi non assegnati. Questo gruppo di amministrazione è disponibile in **Individuazione e distribuzione** → **Individuazione** → **Domini Windows**. La cartella **Domini Windows** è il gruppo padre. Contiene gruppi figlio denominati in base ai domini e ai gruppi di lavoro corrispondenti rilevati durante il polling. Il gruppo padre può anche contenere il gruppo di amministrazione dei dispositivi mobili. È possibile configurare le regole di conservazione dei dispositivi non assegnati per il gruppo padre e ognuno dei gruppi figlio. Le regole di conservazione non dipendono dalle impostazioni di device discovery e operano anche se la device discovery è disabilitata.

Le regole di conservazione dei dispositivi non influiscono sui dispositivi con una o più unità criptate con Criptaggio dell'intero disco. Tali dispositivi non vengono eliminati automaticamente; è possibile eliminarli solo manualmente. Se è necessario eliminare un dispositivo con un'unità criptata, decriptare prima l'unità, quindi eliminare il dispositivo.

Per configurare le regole di conservazione per i dispositivi non assegnati:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Domini Windows**.

2. Eseguire una delle seguenti operazioni:

   - Per configurare le impostazioni del gruppo padre, fare clic sul pulsante **Proprietà**.

     Verrà visualizzata la finestra delle proprietà del dominio Windows.

   - Per configurare le impostazioni di un gruppo figlio, fare clic sul relativo nome.

     Verrà visualizzata la finestra delle proprietà del gruppo figlio.

3. Definire le seguenti impostazioni:

   - **Rimuovi il dispositivo dal gruppo se è inattivo da più di (giorni)**

     Se questa opzione è abilitata, è possibile specificare l'intervallo di tempo al termine del quale il dispositivo viene rimosso automaticamente dal gruppo. Per impostazione predefinita, questa opzione viene distribuita anche ai gruppi figlio. L'intervallo di tempo predefinito è 7 giorni.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Eredita da gruppo padre**

Se questa opzione è abilitata, il periodo di conservazione per i dispositivi del gruppo corrente viene ereditato dal gruppo padre e non può essere modificato.

Questa opzione è disponibile solo per i gruppi figlio.

Per impostazione predefinita, questa opzione è abilitata.

- **Forza ereditarietà nei gruppi figlio**

  I valori delle impostazioni vengono distribuiti ai gruppi figlio, ma nelle proprietà dei gruppi figlio tali impostazioni sono bloccate.

  Per impostazione predefinita, questa opzione è disabilitata.

4. Fare clic sul pulsante **Accetta**.

Le modifiche verranno salvate e applicate.

Configurazione della protezione di rete

Questa sezione contiene informazioni sulla configurazione manuale di criteri e attività, sui ruoli utente, sulla creazione di una struttura di gruppi di amministrazione e sulla gerarchia delle attività.

Scenario: Configurazione della protezione di rete

L'avvio rapido guidato crea criteri e attività con le impostazioni predefinite. Queste impostazioni possono risultare non ottimali o addirittura non consentite dall'organizzazione. Pertanto, è consigliabile ottimizzare tali criteri e attività e creare altri criteri e attività, se necessario per la rete.

Prerequisiti

Prima di iniziare, assicurarsi di aver completato lo scenario di configurazione iniziale di Kaspersky Security Center Cloud Console, incluso l'avvio rapido guidato.

Durante l'esecuzione dell'Avvio rapido guidato, i seguenti criteri e attività vengono creati nel gruppo di amministrazione **Dispositivi gestiti**:

- Criterio di Kaspersky Endpoint Security
- Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
- Criterio di Network Agent
- Trova vulnerabilità e aggiornamenti richiesti (attività di Network Agent)

Passaggi

La configurazione della protezione della rete procede per fasi:

1. **Installazione e propagazione dei criteri e dei profili criterio delle applicazioni Kaspersky**

   Per configurare e propagare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti, è possibile utilizzare due diversi metodi di gestione della protezione: quello incentrato sui dispositivi o quello incentrato sugli utenti. È anche possibile combinare questi due approcci.

2. **Configurazione delle attività per la gestione remota delle applicazioni Kaspersky**

   Controllare le attività create con l'avvio rapido guidato e, se necessario, ottimizzarle.

   Istruzioni dettagliate:

   - Configurazione dell'attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
   - Creazione dell'attività *Find vulnerabilities and required updates*

   Se necessario, creare attività aggiuntive per gestire le applicazioni Kaspersky installate nei dispositivi client.

3. **Valutazione e limitazione del carico di eventi nel database**

Le informazioni sugli eventi durante il funzionamento delle applicazioni gestite vengono trasferite da un dispositivo client e registrate nel database di Administration Server. Per ridurre il carico su Administration Server, valutare e limitare il numero massimo di eventi che possono essere archiviati nel database.

Istruzioni dettagliate: Impostazione del numero massimo di eventi

Risultati

Quando viene completato questo scenario, la rete sarà protetta tramite la configurazione delle applicazioni Kaspersky, delle attività e degli eventi ricevuti da parte di Administration Server:

- Le applicazioni Kaspersky sono configurate in base ai criteri e ai profili criterio.
- Le applicazioni vengono gestite attraverso un set di attività.
- Viene impostato il numero massimo di eventi che è possibile archiviare nel database.

Al termine della configurazione della protezione di rete, è possibile procedere alla configurazione degli aggiornamenti standard nei database e nelle applicazioni Kaspersky.

Informazioni sui metodi di gestione della protezione incentrati sui dispositivi e incentrati sugli utenti

È possibile gestire le impostazioni di protezione dal punto di vista delle funzionalità del dispositivo e dal punto di vista dei ruoli utente. Il primo metodo è denominato *gestione della protezione incentrata sui dispositivi* e il secondo è denominato *gestione della protezione incentrata sugli utenti*. Per applicare impostazioni dell'applicazione diverse a diversi dispositivi è possibile utilizzare uno o entrambi i tipi di gestione insieme.

La gestione della protezione incentrata sui dispositivi consente di applicare diverse impostazioni dell'applicazione di protezione ai dispositivi gestiti in base alle funzionalità specifiche del dispositivo. È ad esempio possibile applicare impostazioni diverse ai dispositivi allocati in diversi gruppi di amministrazione. È inoltre possibile differenziare i dispositivi in base all'utilizzo di tali dispositivi in Active Directory o alle relative specifiche hardware.

La gestione della protezione incentrata sugli utenti consente di applicare diverse impostazioni dell'applicazione di protezione a diversi ruoli utente. È possibile creare diversi ruoli utente, assegnare un ruolo utente appropriato a ciascun utente e definire diverse impostazioni dell'applicazione per i dispositivi di proprietà di utenti con ruoli diversi. È ad esempio possibile applicare differenti impostazioni dell'applicazione ai dispositivi degli addetti alla contabilità e degli specialisti delle risorse umane (HR). Di conseguenza, quando viene implementata la gestione della protezione incentrata sugli utenti, ciascun reparto (reparto account e reparto HR) dispone della propria configurazione delle impostazioni per le applicazioni Kaspersky. Una configurazione delle impostazioni definisce le impostazioni delle applicazioni che possono essere modificate dagli utenti e quelle che vengono forzatamente impostate e bloccate dall'amministratore.

Utilizzando la gestione della protezione incentrata sugli utenti è possibile applicare impostazioni specifiche di un'applicazione per singoli utenti. Questo può essere necessario quando un dipendente ha un ruolo esclusivo nell'azienda o quando si desidera monitorare i problemi di sicurezza relativi ai dispositivi di una persona specifica. A seconda del ruolo di questo dipendente nell'azienda, è possibile espanderne o limitarne i diritti di modifica delle impostazioni dell'applicazione. È ad esempio possibile espandere i diritti di un amministratore di sistema che gestisce i dispositivi client in una sede locale.

È inoltre possibile combinare gli approcci di gestione della protezione incentrata sui dispositivi e incentrata sugli utenti. È ad esempio possibile configurare uno specifico criterio dell'applicazione per ogni gruppo di amministrazione e quindi creare profili criterio per uno o più ruoli utente dell'azienda. In questo caso criteri e profili criterio vengono applicati nel seguente ordine:

1. Vengono applicati i criteri creati per la gestione della protezione incentrata sui dispositivi.
2. Questi vengono modificati dai profili criterio secondo le priorità dei profili criterio.
3. I criteri vengono modificati dai profili criterio associati ai ruoli utente.

Configurazione e propagazione dei criteri: approccio incentrato sui dispositivi

Questa sezione offre uno scenario relativo all'approccio incentrato sui dispositivi alla configurazione centralizzata delle applicazioni Kaspersky installate nei dispositivi gestiti. Al termine di questo scenario, le applicazioni saranno configurate in tutti i dispositivi gestiti in base ai criteri delle applicazioni e ai profili criterio specificati.

È inoltre possibile valutare la gestione della protezione incentrata sull'utente come opzione alternativa o aggiuntiva all'approccio incentrato sui dispositivi.

Processo

Lo scenario di gestione incentrata sui dispositivi delle applicazioni Kaspersky comprende i seguenti passaggi:

1. **Configurazione dei criteri delle applicazioni**

   Configurare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti tramite la creazione di un criterio per ogni applicazione. Questo set di criteri sarà propagato ai dispositivi client.

   Quando si configura la protezione della rete in Avvio rapido guidato, Kaspersky Security Center Cloud Console crea il criterio predefinito per Kaspersky Endpoint Security for Windows. Se è stata completata la configurazione tramite questa procedura guidata, non è necessario creare un nuovo criterio per questa applicazione. Passare alla configurazione manuale del criterio di Kaspersky Endpoint Security.

   Se si dispone di una struttura gerarchica con più gruppi di amministrazione, per impostazione predefinita i gruppi di amministrazione figlio ereditano i criteri dall'Administration Server primario. È possibile forzare l'ereditarietà da parte dei gruppi figlio per impedire eventuali modifiche delle impostazioni configurate nel criterio upstream. Se si desidera forzare l'ereditarietà solo di una parte delle impostazioni, è possibile bloccarle nel criterio upstream. Le rimanenti impostazioni sbloccate saranno disponibili per la modifica nei criteri downstream. La gerarchia di criteri creata consente di gestire in modo efficace i dispositivi nei gruppi di amministrazione.

   Istruzioni dettagliate: Creazione di un criterio

2. **Creazione dei profili criterio (facoltativo)**

   Se si desidera applicare differenti impostazioni dei criteri ai dispositivi all'interno di un singolo gruppo di amministrazione, creare profili criterio per tali dispositivi. Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo nel dispositivo gestito.

   Utilizzando le condizioni di attivazione del profilo, è possibile applicare diversi profili criterio, ad esempio ai dispositivi appartenenti a un determinato gruppo di protezione o a un'unità specifica di Active Directory, con una specifica configurazione hardware o contrassegnati con tag specifici. Utilizzare i tag per filtrare i dispositivi che soddisfano i criteri specificati. È ad esempio possibile creare un tag denominato *Windows*, contrassegnare tutti i dispositivi con sistema operativo Windows con questo tag e quindi specificare il tag come condizione di attivazione per un profilo criterio. Come risultato, le applicazioni Kaspersky installate in tutti i dispositivi che eseguono Windows verranno gestite dal profilo criterio corrispondente.

   Istruzioni dettagliate:

   - Creazione di un profilo criterio

- Creazione di una regola di attivazione del profilo criterio

3. **Propagazione di criteri e profili criterio nei dispositivi gestiti**

   Kaspersky Security Center Cloud Console sincronizza automaticamente Administration Server con i dispositivi gestiti diverse volte all'ora. Durante la sincronizzazione, i criteri e i profili criterio nuovi o modificati vengono propagati ai dispositivi gestiti. È possibile ignorare la sincronizzazione automatica ed eseguire manualmente la sincronizzazione utilizzando il comando Forza sincronizzazione. Al termine della sincronizzazione, i criteri e i profili criterio vengono inviati e applicati alle applicazioni Kaspersky installate.

   È possibile verificare se i criteri e i profili criterio sono stati distribuiti a un dispositivo. Kaspersky Security Center Cloud Console specifica la data e l'ora di invio nelle proprietà del dispositivo.

   Istruzioni dettagliate: Sincronizzazione forzata

Risultati

Al termine dello scenario incentrato sui dispositivi, le applicazioni Kaspersky vengono configurate in base alle impostazioni specificate e propagate tramite la gerarchia di criteri.

I criteri delle applicazioni e i profili criterio configurati verranno applicati automaticamente ai nuovi dispositivi aggiunti ai gruppi di amministrazione.

Configurazione e propagazione dei criteri: approccio incentrato sull'utente

Questa sezione descrive lo scenario relativo all'approccio incentrato sugli utenti alla configurazione centralizzata delle applicazioni Kaspersky installate nei dispositivi gestiti. Al termine di questo scenario, le applicazioni saranno configurate in tutti i dispositivi gestiti in base ai criteri delle applicazioni e ai profili criterio specificati.

È inoltre possibile valutare la gestione della protezione incentrata sui dispositivi come opzione alternativa o aggiuntiva all'approccio incentrato sugli utenti. Ulteriori informazioni sui due approcci di gestione.

Processo

Lo scenario di gestione incentrata sugli utenti delle applicazioni Kaspersky comprende i seguenti passaggi:

1. **Configurazione dei criteri delle applicazioni**

   Configurare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti tramite la creazione di un criterio per ogni applicazione. Questo set di criteri sarà propagato ai dispositivi client.

   Quando si configura la protezione della rete in Avvio rapido guidato, Kaspersky Security Center Cloud Console crea il criterio predefinito per Kaspersky Endpoint Security. Se è stata completata la configurazione tramite questa procedura guidata, non è necessario creare un nuovo criterio per questa applicazione. Passare alla configurazione manuale del criterio di Kaspersky Endpoint Security.

   Se si dispone di una struttura gerarchica con più gruppi di amministrazione, per impostazione predefinita i gruppi di amministrazione figlio ereditano i criteri dall'Administration Server primario. È possibile forzare l'ereditarietà da parte dei gruppi figlio per impedire eventuali modifiche delle impostazioni configurate nel criterio upstream. Se si desidera forzare l'ereditarietà solo di una parte delle impostazioni, è possibile bloccarle nel criterio upstream. Le rimanenti impostazioni sbloccate saranno disponibili per la modifica nei criteri downstream. La gerarchia di criteri creata consente di gestire in modo efficace i dispositivi nei gruppi di amministrazione.

   Istruzioni dettagliate: Creazione di un criterio

2. **Specificazione dei proprietari dei dispositivi**

Assegnare i dispositivi gestiti agli utenti corrispondenti.

Istruzioni dettagliate: Assegnazione di un utente come proprietario dispositivo

3. **Definizione dei ruoli utente tipici dell'azienda**

   Prendere in considerazione i diversi tipi di attività eseguite dai dipendenti dell'azienda. È necessario suddividere tutti i dipendenti in base ai rispettivi ruoli. È ad esempio possibile suddividerli per reparto, professioni o posizioni. A questo punto, sarà necessario creare un ruolo utente per ciascun gruppo. Tenere presente che ogni ruolo utente avrà uno specifico profilo criterio che contiene le impostazioni delle applicazioni specifiche per questo ruolo.

4. **Creazione dei ruoli utente**

   Creare e configurare un ruolo utente per ogni gruppo di dipendenti che è stato definito nel passaggio precedente o utilizzare i ruoli utente predefiniti. I ruoli utente conterranno set di diritti di accesso alle funzionalità dell'applicazione.

   Istruzioni dettagliate: Creazione di un ruolo utente

5. **Definizione dell'ambito di ogni ruolo utente**

   Per ognuno dei ruoli utente creati, definire gli utenti e/o i gruppi di protezione e i gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

   Istruzioni dettagliate: Modifica dell'ambito di un ruolo utente

6. **Creazione di profili criterio**

   Creare un profilo criterio per ogni ruolo utente nell'organizzazione. I profili criterio definiscono le impostazioni che saranno applicate alle applicazioni installate nei dispositivi degli utenti, a seconda del ruolo di ogni utente.

   Istruzioni dettagliate: Creazione di un profilo criterio

7. **Associazione dei profili criterio ai ruoli utente**

   Associare i profili criterio creati ai ruoli utente. In tal modo, il profilo criterio diventa attivo per un utente che ha il ruolo specificato. Le impostazioni configurate nel profilo criterio verranno applicate alle applicazioni Kaspersky installate nei dispositivi dell'utente.

   Istruzioni dettagliate: Associazione dei profili criterio ai ruoli

8. **Propagazione di criteri e profili criterio nei dispositivi gestiti**

   Kaspersky Security Center Cloud Console sincronizza automaticamente Administration Server con i dispositivi gestiti diverse volte all'ora. Durante la sincronizzazione, i criteri e i profili criterio nuovi o modificati vengono propagati ai dispositivi gestiti. È possibile ignorare la sincronizzazione automatica ed eseguire manualmente la sincronizzazione utilizzando il comando Forza sincronizzazione. Al termine della sincronizzazione, i criteri e i profili criterio vengono inviati e applicati alle applicazioni Kaspersky installate.

   È possibile verificare se i criteri e i profili criterio sono stati distribuiti a un dispositivo. Kaspersky Security Center Cloud Console specifica la data e l'ora di invio nelle proprietà del dispositivo.

   Istruzioni dettagliate: Sincronizzazione forzata

Risultati

Al termine dello scenario incentrato sugli utenti, le applicazioni Kaspersky vengono configurate in base alle impostazioni specificate e propagate tramite la gerarchia di criteri e profili criterio.

Per un nuovo utente, sarà necessario creare un nuovo account e quindi assegnare all'utente uno dei ruoli utente creati e i dispositivi. I criteri delle applicazioni e i profili criterio configurati verranno applicati automaticamente ai dispositivi di questo utente.

Configurazione manuale del criterio di Kaspersky Endpoint Security

Questa sezione offre suggerimenti per la configurazione del criterio di Kaspersky Endpoint Security. È possibile eseguire la configurazione nella finestra delle proprietà del criterio. Quando si modifica un'impostazione, fare clic sull'icona del lucchetto a destra del gruppo di impostazioni pertinente per applicare i valori specificati a una workstation.

Configurazione di Kaspersky Security Network

Kaspersky Security Network (KSN) è l'infrastruttura dei servizi cloud che contiene informazioni sulla reputazione di file, risorse Web e software. Kaspersky Security Network consente a Kaspersky Endpoint Security for Windows di rispondere più rapidamente a diversi tipi di minacce, migliora le prestazioni dei componenti della protezione e riduce la probabilità di falsi positivi. Per ulteriori informazioni su Kaspersky Security Network, vedere la Guida di Kaspersky Endpoint Security for Windows.

È possibile configurare il lavoro di Kaspersky Security Network nella finestra delle proprietà dei criteri di Kaspersky Endpoint Security for Windows, nella sezione **Impostazioni applicazione** → **Advanced Threat Protection**.

Per specificare le impostazioni consigliate di KSN:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio passare a **Impostazioni applicazione** → **Protezione minacce avanzata** → **Kaspersky Security Network**.
4. Verificare che l'opzione **Usa Administration Server come server proxy KSN** sia abilitata. L'utilizzo di questa opzione consente di ridistribuire e ottimizzare il traffico nella rete.

   Se si utilizza Managed Detection and Response, è necessario abilitare l'opzione **Proxy KSN** per il punto di distribuzione e abilitare la modalità KSN estesa.
5. [facoltativo] Abilitare l'utilizzo dei server KSN se il servizio proxy KSN non è disponibile. A tale scopo, abilitare l'opzione **Usa i server di Kaspersky Security Network se il server proxy KSN non è disponibile**.

   I server KSN possono essere posizionati sul lato di Kaspersky (quando si utilizza KSN) o sul lato di terzi (quando si utilizza KPSN).
6. Fare clic su **OK**.

Sono state specificate le impostazioni consigliate di KSN.

Controllo dell'elenco delle reti protette dal Firewall

Verificare che il Firewall Kaspersky Endpoint Security for Windows protegga tutte le reti. Per impostazione predefinita il Firewall protegge le reti con i seguenti tipi di connessione:

- **Rete pubblica**. Le applicazioni anti-virus, i firewall o i filtri non proteggono i dispositivi in una rete di questo tipo.
- **Rete locale**. L'accesso a file e stampanti è limitato per i dispositivi in questa rete.
- **Rete attendibile**. I dispositivi in tale rete sono protetti da attacchi e accessi non autorizzati a file e dati.

Se è stata configurata una rete personalizzata, assicurarsi che il Firewall la protegga. A tale scopo, controllare l'elenco delle reti nelle proprietà dei criteri di Kaspersky Endpoint Security for Windows. L'elenco potrebbe non contenere tutte le reti.

Per ulteriori informazioni sul Firewall vedere la Guida di Kaspersky Endpoint Security for Windows.

Per controllare l'elenco delle reti:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio passare a **Impostazioni applicazione** → **Protezione minacce essenziale** → **Firewall**.
4. In **Reti disponibili**, fare clic sul collegamento **Impostazioni di rete**.

   Verrà aperta la finestra **Connessioni di rete**. Questa finestra mostra l'elenco delle reti.
5. Se nell'elenco non è presente una rete, aggiungerla.

Esclusione dei dettagli del software dalla memoria di Administration Server

È consigliabile evitare che Administration Server salvi le informazioni sui moduli software avviati nei dispositivi di rete. Di conseguenza, la memoria di Administration Server non viene sovraccaricata.

È possibile disabilitare il salvataggio di queste informazioni nelle proprietà dei criteri di Kaspersky Endpoint Security for Windows.

Per disabilitare il salvataggio delle informazioni sui moduli software installati:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio passare a **Impostazioni applicazione** → **Impostazioni generali** → **Rapporti e archivi**.
4. In **Trasferimento dei dati ad Administration Server** disabilitare la casella di controllo **Informazioni sulle applicazioni avviate** se è ancora abilitata nel criterio di primo livello.

   Quando questa casella di controllo è selezionata, il database di Administration Server salva informazioni su tutte le versioni di tutti i moduli software nei dispositivi connessi alla rete. Queste informazioni possono richiedere una quantità significativa di spazio su disco nel database di Kaspersky Security Center Cloud Console (decine di gigabyte).

Le informazioni sui moduli software installati non vengono più salvate nel database di Administration Server.

Salvataggio degli eventi di criteri importanti nel database dell'Administration Server

Per evitare l'overflow del database di Administration Server, è consigliabile salvare solo gli eventi importanti nel database.

Per configurare la registrazione degli eventi importanti nel database di Administration Server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio aprire la scheda **Configurazione eventi**.
4. Nella sezione **Critico** fare clic su **Aggiungi evento** e selezionare solo le caselle di controllo accanto ai seguenti eventi:
   - *Violazione del contratto di licenza*
   - *L'esecuzione automatica dell'applicazione è disabilitata*
   - *Errore di attivazione*
   - *È stata rilevata una minaccia attiva. È necessario avviare Disinfezione avanzata*
   - *Disinfezione impossibile*
   - *Rilevato collegamento pericoloso aperto in precedenza*
   - *Processo terminato*
   - *Attività di rete bloccata*
   - *Attacco di rete rilevato*
   - *Avvio dell'applicazione non consentito*
   - *Accesso negato (basi locali)*
   - *Accesso negato (KSN)*
   - *Errore di aggiornamento locale*
   - *Impossibile avviare due attività contemporaneamente*
   - *Errore durante l'interazione con Kaspersky Security Center*
   - *Non tutti i componenti sono stati aggiornati*

- *Errore durante l'applicazione delle regole di criptaggio / decriptaggio dei file*
- *Errore durante l'abilitazione della modalità portatile*
- *Errore durante la disabilitazione della modalità portatile*
- *Impossibile caricare il Modulo di criptaggio*
- *Il criterio non può essere applicato*
- *Errore durante la modifica dei componenti dell'applicazione*

5. Fare clic su **OK**.
6. Nella sezione **Errore funzionale**, fare clic su **Aggiungi evento** e selezionare solo la casella di controllo accanto all'evento *Impostazioni delle attività non valide. Impostazioni non applicate*.
7. Fare clic su **OK**.
8. Nella sezione **Avviso** fare clic su **Aggiungi evento** e selezionare solo le caselle di controllo accanto ai seguenti eventi:
   - *L'Auto-Difesa è disabilitata*
   - *I componenti della protezione sono disabilitati*
   - *Chiave di riserva errata*
   - *È stato rilevato software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali (basi locali)*
   - *È stato rilevato software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali (KSN)*
   - *Oggetto eliminato*
   - *Oggetto disinfettato*
   - *L'utente ha scelto di non applicare il criterio di criptaggio*
   - *Il file è stato ripristinato dalla quarantena sul server di Kaspersky Anti Targeted Attack Platform dall'amministratore*
   - *Il file è stato messo in quarantena sul server di Kaspersky Anti Targeted Attack Platform dall'amministratore*
   - *Messaggio all'amministratore sul divieto di avvio dell'applicazione*
   - *Messaggio all'amministratore sul divieto di accesso al dispositivo*
   - *Messaggio all'amministratore sul divieto di accesso alla pagina Web*
9. Fare clic su **OK**.
10. Nella sezione **Informazioni** fare clic su **Aggiungi evento** e selezionare solo le caselle di controllo accanto ai seguenti eventi:
    - *È stata creata una copia di backup dell'oggetto*

- *Avvio dell'applicazione non consentito in modalità test*

11. Fare clic su **OK**.

La registrazione degli eventi importanti nel database di Administration Server è configurata.

Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security

L'opzione di pianificazione ottimale e consigliata per Kaspersky Endpoint Security è **Quando vengono scaricati nuovi aggiornamenti nell'archivio** quando la casella di controllo **Usa automaticamente il ritardo casuale per l'avvio delle attività** è selezionata.

Attività

Questa sezione descrive le attività utilizzate da Kaspersky Security Center Cloud Console.

Informazioni sulle attività

Kaspersky Security Center Cloud Console consente di gestire le applicazioni di protezione Kaspersky installate nei dispositivi creando ed eseguendo attività. Le *attività* sono necessarie per l'installazione, l'avvio e l'arresto delle applicazioni, la scansione dei file, l'aggiornamento dei database e dei moduli software, oltre che per eseguire altre azioni sulle applicazioni. Le attività possono essere eseguite nell'Administration Server e nei dispositivi.

I seguenti tipi di attività vengono eseguiti nei dispositivi:

- *Attività locali* - Attività eseguite in un dispositivo specifico

  Le attività locali possono essere modificate dall'amministratore che utilizza gli strumenti di amministrazione oppure dall'utente di un dispositivo remoto (ad esempio attraverso l'interfaccia dell'applicazione di protezione). Se un'attività locale viene modificata contemporaneamente dall'amministratore e dall'utente di un dispositivo gestito, hanno effetto le modifiche apportate dall'amministratore perché hanno una priorità più alta.

- *Attività di gruppo* - Attività eseguite su tutti i dispositivi di un gruppo specifico

  A meno che non sia diversamente specificato nelle proprietà dell'attività, un'attività di gruppo si applica anche a tutti i sottogruppi del gruppo selezionato.

- *Attività globali* - Attività eseguite su un set di dispositivi, indipendentemente dalla loro appartenenza a un gruppo

Per ogni applicazione è possibile creare più attività di gruppo, attività globali o attività locali.

È possibile apportare modifiche alle impostazioni delle attività, visualizzarne l'avanzamento, copiarle, esportarle, importarle ed eliminarle.

Le attività vengono avviate in un dispositivo solo se l'applicazione per cui l'attività è stata creata è in esecuzione.

I risultati dell'esecuzione delle attività vengono salvati nel registro eventi del sistema operativo in ciascun dispositivo e nel database di Administration Server.

Non includere dati privati nelle impostazioni dell'attività. Ad esempio, non specificare la password dell'amministratore del dominio.

Informazioni sull'ambito dell'attività

L'*ambito di un'attività* è il set di dispositivi in cui viene eseguita l'attività. I tipi di ambito sono i seguenti:

- Per un'*attività locale*, l'ambito è il dispositivo stesso.
- Per un'*attività di Administration Server*, l'ambito è Administration Server.
- Per un'*attività di gruppo*, l'ambito è l'elenco dei dispositivi inclusi nel gruppo.

Durante la creazione di un'*attività globale*, è possibile utilizzare i seguenti metodi per specificare l'ambito:

- Specificare manualmente specifici dispositivi.

  È possibile utilizzare un indirizzo IP (o un intervallo IP), un nome NetBIOS o un nome DNS come indirizzo del dispositivo.

- Importare un elenco di dispositivi da un file TXT con gli indirizzi dei dispositivi da aggiungere (ogni indirizzo deve essere specificato su una riga distinta).

  Se si importa un elenco di dispositivi da un file o se ne crea uno manualmente e i dispositivi vengono identificati con i rispettivi nomi, l'elenco deve contenere solo dispositivi per cui sono già state immesse le informazioni nel database di Administration Server. Inoltre, le informazioni devono essere state immesse al momento della connessione dei dispositivi o durante la device discovery.

- Specificare una selezione dispositivi.

  Nel corso del tempo, l'ambito un'attività si modifica, perché il set di dispositivi inclusi nella selezione cambia. Una selezione di dispositivi può essere creata sulla base degli attributi dei dispositivi, incluso il software installato in un dispositivo, e utilizzando i tag assegnati ai dispositivi. Una selezione dispositivi è il modo più flessibile per specificare l'ambito di un'attività.

  Le attività per le selezioni dispositivi vengono sempre eseguite in base a una pianificazione da Administration Server. Queste attività non possono essere eseguite nei dispositivi che non dispongono di una connessione ad Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite direttamente nei dispositivi, pertanto non dipendono dalla connessione del dispositivo ad Administration Server.

Le attività per le selezioni dispositivi non vengono eseguite in base all'ora locale di un dispositivo, ma in base all'ora locale di Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite in base all'ora locale di un dispositivo.

Creazione di un'attività

È possibile creare un'attività nell'elenco delle attività, oppure selezionare i dispositivi nell'elenco **Dispositivi gestiti**, quindi creare una nuova attività assegnata ai dispositivi selezionati.

Per creare un'attività nell'elenco delle attività:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni visualizzate.
3. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completa creazione attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
4. Fare clic sul pulsante **Fine**.

L'attività verrà creata e visualizzata nell'elenco delle attività.

Per creare una nuova attività assegnata ai dispositivi selezionati:

Nel menu principale accedere a **Risorse (dispositivi)** →**Dispositivi gestiti**.

Verrà visualizzato l'elenco dei dispositivi gestiti.

1. Nell'elenco dei dispositivi gestiti, selezionare le caselle di controllo accanto ai dispositivi per eseguire l'attività per gli stessi. È possibile utilizzare le funzioni di ricerca e filtraggio per trovare i dispositivi cercati.
2. Fare clic sul pulsante **Esegui attività**, quindi selezionare **Crea nuova attività**.

   Verrà avviata la Creazione guidata nuova attività.

   Nel primo passaggio della procedura guidata, è possibile rimuovere i dispositivi selezionati da includere nell'ambito dell'attività. Seguire le istruzioni della procedura guidata.
3. Fare clic sul pulsante **Fine**.

L'attività viene creata per i dispositivi selezionati.

Visualizzazione dell'elenco delle attività

È possibile visualizzare l'elenco delle attività create in Kaspersky Security Center Cloud Console.

Per visualizzare l'elenco delle attività,

Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

Verrà visualizzato l'elenco delle attività. Le attività sono raggruppate in base ai nomi delle applicazioni a cui sono correlate. Ad esempio, l'attività Disinstalla l'applicazione in remoto è correlata ad Administration Server e l'attività Trova vulnerabilità e aggiornamenti richiesti fa riferimento a Network Agent.

Per visualizzare le proprietà di un'attività:

Fare clic sul nome dell'attività.

Verrà visualizzata la finestra delle proprietà dell'attività con diverse schede denominate. Ad esempio, **Tipo di attività** viene visualizzato nella scheda **Generale** e la pianificazione dell'attività nella scheda **Pianificazione**.

Avvio manuale di un'attività

L'applicazione avvia le attività in base alle impostazioni di pianificazione specificate nelle proprietà di ciascuna attività. È possibile avviare manualmente un'attività in qualsiasi momento nell'elenco delle attività, oppure selezionare i dispositivi nell'elenco **Dispositivi gestiti**, quindi avviare un'attività esistente per gli stessi.

Per avviare un'attività manualmente:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Nell'elenco delle attività selezionare la casella di controllo accanto all'attività da avviare.
3. Fare clic sul pulsante **Avvia**.

   L'attività viene avviata. È possibile controllare lo stato dell'attività nella colonna **Stato** o facendo clic sul pulsante **Risultato**.

Avvio di un'attività per i dispositivi selezionati

È possibile selezionare uno o più dispositivi client nell'elenco dei dispositivi e quindi avviare un'attività creata in precedenza per gli stessi. In questo modo, è possibile eseguire attività create in precedenza per un set specifico di dispositivi.

Questa operazione modifica i dispositivi a cui è stata assegnata l'attività nell'elenco dei dispositivi selezionati durante l'esecuzione dell'attività.

Per avviare un'attività per i dispositivi selezionati:

1. Nel menu principale, accedere a **Risorse (dispositivi)** →**Dispositivi gestiti**. Verrà visualizzato l'elenco dei dispositivi gestiti.

Nell'elenco dei dispositivi gestiti, utilizzare le caselle di controllo per selezionare i dispositivi per cui eseguire l'attività. È possibile utilizzare le funzioni di ricerca e filtraggio per trovare i dispositivi cercati.

1. Fare clic sul pulsante **Esegui attività**, quindi selezionare **Applica attività esistente**.

   Verrà visualizzato l'elenco delle attività esistenti.
2. I dispositivi selezionati vengono visualizzati sopra l'elenco delle attività. Se necessario, è possibile rimuovere un dispositivo da questo elenco. È possibile eliminare tutti i dispositivi tranne uno.
3. Selezionare l'attività desiderata nell'elenco. È possibile utilizzare la casella di ricerca sopra l'elenco per cercare l'attività desiderata in base al nome. È possibile selezionare una sola attività.
4. Fare clic su **Salva e avvia attività**.

   L'attività selezionata viene avviata immediatamente per i dispositivi selezionati. Le impostazioni di avvio pianificato nell'attività non vengono modificate.

Proprietà e impostazioni generali delle attività

Questa sezione contiene le impostazioni che è possibile configurare per la maggior parte delle attività. L'elenco delle impostazioni disponibili dipende dall'attività che si sta configurando.

Impostazioni specificate durante la creazione dell'attività

È possibile specificare le seguenti impostazioni durante la creazione di un'attività. Alcune di queste impostazioni possono anche essere modificate nelle proprietà dell'attività creata.

- Dispositivi a cui assegnare l'attività:
  - **Assegna 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.

    Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

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

    L'attività viene assegnata a dispositivi specifici. È possibile specificare i dispositivi utilizzando uno dei seguenti metodi:

    - Specificare l'indirizzo IP, il nome NetBIOS o il nome DNS del dispositivo.
    - Specificare l'intervallo IP.

      Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.
    - Selezionare i dispositivi rilevati dall'Administration Server, inclusi i dispositivi non assegnati.

      Questa opzione può ad esempio essere utilizzata in un'attività per l'installazione di Network Agent nei dispositivi non assegnati.

  - **Assegna attività a una selezione dispositivi**

    L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

    Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

- Impostazioni per l'account:
  - **Account predefinito**

L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

Per impostazione predefinita, questa opzione è selezionata.

- **Specifica account**

  Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

- Impostazioni per il riavvio del sistema operativo:

  - **Non riavviare**

    I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

  - **Riavvia il dispositivo**

    I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

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

    Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- Forza la chiusura delle applicazioni nelle sessioni bloccate

  L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

  Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

  Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

  Per impostazione predefinita, questa opzione è disabilitata.

Impostazioni specificate dopo la creazione dell'attività

È possibile specificare le seguenti impostazioni solo dopo la creazione di un'attività.

- Impostazioni delle attività di gruppo:
  - Distribuisci ai sottogruppi

    Questa opzione è disponibile solo nelle impostazioni delle attività di gruppo.

    Quando questa opzione è abilitata, l'ambito dell'attività include:
    - Il gruppo di amministrazione selezionato durante la creazione dell'attività.
    - I gruppi di amministrazione subordinati al gruppo di amministrazione selezionato a qualsiasi livello inferiore nella gerarchia dei gruppi.

    Quando questa opzione è disabilitata, l'ambito dell'attività include solo il gruppo di amministrazione selezionato durante la creazione dell'attività.

    Per impostazione predefinita, questa opzione è abilitata.

  - Distribuisci negli Administration Server secondari e virtuali

    Quando questa opzione è abilitata, l'attività valida nell'Administration Server primario viene applicata anche negli Administration Server secondari (compresi quelli virtuali). Se un'attività dello stesso tipo esiste già nell'Administration Server secondario, nell'Administration Server secondario vengono applicate entrambe le attività: quella esistente e quella ereditata dall'Administration Server primario.

    Questa opzione è disponibile solo quando l'opzione **Distribuisci ai sottogruppi** è abilitata.

    Per impostazione predefinita, questa opzione è disabilitata.

- Impostazioni di pianificazione dell'attività:
  - **Impostazione Avvio pianificato:**

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è abilitata.

- **Ogni N minuti**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

  Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

- **Ogni N ore**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

  Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N giorni**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

  Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N settimane**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

- **Giornaliera (ora legale non supportata)**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

  Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center Cloud Console.

  Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

- **Settimanale**

  L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è 18:00:00.

- **Quando vengono scaricati nuovi aggiornamenti nell'archivio**

  Quando i nuovi aggiornamenti vengono scaricati negli archivi dei punti di distribuzione, Kaspersky Security Center Cloud Console esegue tutte le attività con questa pianificazione. Network Agent verifica la disponibilità degli aggiornamenti durante la sincronizzazione periodica tra il dispositivo gestito e l'Administration Server (heartbeat).

  È ad esempio possibile utilizzare questa pianificazione per l'attività di aggiornamento relativa a un'applicazione di protezione, come Kaspersky Endpoint Security.

  Se Network Agent in un dispositivo gestito non rileva nuovi aggiornamenti per almeno 25 ore, Kaspersky Security Center Cloud Console esegue in questo dispositivo tutte le attività con questa pianificazione. Queste attività vengono eseguite ogni ora fino a quando non vengono rilevati nuovi aggiornamenti. Kaspersky Security Center Cloud Console esegue queste attività ogni ora anche in assenza di connessione tra il dispositivo gestito e il punto di distribuzione che scarica gli aggiornamenti nell'archivio.

- **Durante un'epidemia di virus**

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione anti-virus che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

L'attività corrente viene avviata dopo il completamento di un'altra attività. È possibile selezionare la modalità di completamento dell'attività precedente (correttamente o con errori) per l'attivazione dell'avvio dell'attività corrente. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus*. Questo parametro funziona solo se entrambe le attività sono assegnate agli stessi dispositivi.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, vengono eseguite solo le attività pianificate nei dispositivi client. Per le opzioni **Manualmente**, **Una sola volta** e **Immediatamente**, le attività sono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è abilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

- **Accendi i dispositivi utilizzando la funzione Wake-on-LAN prima di avviare l'attività (min)**

Il sistema operativo nel dispositivo verrà avviato in base al periodo di tempo specificato prima dell'avvio dell'attività pianificata. Il periodo di tempo predefinito è cinque minuti.

Abilitare questa opzione se si desidera eseguire l'attività in tutti i dispositivi client nell'ambito dell'attività, inclusi quelli che sono spenti al momento dell'avvio dell'attività.

Se si desidera che il dispositivo si spenga automaticamente al termine dell'attività, abilitare l'opzione **Spegni i dispositivi dopo il completamento dell'attività**. Questa opzione è disponibile nella stessa finestra.

Per impostazione predefinita, questa opzione è disabilitata.

- Spegni i dispositivi dopo il completamento dell'attività

  Questa opzione può ad esempio essere abilitata per un'attività di aggiornamento dell'installazione che installa gli aggiornamenti nei dispositivi client ogni venerdì dopo l'orario lavorativo e quindi spegne tali dispositivi per il fine settimana.

  Per impostazione predefinita, questa opzione è disabilitata.

- Arresta se l'attività viene eseguita per più di (min)

  Al termine del periodo di tempo specificato, l'attività viene arrestata automaticamente, che sia stata completata o meno.

  Abilitare questa opzione se si desidera interrompere (o arrestare) le attività che richiedono troppo tempo per l'esecuzione.

  Per impostazione predefinita, questa opzione è disabilitata. Il tempo predefinito per l'esecuzione dell'attività è 120 minuti.

- Notifiche:
  - Sezione **Salva cronologia attività**:
    - **Salva tutti gli eventi**
    - **Salva eventi correlati all'avanzamento dell'attività**
    - **Salva solo i risultati dell'esecuzione dell'attività**
    - Archivia nel database di Administration Server per (giorni)

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività in tutti i dispositivi client nell'ambito dell'attività vengono archiviati nell'Administration Server per il numero di giorni specificato. Al termine di questo periodo, le informazioni vengono eliminate da Administration Server.

      Per impostazione predefinita, questa opzione è abilitata.

    - Archivia nel registro eventi del sistema operativo del dispositivo

Gli eventi dell'applicazione relativi all'esecuzione dell'attività vengono archiviati in locale nel registro eventi di Windows di ogni dispositivo client.

Per impostazione predefinita, questa opzione è disabilitata.

- **Notifica solo errori**
- **Notifica tramite e-mail**

- Impostazioni dell'ambito dell'attività
- Esclusioni dall'ambito

  È possibile specificare gruppi di dispositivi a cui non deve essere applicata l'attività. I gruppi da escludere possono essere solo sottogruppi del gruppo di amministrazione a cui è applicata l'attività.

- **Cronologia revisioni**

Esportazione di un'attività

Kaspersky Security Center Cloud Console consente di salvare un'attività e le relative impostazioni in un file KLT. È possibile utilizzare questo file KLT per importare l'attività salvata sia per Kaspersky Security Center Windows che per Kaspersky Security Center Linux.

Per esportare un'attività:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Selezionare la casella di controllo accanto all'attività che si desidera esportare.

   Non è possibile esportare più attività contemporaneamente. Se si selezionano più attività, il pulsante **Esporta** verrà disabilitato. Neanche le attività di Administration Server sono disponibili per l'esportazione.
3. Fare clic sul pulsante **Esporta**.
4. Nella finestra **Salva con nome** visualizzata, specificare il percorso e il nome del file di attività. Fare clic sul pulsante **Salva**.

   La finestra **Salva con nome** viene visualizzata solo se si utilizza Google Chrome, Microsoft Edge oppure Opera. Se si utilizza un altro browser, il file di attività viene salvato automaticamente nella cartella **Download**.

Importazione di un'attività

Kaspersky Security Center Cloud Console consente di importare un'attività da un file KLT. Il file KLT contiene l'attività esportata e le sue impostazioni.

Per importare un'attività:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

2. Fare clic sul pulsante **Importa**.

3. Fare clic sul pulsante **Sfoglia** per scegliere un file di attività da importare.

4. Nella finestra visualizzata, specificare il percorso del file di attività KLT, quindi fare clic sul pulsante **Apri**. Si noti che è possibile selezionare solo un file di attività.

   Viene avviata l'elaborazione dell'attività.

5. Dopo che l'attività è stata elaborata correttamente, selezionare i dispositivi a cui si desidera assegnare l'attività. A tale scopo, selezionare una delle seguenti opzioni:

   - **Assegna 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.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

   - **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.

     Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

   - **Assegna attività a una selezione dispositivi**

     L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

6. Specificare l'ambito dell'attività.

7. Fare clic sul pulsante **Completa** per completare l'importazione dell'attività.

Viene visualizzata la notifica con i risultati dell'importazione. Se l'attività viene importata correttamente, è possibile fare clic sul collegamento **Dettagli** per visualizzare le proprietà dell'attività.

Dopo un'importazione riuscita, l'attività viene visualizzata nell'elenco delle attività. Vengono importate anche le impostazioni e la pianificazione dell'attività. L'attività verrà avviata in base alla sua pianificazione.

Se l'attività appena importata ha un nome identico a un'attività esistente, il nome dell'attività importata viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Gestione dei dispositivi client

Questa sezione descrive come gestire i dispositivi nei gruppi di amministrazione.

Impostazioni di un dispositivo gestito

Per visualizzare le impostazioni di un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo richiesto.

Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.

Nella parte superiore della finestra delle proprietà vengono visualizzate le seguenti schede che rappresentano i principali gruppi di impostazioni:

- Generale

Questa scheda comprende le seguenti sezioni:

- La sezione **Generale** visualizza informazioni generali sul dispositivo client. Le informazioni sono fornite in base ai dati ricevuti durante l'ultima sincronizzazione del dispositivo client con Administration Server:
  - Nome

    In questo campo è possibile visualizzare e modificare il nome di un dispositivo client nel gruppo di amministrazione.
  - Descrizione

    In questo campo è possibile immettere un'ulteriore descrizione di un dispositivo client.
  - Stato dispositivo

    Stato del dispositivo client assegnato in base ai criteri definiti dall'amministratore per lo stato della protezione anti-virus nel dispositivo e l'attività del dispositivo nella rete.
  - Proprietario dispositivo

    Nome del proprietario del dispositivo. È possibile assegnare o rimuovere un utente come proprietario del dispositivo facendo clic sul collegamento **Gestisci proprietario dispositivo**.
  - Nome completo del gruppo

    Gruppo di amministrazione che include il dispositivo client.
  - Ultimo aggiornamento dei database anti-virus

    Data dell'ultimo aggiornamento delle applicazioni o dei database anti-virus.
  - Connesso ad Administration Server

    Data e ora dell'ultima connessione del Network Agent installato nel dispositivo client ad Administration Server.
  - Ultima visibilità

    Data e ora in cui il dispositivo è risultato visibile nella rete per l'ultima volta.
  - Versione di Network Agent

    Versione del Network Agent installato.
  - Data creazione

Data di creazione del dispositivo in Kaspersky Security Center Cloud Console.

- Non eseguire la disconnessione da Administration Server

  Se questa opzione è abilitata, viene mantenuta una connessione continua tra il dispositivo gestito e Administration Server. È consigliabile utilizzare questa opzione se non si utilizzano server push, che offrono questo tipo di connettività.

  Se questa opzione è disabilitata e i server push non sono in uso, il dispositivo gestito si connette ad Administration Server solo per sincronizzare i dati o trasmettere le informazioni.

  Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

  Questa opzione è disabilitata per impostazione predefinita nei dispositivi gestiti. Questa opzione è abilitata per impostazione predefinita nel dispositivo in cui è installato Administration Server e rimane abilitata anche se si tenta di disabilitarla.

- La sezione **Rete** visualizza le seguenti informazioni sulle proprietà di rete del dispositivo client:
  - Indirizzo IP

    Indirizzo IP del dispositivo.

  - Dominio Windows

    Gruppo di lavoro o dominio Windows che contiene il dispositivo.

  - Nome DNS

    Nome del dominio DNS del dispositivo client.

  - Nome NetBIOS

    Nome di rete di Windows del dispositivo client.

  - **Indirizzo IPv6**
- La sezione **Sistema** fornisce le informazioni sul sistema operativo installato nel dispositivo client.
  - **Sistema operativo**
  - **Architettura della CPU**
  - **Fornitore del sistema operativo**
  - **Cartella del sistema operativo**
  - **Nome dispositivo**
  - Tipo di macchina virtuale

Produttore della macchina virtuale.

- **Macchina virtuale dinamica come parte di VDI**

  Questa riga mostra se il dispositivo client è una macchina virtuale dinamica come parte della VDI.

- **Build del sistema operativo**

- Nella sezione **Protezione** vengono visualizzate le seguenti informazioni sullo stato corrente della protezione anti-virus nel dispositivo client:

  - **Visibile**

    Stato di visibilità del dispositivo client.

  - **Stato dispositivo**

    Stato del dispositivo client assegnato in base ai criteri definiti dall'amministratore per lo stato della protezione anti-virus nel dispositivo e l'attività del dispositivo nella rete.

  - **Descrizione stato**

    Stato della protezione del dispositivo client e della connessione ad Administration Server.

  - **Stato protezione**

    Questo campo indica lo stato corrente della protezione in tempo reale nel dispositivo client.

    Quando cambia lo stato del dispositivo, il nuovo stato viene visualizzato nella finestra delle proprietà del dispositivo solo dopo la sincronizzazione del dispositivo client con l'Administration Server.

  - **Ultima scansione completa**

    Data e ora dell'ultima scansione malware eseguita nel dispositivo client.

  - **Rilevato virus**

    Numero totale di minacce rilevate nel dispositivo client dall'installazione dell'applicazione anti-virus (prima scansione) o dall'ultimo azzeramento del contatore delle minacce.

  - **Oggetti per cui la disinfezione non è riuscita**

    Numero di file non elaborati nel dispositivo client.

    Questo campo ignora il numero di file non elaborati nei dispositivi mobili.

  - **Stato criptaggio disco**

Stato corrente del criptaggio dei file nelle unità locali del dispositivo. Per una descrizione degli stati consultare la Guida di Kaspersky Endpoint Security for Windows.

- La sezione **Stato dispositivo definito dall'applicazione** fornisce informazioni sullo stato del dispositivo definito dall'applicazione gestita installata nel dispositivo. Lo stato del dispositivo può essere diverso da quello definito da Kaspersky Security Center Cloud Console.

- Applicazioni

  In questa scheda sono elencate tutte le applicazioni Kaspersky installate nel dispositivo client. È possibile fare clic sul nome dell'applicazione per visualizzare informazioni generali sull'applicazione, un elenco di eventi che si sono verificati nel dispositivo e le impostazioni dell'applicazione.

- Criteri attivi e profili criterio

  In questa scheda sono elencati i criteri e i profili criterio attualmente attivi nel dispositivo gestito.

- Attività

  Nella scheda **Attività**, è possibile gestire le attività dei dispositivi client: visualizzare l'elenco delle attività esistenti, creare nuove attività, rimuovere, avviare e arrestare le attività, modificare le relative impostazioni e visualizzare i risultati dell'esecuzione. L'elenco delle attività è basato sui dati ricevuti durante l'ultima sessione di sincronizzazione del client con Administration Server. Administration Server richiede i dettagli dello stato delle attività al dispositivo client. Se la connessione non viene stabilita, lo stato non viene visualizzato.

- Eventi

  Nella scheda **Eventi** sono visualizzati gli eventi registrati in Administration Server per il dispositivo client selezionato.

- Problemi di sicurezza

  Nella scheda **Problemi di sicurezza**, è possibile visualizzare, modificare e creare problemi di sicurezza per il dispositivo client. I problemi di sicurezza possono essere creati automaticamente, tramite le applicazioni gestite Kaspersky installate nel dispositivo client, o manualmente, dall'amministratore. Se ad esempio alcuni utenti trasferiscono regolarmente malware dalle proprie unità rimovibili nei dispositivi, l'amministratore può creare un problema di sicurezza. L'amministratore può fornire una breve descrizione del caso e le azioni consigliate (ad esempio, azioni disciplinari da intraprendere nei confronti di un utente) nel testo del problema di sicurezza e può aggiungere un collegamento per l'utente o gli utenti.

  Un problema di sicurezza per cui sono state eseguite tutte le azioni richieste viene definito *elaborato*. La presenza di problemi di sicurezza non elaborati può essere selezionata come condizione per il passaggio dello stato del dispositivo a *Critico* o *Avviso*.

  Questa sezione contiene un elenco dei problemi di sicurezza creati per il dispositivo. I problemi di sicurezza sono classificati in base al tipo e al livello di criticità. Il tipo di un problema di sicurezza è definito dall'applicazione Kaspersky che crea il problema di sicurezza. È possibile evidenziare i problemi di sicurezza elaborati nell'elenco selezionando la casella di controllo nella colonna **Trattati**.

- Tag

Nella sezione **Tag** è possibile gestire l'elenco di parole chiave utilizzate per cercare i dispositivi client: visualizzare l'elenco dei tag esistenti, assegnare tag dall'elenco, configurare le regole per il tagging automatico, aggiungere nuovi tag e rinominare tag esistenti, nonché rimuovere tag.

- Avanzate

Questa scheda comprende le seguenti sezioni:

- **Registro delle applicazioni**. In questa sezione, è possibile visualizzare il registro delle applicazioni installate nel dispositivo client e i relativi aggiornamenti, nonché configurare la visualizzazione del registro delle applicazioni.

  Le informazioni sulle applicazioni installate vengono fornite se Network Agent installato nel dispositivo client invia le informazioni richieste ad Administration Server. È possibile configurare l'invio di informazioni ad Administration Server nella finestra delle proprietà di Network Agent o del relativo criterio, nella sezione **Archivi**.

  Facendo clic sul nome di un'applicazione, viene visualizzata una finestra che contiene i dettagli dell'applicazione e un elenco dei pacchetti di aggiornamento installati per l'applicazione.

- **File eseguibili**. In questa sezione sono visualizzati i file eseguibili rilevati nel dispositivo client.

- **Punti di distribuzione**. In questa sezione viene fornito un elenco dei punti di distribuzione con cui interagisce il dispositivo.

  - Esporta in un file

    Fare clic sul pulsante **Esporta in un file** per salvare in un file un elenco di punti di distribuzione con cui interagisce il dispositivo. Per impostazione predefinita, l'applicazione esporta l'elenco di dispositivi in un file CSV.

  - Proprietà

    Fare clic sul pulsante **Proprietà** per visualizzare e configurare il punto di distribuzione con cui interagisce il dispositivo.

- **Registro hardware**. In questa sezione è possibile visualizzare le informazioni relative all'hardware installato nel dispositivo client.

- **Aggiornamenti disponibili**. Questa sezione visualizza un elenco degli aggiornamenti software rilevati nel dispositivo, ma non ancora installati.

- **Vulnerabilità del software**. In questa sezione, sono fornite informazioni sulle vulnerabilità delle applicazioni di terze parti installate nei dispositivi client.

  Per salvare le vulnerabilità in un file, selezionare le caselle di controllo accanto alle vulnerabilità che si desidera salvare, quindi fare clic sul pulsante **Esporta in CSV** o sul pulsante **Esporta in TXT**.

  Questa sezione contiene le seguenti impostazioni:

  - Mostra solo le vulnerabilità che possono essere risolte

    Se questa opzione è abilitata, nella sezione verranno visualizzate le vulnerabilità che è possibile correggere tramite una patch.

    Se questa opzione è disabilitata, nella sezione verranno visualizzate sia le vulnerabilità che è possibile correggere tramite una patch che quelle per cui non è disponibile alcuna patch.

    Per impostazione predefinita, questa opzione è abilitata.

  - Proprietà vulnerabilità

Fare clic sul nome di una vulnerabilità del software nell'elenco per visualizzare le proprietà della vulnerabilità del software selezionata in una finestra separata. Nella finestra è possibile eseguire le seguenti operazioni:

- Ignorare la vulnerabilità del software in questo dispositivo gestito (in Administration Console o in Kaspersky Security Center Cloud Console).
- Visualizzare l'elenco delle correzioni consigliate per la vulnerabilità.
- Specificare manualmente gli aggiornamenti software per correggere la vulnerabilità (in Administration Console o in Kaspersky Security Center Cloud Console).
- Visualizzare le istanze della vulnerabilità.
- Visualizzare l'elenco delle attività esistenti per correggere la vulnerabilità e creare nuove attività per correggere la vulnerabilità.

- **Diagnostica remota**. In questa sezione, è possibile eseguire la diagnostica remota dei dispositivi client.

Selezioni dispositivi

Le *selezioni dispositivi* sono uno strumento per filtrare i dispositivi in base a condizioni specifiche. È possibile utilizzare le selezioni dispositivi per gestire diversi dispositivi, ad esempio per visualizzare un rapporto solo su questi dispositivi o per spostare tutti questi dispositivi in un altro gruppo.

Kaspersky Security Center Cloud Console offre un'ampia gamma di *selezioni predefinite* (ad esempio, **Dispositivi con stato Critico**, **Protezione disattivata** o **Rilevate minacce attive**). Le selezioni predefinite non possono essere eliminate. È inoltre possibile creare e configurare ulteriori *selezioni definite dall'utente*.

Nelle selezioni definite dall'utente è possibile impostare l'ambito di ricerca e selezionare tutti i dispositivi, i dispositivi gestiti o i dispositivi non assegnati. I parametri di ricerca sono specificati nelle condizioni. Nella selezione dispositivi è possibile creare diverse condizioni con parametri di ricerca differenti. È ad esempio possibile creare due condizioni e specificare intervalli IP diversi in ciascuna di esse. Se vengono specificate più condizioni, una selezione visualizza i dispositivi che soddisfano una qualsiasi delle condizioni. Al contrario, i parametri di ricerca in una condizione vengono sovrapposti. Se in una condizione si specificano sia un intervallo IP che il nome di un'applicazione installata, verranno visualizzati solo i dispositivi in cui è installata l'applicazione e con un indirizzo IP che appartiene all'intervallo specificato.

Visualizzazione dell'elenco dei dispositivi da una selezione di dispositivi

Kaspersky Security Center Cloud Console consente di visualizzare l'elenco dei dispositivi da una selezione di dispositivi.

Per visualizzare l'elenco dei dispositivi dalla selezione di dispositivi:

1. Nel menu principale, passare alla sezione **Risorse (dispositivi)** → **Selezioni dispositivi** o **Individuazione e distribuzione** → **Selezioni dispositivi**.
2. Nell'elenco delle selezioni fare clic sul nome della selezione di dispositivi.

La pagina mostra una tabella con le informazioni sui dispositivi inclusi nella selezione di dispositivi.

3. È possibile raggruppare e filtrare i dati della tabella dei dispositivi come segue:

   - Fare clic sull'icona delle impostazioni ( ), quindi selezionare le colonne da visualizzare nella tabella.
   - Fare clic sull'icona del filtro ( ), quindi specificare e applicare il criterio di filtro nel menu richiamato.

     Viene visualizzata la tabella filtrata dei dispositivi.

È possibile selezionare uno o più dispositivi nella selezione di dispositivi e fare clic sul pulsante **Nuova attività** per creare un'attività che verrà applicata a tali dispositivi.

Per spostare i dispositivi selezionati della selezione di dispositivi in un altro gruppo di amministrazione, fare clic sul pulsante **Sposta nel gruppo**, quindi selezionare il gruppo di amministrazione di destinazione.

Creazione di una selezione dispositivi

Per creare una selezione dispositivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Selezioni dispositivi**.

   Verrà visualizzata una pagina con un elenco di selezioni dispositivi.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Impostazioni della selezione dispositivi**.

3. Immettere il nome della nuova selezione.

4. Specificare il gruppo che contiene i dispositivi da includere nella selezione di dispositivi:

   - **Trova qualsiasi dispositivo**: ricerca dei dispositivi che soddisfano i criteri di selezione e inclusi nel gruppo **Dispositivi gestiti** o **Dispositivi non assegnati**.
   - **Trova dispositivi gestiti**: ricerca dei dispositivi che soddisfano i criteri di selezione e inclusi nel gruppo **Dispositivi gestiti**.
   - **Trova dispositivi non assegnati**: ricerca dei dispositivi che soddisfano i criteri di selezione e inclusi nel gruppo **Dispositivi non assegnati**.

   È possibile abilitare la casella di controllo **Includi i dati degli Administration Server secondari** per abilitare la ricerca dei dispositivi che soddisfano i criteri di selezione e gestiti dagli Administration Server secondari.

5. Fare clic sul pulsante **Aggiungi**.

6. Nella finestra visualizzata specificare le condizioni che devono essere soddisfatte per includere i dispositivi in questa selezione, quindi fare clic sul pulsante **OK**.

7. Fare clic sul pulsante **Salva**.

La selezione dispositivi viene creata e aggiunta all'elenco delle selezioni dispositivi.

Configurazione di una selezione dispositivi

Per configurare una selezione dispositivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Selezioni dispositivi**.

   Verrà visualizzata una pagina con un elenco di selezioni dispositivi.

2. Selezionare la selezione di dispositivi definita dall'utente pertinente e fare clic sul pulsante **Proprietà**.

   Verrà visualizzata la finestra **Impostazioni della selezione dispositivi**.

3. Nella scheda **Generale**, fare clic sul collegamento **Nuova condizione**.

4. Specificare le condizioni da soddisfare per l'inclusione dei dispositivi nella selezione.

5. Fare clic sul pulsante **Salva**.

   Le impostazioni verranno applicate e salvate.

Di seguito sono descritte le condizioni per l'assegnazione dei dispositivi a una selezione. Le condizioni vengono combinate tramite l'operatore logico OR: la selezione conterrà i dispositivi conformi ad almeno una delle condizioni elencate.

Generale

Nella sezione **Generale** è possibile modificare il nome della condizione di selezione e specificare se tale condizione deve essere invertita:

Inverti condizione selezione

Se questa opzione è abilitata, la condizione di selezione specificata verrà invertita. La selezione includerà tutti i dispositivi che non soddisfano la condizione.

Per impostazione predefinita, questa opzione è disabilitata.

Infrastruttura di rete

Nella sottosezione **Rete**, è possibile specificare i criteri che verranno utilizzati per includere i dispositivi nella selezione in base ai dati della rete:

- Nome dispositivo

  Nome di rete Windows (nome NetBIOS) del dispositivo o indirizzo IPv4 o IPv6.

- Dominio

  Visualizza tutti i dispositivi inclusi nel dominio Windows specificato.

- Gruppo di amministrazione

  Visualizza i dispositivi inclusi nel gruppo di amministrazione specificato.

- Descrizione

  Testo contenuto nella finestra delle proprietà del dispositivo: nel campo **Descrizione** della sezione **Generale**.

  Per inserire il testo nel campo **Descrizione**, è possibile utilizzare i seguenti caratteri:

  - All'interno di una parola:

    - *. Sostituisce qualsiasi stringa con qualsiasi numero di caratteri.

    Esempio:

    Per descrivere parole come **Server** o **Server's**, è possibile immettere **Server***.

    - **?.** Sostituisce qualsiasi carattere singolo.

    Esempio:

    Per descrivere parole come **Finestra** o **Finestre**, è possibile immettere **Finestr?**.

    Non è possibile utilizzare l'asterisco (*****) o il punto interrogativo (**?**) come primo carattere nella query.

  - Per trovare più parole:

    - Spazio. Visualizza tutti i dispositivi le cui descrizioni contengono una delle parole elencate.

    Esempio:

    Per trovare una frase contenente le parole **Secondario** o **Virtuale**, è possibile includere la riga **Secondario Virtuale** nella query.

    - **+**. Quando una parola è preceduta dal segno +, tutti i risultati della ricerca conterranno tale parola.

    Esempio:

    Per trovare una frase contenente sia **Secondario** che **Virtuale**, immettere la query **+Secondario+Virtuale**.

    - **-**. Quando una parola è preceduta dal segno -, nessun risultato della ricerca conterrà tale parola.

    Esempio:

    Per trovare una frase contenente **Secondario** e non contenente **Virtuale**, immettere la query **+Secondario-Virtuale**.

    - **"<testo>"**. Verranno visualizzati i risultati che contengono il testo racchiuso tra virgolette.

    Esempio:

    Per trovare una frase contenente la combinazione di parole **Server secondario**, è possibile immettere **"Server secondario"** nella query.

- Intervallo IP

  Se questa opzione è abilitata, è possibile immettere gli indirizzi IP iniziale e finale dell'intervallo IP in cui i dispositivi rilevanti devono essere inclusi.

  Per impostazione predefinita, questa opzione è disabilitata.

- Gestito da un altro Administration Server

Selezionare uno dei seguenti valori:

- **Sì**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti da altri Administration Server. Questi server sono diversi dal server su cui si configura la regola di spostamento dei dispositivi.
- **No**. La regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti dall'Administration Server corrente.
- **Nessun valore selezionato**. La condizione non si applica.

Nella sottosezione **Active Directory**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base ai dati di Active Directory:

- Il dispositivo si trova in un'unità organizzativa di Active Directory

  Se questa opzione è abilitata, la selezione includerà i dispositivi dell'unità organizzativa Active Directory specificata nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

- Includi unità organizzative secondarie

  Se questa opzione è abilitata, la selezione includerà i dispositivi in tutte le unità organizzative secondarie dell'unità organizzativa di Active Directory specificata.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il dispositivo fa parte di un gruppo di Active Directory

  Se questa opzione è abilitata, la selezione includerà i dispositivi del gruppo Active Directory specificato nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Attività di rete**, è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base alle relative attività della rete:

- Funge da punto di distribuzione

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione include i dispositivi che operano come punti di distribuzione.
  - **No**. I dispositivi che operano come punti di distribuzione non sono inclusi nella selezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Non eseguire la disconnessione da Administration Server

Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

- **Abilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è selezionata.
- **Disabilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è deselezionata.
- **Nessun valore selezionato**. Il criterio non verrà applicato.

- Profilo connessione cambiato

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **No**. La selezione non includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Ultima connessione ad Administration Server

  È possibile utilizzare questa casella di controllo per impostare un criterio di ricerca per i dispositivi in base all'ora dell'ultima connessione ad Administration Server.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stata stabilita l'ultima connessione tra Network Agent installato nel dispositivo client e Administration Server. La selezione includerà i dispositivi che rientrano nell'intervallo specificato.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Rilevati nuovi dispositivi durante il polling della rete

  Cerca nuovi dispositivi rilevati dal polling della rete negli ultimi giorni.

  Se questa opzione è abilitata, la selezione includerà soltanto i nuovi dispositivi rilevati dalla device discovery nel numero di giorni specificato nel campo **Periodo di rilevamento (giorni)**.

  Se questa opzione è disabilitata, la selezione includerà tutti i dispositivi rilevati dalla device discovery.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il dispositivo è visibile

Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

- **Sì**. L'applicazione include nella selezione i dispositivi attualmente visibili nella rete.
- **No**. L'applicazione include nella selezione i dispositivi attualmente invisibili nella rete.
- **Nessun valore selezionato**. Il criterio non verrà applicato.

Nella sottosezione **Segmenti cloud**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base ai rispettivi segmenti cloud:

- Il dispositivo si trova in un segmento cloud

  Se questa opzione è abilitata, è possibile scegliere i dispositivi dai segmenti cloud AWS, Azure e Google.

  Se anche l'opzione **Includi gli oggetti figlio** è abilitata, la ricerca viene eseguita in tutti gli oggetti figlio del segmento selezionato.

  I risultati di ricerca includono solo i dispositivi del segmento selezionato.

- Dispositivo rilevato tramite l'API

  Nell'elenco a discesa, è possibile selezionare se un dispositivo deve essere rilevato o meno dagli strumenti API:

  - **Sì**. Il dispositivo viene rilevato tramite l'API AWS, Azure o Google.
  - **No**. Il dispositivo non può essere rilevato tramite l'API AWS, Azure o Google. In altre parole, il dispositivo si trova all'esterno dell'ambiente cloud o si trova nell'ambiente cloud ma non può essere rilevato tramite un'API.
  - Nessun valore. Questa condizione non viene applicata.

Stati dispositivi

Nella sottosezione **Stato del dispositivo gestito**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base alla descrizione dello stato dei dispositivi ottenuta da un'applicazione gestita:

- Stato dispositivo

  Elenco a discesa in cui è possibile selezionare uno degli stati del dispositivo: *OK*, *Critico* o *Avviso*.

- Stato protezione in tempo reale

  Elenco a discesa in cui è possibile selezionare lo stato della protezione in tempo reale. I dispositivi con lo stato della protezione in tempo reale specificato vengono inclusi nella selezione.

- Descrizione stato del dispositivo

In questo campo è possibile selezionare le caselle di controllo accanto alle condizioni che, se soddisfatte, assegnano al dispositivo uno dei seguenti stati: *OK*, *Critico* o *Avviso*.

Nella sezione **Stato dei componenti nelle applicazioni gestite**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base agli stati dei componenti nelle applicazioni gestite:

- Stato prevenzione fughe di dati

  Cercare i dispositivi in base allo stato di prevenzione della perdita dei dati (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

- Stato protezione server di collaborazione

  Cercare i dispositivi in base allo stato di protezione della collaborazione server (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

- Stato protezione anti-virus server di posta

  Cercare i dispositivi in base allo stato di protezione dei server di posta (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

- Stato Endpoint Sensor

  Cercare i dispositivi in base allo stato del componente Sensore Endpoint (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

Nella sezione **Problemi che influiscono sullo stato nelle applicazioni gestite** è possibile specificare i criteri per l'inclusione dei dispositivi nella selezione in base all'elenco dei possibili problemi rilevati da un'applicazione gestita. Se è presente almeno un problema selezionato in un dispositivo, il dispositivo verrà incluso nella selezione. Quando si seleziona un problema elencato per diverse applicazioni, è possibile selezionare automaticamente questo problema in tutti gli elenchi.

È possibile selezionare le caselle di controllo relative alle descrizioni degli stati dall'applicazione gestita. Alla ricezione di questi stati, i dispositivi verranno inclusi nella selezione. Quando si seleziona uno stato elencato per diverse applicazioni, è possibile selezionare automaticamente questo stato in tutti gli elenchi.

Dettagli di sistema

Nella sezione **Sistema operativo** è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base al tipo di sistema operativo.

- Tipo di piattaforma

  Se la casella di controllo è selezionata, è possibile selezionare un sistema operativo dall'elenco. I dispositivi in cui sono installati i sistemi operativi specificati saranno inclusi nei risultati della ricerca.

- Versione Service Pack del sistema operativo

In questo campo è possibile specificare la versione del pacchetto del sistema operativo (nel formato *X.Y*), da cui dipenderà l'applicazione della regola di spostamento al dispositivo. Per impostazione predefinita, non è specificato alcun valore per la versione.

- Dimensioni in bit del sistema operativo

  Nell'elenco a discesa è possibile selezionare l'architettura del sistema operativo da cui dipenderà l'applicazione della regola di spostamento al dispositivo (**Sconosciuto**, **x86**, **AMD64** o **IA64**). Per impostazione predefinita, non è selezionata alcuna opzione nell'elenco, pertanto l'architettura del sistema operativo non è definita.

- Build del sistema operativo

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Numero di build del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un numero di build uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti i numeri di build ad eccezione di quello specificato.

- Numero di rilascio del sistema operativo

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Identificatore della versione (ID) del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un ID di rilascio uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti gli ID di rilascio ad eccezione di quello specificato.

Nella sezione **Macchine virtuali** è possibile configurare i criteri per l'inclusione dei dispositivi nella selezione in base al fatto che siano macchine virtuali o che facciano parte di Microsoft Virtual Desktop Infrastructure (VDI):

- Questa è una macchina virtuale

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Indefinito**.
  - **No**. I dispositivi che non sono macchine virtuali vengono trovati.
  - **Sì**. Vengono trovati i dispositivi che sono macchine virtuali.

- Tipo di macchina virtuale

  Nell'elenco a discesa è possibile selezionare il produttore della macchina virtuale.

  Questo elenco a discesa è disponibile se è selezionato il valore **Sì** o **Non importante** nell'elenco a discesa **Questa è una macchina virtuale**.

- Parte di Virtual Desktop Infrastructure

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Indefinito**.
  - **No**. Vengono trovati i dispositivi che non fanno parte di Virtual Desktop Infrastructure.
  - **Sì**. Vengono trovati i dispositivi che fanno parte di Microsoft Virtual Desktop Infrastructure (VDI).

Nella sottosezione **Registro hardware**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'hardware installato:

Assicurarsi che l'utilità lshw sia installata nei dispositivi Linux da cui si desidera recuperare i dettagli dell'hardware. I dettagli dell'hardware recuperati dalle macchine virtuali potrebbero essere incompleti a seconda dell'hypervisor utilizzato.

- Dispositivo

  Nell'elenco a discesa è possibile selezionare un tipo di unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- Fornitore

  Nell'elenco a discesa è possibile selezionare il nome di un produttore dell'unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- Nome dispositivo

  Nome del dispositivo nella rete Windows. Il dispositivo con il nome specificato verrà incluso nella selezione.

- Descrizione

  Descrizione del dispositivo o dell'unità hardware. I dispositivi con la descrizione specificata in questo campo verranno inclusi nella selezione.

  La descrizione di un dispositivo in qualsiasi formato può essere immessa nella finestra delle proprietà del dispositivo. Il campo supporta la ricerca full-text.

- Produttore dispositivo

  Nome del produttore del dispositivo. I dispositivi del produttore specificato in questo campo verranno inclusi nella selezione.

  È possibile inserire il nome del produttore nella finestra delle proprietà di un dispositivo.

- Numero di serie

Tutte le unità hardware con il numero di serie specificato in questo campo verranno incluse nella selezione.

- **Numero di inventario**

  L'apparecchiatura con il numero di inventario specificato in questo campo verrà inclusa nella selezione.

- **Utente**

  Tutte le unità hardware dell'utente specificato in questo campo verranno incluse nella selezione.

- **Posizione**

  Posizione del dispositivo o dell'unità hardware (ad esempio nella sede principale o in una filiale). I computer o gli altri dispositivi distribuiti al percorso specificato in questo campo verranno inclusi nella selezione.

  È possibile descrivere il percorso di un dispositivo in qualsiasi formato nella finestra delle proprietà del dispositivo.

- **Frequenza di clock della CPU (in MHz) da**

  La frequenza di clock minima di una CPU. I dispositivi con una CPU che corrisponde all'intervallo di frequenza di clock specificati nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Frequenza di clock della CPU (in MHz) a**

  La frequenza di clock massima di una CPU. I dispositivi con una CPU che corrisponde all'intervallo di frequenza di clock specificati nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Numero di core CPU virtuali, da**

  Il numero minimo di core CPU virtuali. I dispositivi con una CPU che corrisponde all'intervallo del numero di core virtuali specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Numero di core CPU virtuali, a**

  Il numero massimo di core CPU virtuali. I dispositivi con una CPU che corrisponde all'intervallo del numero di core virtuali specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Volume disco rigido (GB) da**

  Il volume minimo del disco rigido sul dispositivo. I dispositivi con un disco rigido che corrisponde all'intervallo di volumi nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Volume disco rigido (GB) a**

  Il volume massimo del disco rigido sul dispositivo. I dispositivi con un disco rigido che corrisponde all'intervallo di volumi nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Dimensione RAM (MB) da**

La dimensione minima della RAM del dispositivo. I dispositivi con una RAM che corrisponde all'intervallo di dimensione specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

- Dimensione RAM (MB) a

  La dimensione massima della RAM del dispositivo. I dispositivi con una RAM che corrisponde all'intervallo di dimensione specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

Dettagli software di terze parti

Nella sottosezione **Registro delle applicazioni**, è possibile impostare i criteri di ricerca dei dispositivi in base alle applicazioni installate:

- Nome applicazione

  Elenco a discesa da cui è possibile selezionare un'applicazione. I dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- Versione applicazione

  Campo di immissione in cui è possibile specificare la versione dell'applicazione selezionata.

- Fornitore

  Elenco a discesa da cui è possibile selezionare il produttore di un'applicazione installata nel dispositivo.

- Stato applicazione

  Elenco a discesa da cui è possibile selezionare lo stato di un'applicazione (*Installata*, *Non installata*). Verranno inclusi nella selezione i dispositivi in cui è installata o non è installata l'applicazione specificata, in base allo stato selezionato.

- Trova per aggiornamento

  Se questa opzione è abilitata, la ricerca verrà eseguita utilizzando i dettagli degli aggiornamenti per le applicazioni installate nei dispositivi. Dopo aver selezionato la casella di controllo, i campi **Nome applicazione**, **Versione applicazione** e **Stato applicazione** diventano rispettivamente **Nome aggiornamento**, **Versione aggiornamento** e **Stato**.

  Per impostazione predefinita, questa opzione è disabilitata.

- Nome dell'applicazione di protezione incompatibile

  Elenco a discesa da cui è possibile selezionare applicazioni di protezione di terze parti. Durante la ricerca, i dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- Tag applicazione

Nell'elenco a discesa è possibile selezionare il tag di un'applicazione. Tutti i dispositivi che hanno applicazioni installate con il tag selezionato nella descrizione sono inclusi nella selezione dispositivi.

- Applica ai dispositivi senza i tag specificati

  Se questa opzione è abilitata, la selezione includerà i dispositivi con descrizioni che non contengono alcuno dei tag selezionati.

  Se questa opzione è disabilitata, il criterio non viene applicato.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Vulnerabilità e aggiornamenti**, è possibile specificare i criteri per l'inclusione dei dispositivi nella selezione in base all'origine di Windows Update:

WUA è passato ad Administration Server

È possibile selezionare una delle seguenti opzioni di ricerca nell'elenco a discesa:

- **Sì**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da Administration Server.
- **No**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da altre origini.

Dettagli delle applicazioni Kaspersky

Nella sottosezione **Applicazioni Kaspersky**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'applicazione gestita selezionata:

- Nome applicazione

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome di un'applicazione Kaspersky.

  L'elenco contiene solo i nomi delle applicazioni con plug-in di gestione installati nella workstation di amministrazione.

  Se non è selezionata alcuna applicazione, il criterio non verrà applicato.

- Versione applicazione

  Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al numero versione di un'applicazione Kaspersky.

  Se non è specificato alcun numero di versione, il criterio non verrà applicato.

- Nome aggiornamento critico

  Elenco a discesa da cui è possibile selezionare lo stato di un'applicazione (*Installata*, *Non installata*). Verranno inclusi nella selezione i dispositivi in cui è installata o non è installata l'applicazione specificata, in base allo stato selezionato.

Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome dell'applicazione o al numero del pacchetto di aggiornamento.

Se il campo è vuoto, il criterio non verrà applicato.

- Selezionare il periodo dell'ultimo aggiornamento dei moduli

  È possibile utilizzare questa opzione per impostare un criterio per la ricerca dei dispositivi in base all'ora dell'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stato eseguito l'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Il dispositivo è gestito tramite Administration Server

  Nell'elenco a discesa, è possibile includere nella selezione i dispositivi gestiti tramite Kaspersky Security Center Cloud Console:

  - **Sì**. L'applicazione include nella selezione i dispositivi gestiti tramite Kaspersky Security Center Cloud Console.
  - **No**. L'applicazione include nella selezione i dispositivi non gestiti tramite Kaspersky Security Center Cloud Console.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- L'applicazione di protezione è installata

  Nell'elenco a discesa è possibile includere nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione:

  - **Sì**. L'applicazione include nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione.
  - **No**. L'applicazione include nella selezione tutti i dispositivi in cui non è installata un'applicazione di protezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Nella sottosezione **Protezione anti-virus**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base allo stato della protezione:

- Data rilascio database

  Se questa opzione è selezionata, è possibile eseguire la ricerca dei dispositivi client in base alla data di rilascio del database anti-virus. Nei campi di immissione è possibile impostare l'intervallo di tempo in base al quale eseguire la ricerca.

  Per impostazione predefinita, questa opzione è disabilitata.

- Conteggio record database

Se questa opzione è abilitata, è possibile eseguire la ricerca di dispositivi client in base al numero di record del database. Nei campi di immissione è possibile impostare i valori di soglia inferiore e superiore per i record del database anti-virus.

Per impostazione predefinita, questa opzione è disabilitata.

- **Ultima scansione**

  Se questa opzione è abilitata, è possibile eseguire la ricerca dei dispositivi client in base all'ora dell'ultima scansione malware. Nei campi di immissione è possibile specificare il periodo di tempo entro il quale è stata eseguita l'ultima scansione malware.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Minacce**

  Algoritmo di cifratura a blocchi AES (Advanced Encryption Standard). Nell'elenco a discesa è possibile selezionare le dimensioni della chiave di criptaggio (56 bit, 128 bit, 192 bit o 256 bit).

  Valori disponibili: *AES56*, *AES128*, *AES192* e *AES256*.

  Se questa opzione è abilitata, è possibile eseguire la ricerca di dispositivi client in base al numero di virus rilevati. Nei campi di immissione è possibile impostare i valori di soglia inferiore e superiore per il numero di virus trovati.

  Per impostazione predefinita, questa opzione è disabilitata.

La sottosezione **Componenti dell'applicazione** contiene un elenco dei componenti delle applicazioni per cui sono installati plug-in di gestione corrispondenti in Kaspersky Security Center Cloud Console.

Nella sottosezione **Componenti dell'applicazione**, è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base agli stati e ai numeri di versione dei componenti che fanno riferimento all'applicazione selezionata:

- **Stato**

Ricerca dei dispositivi in base allo stato dei componenti inviato da un'applicazione all'Administration Server. È possibile selezionare uno dei seguenti stati: *N/D, Arrestato*, *Sospeso*, *Avvio in corso*, *In esecuzione, Non riuscito, Non installato, Non supportato dalla licenza*. Se il componente selezionato dell'applicazione installata in un dispositivo gestito presenta lo stato specificato, il dispositivo viene incluso nella selezione dispositivi.

Stati inviati dalle applicazioni:

- *Arrestato* - Il componente è disabilitato e al momento non è in esecuzione.
- *Sospeso* - Il componente è sospeso, ad esempio dopo che l'utente ha sospeso la protezione nell'applicazione gestita.
- *Avvio in corso* - Il componente è attualmente in fase di inizializzazione.
- *In esecuzione* - Il componente è abilitato e correttamente in esecuzione.
- *Non riuscito* - Si è verificato un errore durante l'esecuzione del componente.
- *Non installato* - L'utente non ha selezionato il componente per l'installazione durante la configurazione dell'installazione personalizzata dell'applicazione.
- *Non supportato dalla licenza* - La licenza non copre il componente selezionato.

A differenza degli altri stati, lo stato *N/D* non viene inviato dalle applicazioni. Questa opzione indica che le applicazioni non dispongono di alcuna informazione sullo stato del componente selezionato. Ciò può ad esempio verificarsi quando il componente selezionato non appartiene ad alcuna delle applicazioni installate nel dispositivo o quando il dispositivo è spento.

- **Versione**

  Ricerca dei dispositivi in base al numero di versione del componente selezionato nell'elenco. È possibile digitare un numero di versione, ad esempio `3.4.1.0`, e quindi specificare se il componente selezionato deve avere una versione uguale, precedente o successiva. È anche possibile configurare la ricerca di tutte le versioni ad eccezione di quella specificata.

Tag

Nella sezione **Tag** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base alle parole chiave (tag) che sono state aggiunte in precedenza alle descrizioni dei dispositivi gestiti:

Applica se almeno uno dei tag specificati corrisponde

Se questa opzione è abilitata, i risultati di ricerca visualizzeranno i dispositivi con descrizioni contenenti almeno uno dei tag selezionati.

Se questa opzione è disabilitata, i risultati di ricerca visualizzeranno solo i dispositivi con descrizioni contenenti tutti i tag selezionati.

Per impostazione predefinita, questa opzione è disabilitata.

Per aggiungere tag al criterio, fare clic sul pulsante **Aggiungi** e selezionare i tag facendo clic sul campo di immissione **Tag**. Specificare se includere o escludere i dispositivi con i tag selezionati nella selezione di dispositivi.

- **Deve essere incluso**

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

  Per impostazione predefinita, questa opzione è selezionata.

- **Deve essere escluso**

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni non contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

Utenti

Nella sezione **Utenti** è possibile impostare i criteri per l'inclusione dei dispositivi nella selezione in base agli account degli utenti che hanno eseguito l'accesso al sistema operativo.

- **Ultimo utente che ha eseguito l'accesso al sistema**

  Se questa opzione è abilitata, è possibile selezionare l'account utente per configurare il criterio. Si noti che l'elenco degli utenti viene filtrato e mostra gli utenti interni. I risultati della ricerca includeranno i dispositivi in cui l'utente selezionato ha eseguito l'ultimo accesso al sistema.

- **Utente che ha eseguito l'accesso al sistema almeno una volta**

  Se questa opzione è abilitata, è possibile selezionare l'account utente per configurare il criterio. Si noti che l'elenco degli utenti viene filtrato e mostra gli utenti interni. I risultati della ricerca includeranno i dispositivi in cui l'utente specificato ha eseguito l'accesso al sistema almeno una volta.

Esportazione dell'elenco dei dispositivi da una selezione di dispositivi

Kaspersky Security Center Cloud Console consente di salvare le informazioni sui dispositivi da una selezione di dispositivi ed esportarle in un file CSV o TXT.

Per esportare l'elenco dei dispositivi dalla selezione di dispositivi:

1. Aprire la tabella con i dispositivi dalla selezione di dispositivi.
2. Utilizzare uno dei seguenti metodi per selezionare i dispositivi che si desidera esportare:
   - Per selezionare dispositivi specifici, selezionare le caselle di controllo accanto ad essi.
   - Per selezionare tutti i dispositivi dalla pagina della tabella corrente, selezionare la casella di controllo nell'intestazione della tabella dei dispositivi, quindi selezionare la casella di controllo **Seleziona tutto nella pagina corrente**.
   - Per selezionare tutti i dispositivi dalla tabella, selezionare la casella di controllo nell'intestazione della tabella dei dispositivi, quindi selezionare la casella di controllo **Seleziona tutto**.

Fare clic sul pulsante **Esporta in CSV** o **Esporta in TXT**. Tutte le informazioni sui dispositivi selezionati inclusi nella tabella verranno esportate.

Si noti che se è stato applicato un criterio di filtraggio alla tabella dei dispositivi, solo i dati filtrati dalle colonne visualizzate verranno esportati.

Rimozione di dispositivi dai gruppi di amministrazione in una selezione

Durante l'utilizzo di una selezione dispositivi, è possibile rimuovere i dispositivi dai gruppi di amministrazione in questa selezione senza passare ai gruppi di amministrazione da cui devono essere rimossi i dispositivi.

Per rimuovere dispositivi dai gruppi di amministrazione:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Selezioni dispositivi** o **Individuazione e distribuzione** → **Selezioni dispositivi**.
2. Nell'elenco delle selezioni fare clic sul nome della selezione di dispositivi.

   La pagina mostra una tabella con le informazioni sui dispositivi inclusi nella selezione di dispositivi.
3. Selezionare i dispositivi che si desidera rimuovere, quindi fare clic su **Elimina**.

   I dispositivi selezionati verranno rimossi dai gruppi di amministrazione corrispondenti.

Visualizzazione e configurazione delle azioni per i dispositivi inattivi

È possibile ottenere notifiche relative ai dispositivi client all'interno di un gruppo che risultano inattivi. È anche possibile eliminare automaticamente tali dispositivi.

Per visualizzare o configurare le azioni eseguite quando i dispositivi nel gruppo risultano inattivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Fare clic sul nome del gruppo di amministrazione desiderato.

   Verrà visualizzata la finestra delle proprietà dal gruppo di amministrazione.
3. Nella finestra delle proprietà passare alla scheda **Impostazioni**.
4. Nella sezione **Ereditarietà** abilitare o disabilitare le seguenti opzioni:

   - Eredita da gruppo padre

     Le impostazioni di questa sezione saranno ereditate dal gruppo padre di cui fa parte il dispositivo client. Se questa opzione è abilitata, le impostazioni in **Attività dei dispositivi nella rete** sono bloccate dalle modifiche.

     Questa opzione è disponibile solo se il gruppo di amministrazione ha un gruppo padre.

     Per impostazione predefinita, questa opzione è abilitata.

- **Forza ereditarietà delle impostazioni nei gruppi figlio**

  I valori delle impostazioni vengono distribuiti ai gruppi figlio, ma nelle proprietà dei gruppi figlio tali impostazioni sono bloccate.

  Per impostazione predefinita, questa opzione è disabilitata.

5. Nella sezione **Attività dei dispositivi** abilitare o disabilitare le seguenti opzioni:

- **Avvisa l'amministratore se il dispositivo è inattivo da più di (giorni)**

  Se questa opzione è abilitata, l'amministratore riceve le notifiche sui dispositivi inattivi. È possibile specificare l'intervallo di tempo al termine del quale verrà creato l'evento **Il dispositivo risulta inattivo nella rete da molto tempo**. L'intervallo di tempo predefinito è 7 giorni.

  Per impostazione predefinita, questa opzione è abilitata.

- **Rimuovi il dispositivo dal gruppo se è inattivo da più di (giorni)**

  Se questa opzione è abilitata, è possibile specificare l'intervallo di tempo al termine del quale il dispositivo viene rimosso automaticamente dal gruppo. L'intervallo di tempo predefinito è 60 giorni.

  Per impostazione predefinita, questa opzione è abilitata.

6. Fare clic su **Salva**.

Le modifiche verranno salvate e applicate.

Informazioni sugli stati dei dispositivi

Kaspersky Security Center Cloud Console assegna uno stato a ciascun dispositivo gestito. Lo stato specifico dipende dal rispetto delle condizioni definite dall'utente. In alcuni casi, durante l'assegnazione di uno stato a un dispositivo, Kaspersky Security Center Cloud Console prende in considerazione il flag di visibilità del dispositivo nella rete (vedere la tabella seguente). Se Kaspersky Security Center Cloud Console non rileva un dispositivo nella rete entro due ore, il flag di visibilità del dispositivo è impostato su *Non visibile*.

Gli stati sono i seguenti:

- *Critico* o *Critico / Visibile*
- *Avviso* o *Avviso / Visibile*
- *OK* o *OK / Visibile*

La tabella seguente elenca le condizioni predefinite da soddisfare per assegnare a un dispositivo lo stato *Critico* o *Avviso*, con tutti i possibili valori.

Condizioni per l'assegnazione di uno stato a un dispositivo

Condizione	Descrizione della condizione	Valori disponibili
Applicazione di protezione non installata	Network Agent è installato nel dispositivo, ma un'applicazione di protezione non è installata.	• L'interruttore è attivato.

		• L'interruttore è disattivato.
Troppi virus rilevati	Nel dispositivo sono stati rilevati alcuni virus da parte di un'attività per il rilevamento dei virus, ad esempio l'attività Scansione virus, e il numero di virus trovati supera il valore specificato.	Più di 0.
Livello protezione in tempo reale diverso da quello impostato dall'amministratore	Il dispositivo è visibile nella rete, ma il livello della protezione in tempo reale è diverso dal livello impostato (nella condizione) dall'amministratore per lo stato del dispositivo.	• Arrestata. • Sospesa. • In esecuzione.
Scansione malware non eseguita da molto tempo	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma né l'attività *Scansione malware* né un'attività di scansione locale sono state eseguite nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server 7 giorni o più di 7 giorni prima.	Più di 1 giorno.
I database non sono aggiornati	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma i database anti-virus non vengono aggiornati nel dispositivo nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server un giorno o più di un giorno prima.	Più di 1 giorno.
Connessione non eseguita da molto tempo	Network Agent è installato nel dispositivo, ma il dispositivo non viene connesso a un Administration Server nell'intervallo di tempo specificato, perché il dispositivo era spento.	Più di 1 giorno.
Rilevate minacce attive	Il numero di oggetti non elaborati nella cartella **Minacce attive** è superiore al valore specificato.	Più di 0 elementi.
È necessario il riavvio	Il dispositivo è visibile nella rete, ma un'applicazione richiede il riavvio del dispositivo da un periodo superiore all'intervallo di tempo specificato e per uno dei motivi selezionati.	Più di 0 minuti.
Applicazioni incompatibili installate	Il dispositivo è visibile nella rete, ma l'inventario software eseguito tramite Network Agent ha rilevato applicazioni incompatibili installate nel dispositivo.	• L'interruttore è disattivato. • L'interruttore è attivato.
Rilevate vulnerabilità del software	Il dispositivo è visibile nella rete e Network Agent è installato nel dispositivo, ma l'attività *Trova vulnerabilità e aggiornamenti richiesti* ha rilevato vulnerabilità con il livello di criticità specificato nelle applicazioni installate nel dispositivo.	• Critico. • Alto. • Medio. • Ignora se non è possibile correggere il tipo di vulnerabilità.

		• Ignora se un aggiornamento è assegnato per l'installazione.
La licenza è scaduta	Il dispositivo è visibile nella rete, ma la licenza è scaduta.	• L'interruttore è disattivato. • L'interruttore è attivato.
La licenza sta per scadere	Il dispositivo è visibile nella rete, ma la licenza nel dispositivo scadrà tra un numero di giorni inferiore rispetto a quello specificato.	Più di 0 giorni.
Verifica disponibilità aggiornamenti di Windows Update non eseguita da molto tempo	Il dispositivo è visibile nella rete, ma l'attività Esegui sincronizzazione di Windows Update non viene eseguita nell'intervallo di tempo specificato.	Più di 1 giorno.
Stato criptaggio non valido	Network Agent è installato nel dispositivo, ma il risultato del criptaggio dispositivo è uguale al valore specificato.	• Non è conforme al criterio a causa di un rifiuto dell'utente (solo per i dispositivi esterni). • Non è conforme al criterio a causa di un errore. • È richiesto il riavvio per l'applicazione del criterio. • Non è specificato alcun criterio di criptaggio. • Non supportato. • Quando viene applicato il criterio.

Impostazioni dispositivo mobile non conformi al criterio	Le impostazioni del dispositivo mobile sono diverse dalle impostazioni specificate nel criterio di Kaspersky Endpoint Security for Android durante il controllo delle regole di conformità.	• L'interruttore è disattivato. • L'interruttore è attivato.
Problemi di sicurezza non elaborati rilevati	Sono stati rilevati nel dispositivo alcuni problemi di sicurezza non elaborati. I problemi di sicurezza possono essere creati automaticamente, tramite le applicazioni gestite Kaspersky installate nel dispositivo client, o manualmente, dall'amministratore.	• L'interruttore è disattivato. • L'interruttore è attivato.
Stato dispositivo definito dall'applicazione	Lo stato del dispositivo è definito dall'applicazione gestita.	• L'interruttore è disattivato. • L'interruttore è attivato.
Spazio su disco esaurito nel dispositivo	Lo spazio disponibile sul disco nel dispositivo è inferiore al valore specificato o il dispositivo non può essere sincronizzato con Administration Server. Lo stato *Critico* o *Avviso* diventa *OK* quando il dispositivo viene sincronizzato con Administration Server e lo spazio disponibile nel dispositivo è maggiore o uguale al valore specificato.	Più di 0 MB.
Il dispositivo è diventato non gestito	Durante l'individuazione dispositivi, il dispositivo è stato riconosciuto come visibile nella rete, ma più di tre tentativi di sincronizzazione con Administration Server hanno avuto esito negativo.	• L'interruttore è disattivato. • L'interruttore è attivato.
Protezione disattivata	Il dispositivo è visibile nella rete, ma l'applicazione di protezione nel dispositivo è stata disabilitata per un periodo superiore all'intervallo di tempo specificato. In questo caso, lo stato dell'applicazione di protezione è *interrotto* o *non riuscito* e differisce dai seguenti: *avvio*, *esecuzione* o *sospensione*.	Più di 0 minuti.
Applicazione di protezione non in esecuzione	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma non è in esecuzione.	• L'interruttore è disattivato. • L'interruttore è attivato.

Kaspersky Security Center Cloud Console consente di configurare la selezione automatica dello stato di un dispositivo in un gruppo di amministrazione quando vengono soddisfatte le condizioni specificate. Quando vengono soddisfatte le condizioni specificate, al dispositivo client viene assegnato uno dei seguenti stati: *Critico* o *Avviso*. Quando le condizioni specificate non vengono soddisfatte, al dispositivo client viene assegnato lo stato *OK*.

Diversi stati possono corrispondere ai diversi valori di una condizione. Ad esempio, per impostazione predefinita, se alla condizione **I database non sono aggiornati** è associato il valore **Più di 3 giorni**, al dispositivo client sarà assegnato lo stato *Avviso*; se il valore è **Più di 7 giorni**, verrà assegnato lo stato *Critico*.

Quando Kaspersky Security Center Cloud Console assegna uno stato a un dispositivo, per alcune condizioni (vedere la colonna Descrizione della condizione) viene preso in considerazione il flag di visibilità. Ad esempio, se a un dispositivo gestito è stato assegnato lo stato *Critico* perché è stata soddisfatta la condizione I database non sono aggiornati e successivamente è stato impostato il flag di visibilità per il dispositivo, al dispositivo viene assegnato lo stato *OK*.

Configurazione del passaggio degli stati del dispositivo

È possibile modificare le condizioni per assegnare lo stato *Critico* o *Avviso* a un dispositivo.

Per abilitare la modifica dello stato del dispositivo in Critico:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.
4. Nel riquadro sinistro selezionare **Critico**.
5. Nel riquadro destro, nella sezione **Imposta su Critico se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Critico*.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio padre.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.
7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.
8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.

9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Critico*.

Per abilitare la modifica dello stato del dispositivo in Avviso:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.
4. Nel riquadro sinistro selezionare **Avviso**.
5. Nel riquadro destro, nella sezione **Imposta su Avviso se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Avviso*.

È possibile modificare solo le impostazioni che non sono bloccate nel criterio padre.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.
7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.
8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.
9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Avviso*.

Modifica di Administration Server per i dispositivi client

È possibile sostituire l'Administration Server che gestisce i dispositivi client con un altro server mediante l'attività **Cambia Administration Server**. Dopo il completamento dell'attività, i dispositivi client selezionati passeranno sotto la gestione dell'Administration Server specificato. È possibile alternare la gestione dei dispositivi tra i seguenti Administration Server:

- Administration Server primario e uno dei relativi Administration Server virtuali
- Due Administration Server virtuali dello stesso Administration Server primario

Per sostituire l'Administration Server che gestisce i dispositivi client con un altro server:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Per l'applicazione Kaspersky Security Center Cloud Console, selezionare il tipo di attività **Cambia Administration Server**.
4. Specificare il nome dell'attività che si intende creare.

   Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare i dispositivi a cui assegnare l'attività.
6. Selezionare l'Administration Server che si desidera utilizzare per gestire i dispositivi selezionati.
7. Specificare le impostazioni per l'account:
   - Account predefinito

     L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

     Per impostazione predefinita, questa opzione è selezionata.

- **Specifica account**

  Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

- **Account**

  Account tramite il quale viene eseguita l'attività.

- **Password**

  Password dell'account con cui verrà eseguita l'attività.

8. Se nella pagina **Completa creazione attività** si abilita l'opzione **Apri i dettagli dell'attività al termine della creazione**, è possibile modificare le impostazioni predefinite dell'attività. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

9. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.

10. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

11. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

12. Fare clic sul pulsante **Salva**.

    L'attività verrà creata e configurata.

13. Eseguire l'attività creata.

Dopo il completamento dell'attività, i dispositivi client per cui è stata creata passano sotto la gestione dell'Administration Server specificato nelle impostazioni dell'attività.

Informazioni sui cluster e sugli array di server

Kaspersky Security Center Cloud Console supporta la tecnologia cluster. Se Network Agent invia ad Administration Server informazioni che confermano che l'applicazione installata in un dispositivo client fa parte di un array di server, il dispositivo client diventa un nodo del cluster.

Se un gruppo di amministrazione contiene cluster o array di server, la pagina **Dispositivi gestiti** mostra due schede: una per i singoli dispositivi e una per i cluster e gli array di server. Dopo che i dispositivi gestiti vengono rilevati come nodi del cluster, il cluster viene aggiunto come oggetto singolo alla scheda **Cluster e array di server**.

I nodi del cluster o dell'array di server sono elencati nella scheda **Dispositivi**, insieme ad altri dispositivi gestiti. È possibile visualizzare le proprietà dei nodi come dispositivi singoli ed eseguire altre operazioni, ma non è possibile eliminare un nodo del cluster o spostarlo in un altro gruppo di amministrazione separatamente dal relativo cluster. È solo possibile eliminare o spostare un intero cluster.

È possibile eseguire le seguenti operazioni con cluster o array di server:

- Visualizzare le proprietà
- Spostare il cluster o l'array di server in un altro gruppo di amministrazione

  Quando si sposta un cluster o un array di server in un altro gruppo, tutti i suoi nodi vengono spostati con esso, perché un cluster e uno qualsiasi dei suoi nodi appartengono sempre allo stesso gruppo di amministrazione.
- Elimina

  È ragionevole eliminare un cluster o un array di server solo quando il cluster o l'array di server non esiste più nella rete dell'organizzazione. Se un cluster è ancora visibile nella rete e Network Agent e l'applicazione di sicurezza Kaspersky sono ancora installati nei nodi del cluster, Kaspersky Security Center Cloud Console restituisce automaticamente il cluster eliminato e i relativi nodi all'elenco dei dispositivi gestiti.

Proprietà di un cluster o di un array di server

Per visualizzare le impostazioni di un cluster o di un array di server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti** → **Cluster e array di server**.

   Viene visualizzato l'elenco dei cluster e degli array di server.
2. Fare clic sul nome del cluster o dell'array di server richiesto.

Verrà visualizzata la finestra delle proprietà del cluster o dell'array di server selezionato.

Generale

La sezione **Generale** mostra informazioni generali sul cluster o sull'array di server. Le informazioni sono fornite in base ai dati ricevuti durante l'ultima sincronizzazione dei nodi del cluster con Administration Server:

- **Nome**
- **Descrizione**
- **Dominio Windows**

  Dominio o gruppo di lavoro di Windows, che contiene il cluster o l'array di server.
- **Nome NetBIOS**

  Nome di rete Windows del cluster o dell'array di server.
- **Nome DNS**

  Nome del dominio DNS del cluster o dell'array di server.

Attività

Nella scheda **Attività**, è possibile gestire le attività assegnate al cluster o all'array di server: visualizzare l'elenco delle attività esistenti, creare nuove attività, rimuovere, avviare e arrestare le attività, modificare le impostazioni delle attività e visualizzare i risultati dell'esecuzione. Le attività elencate si riferiscono all'applicazione di sicurezza Kaspersky installata nei nodi del cluster. Kaspersky Security Center Cloud Console riceve l'elenco delle attività e i dettagli sullo stato delle attività dai nodi del cluster. Se non viene stabilita una connessione, lo stato non viene visualizzato.

Nodi

Questa scheda mostra un elenco di nodi inclusi nel cluster o nell'array di server. È possibile fare clic sul nome di un nodo per visualizzare la finestra delle proprietà del dispositivo.

Applicazione Kaspersky

La finestra delle proprietà può contenere anche schede aggiuntive con le informazioni e le impostazioni relative all'applicazione di sicurezza Kaspersky installata nei nodi del cluster.

Tag dispositivo

Questa sezione descrive i tag dispositivo e fornisce istruzioni per crearli e modificarli, nonché per l'assegnazione manuale o automatica di tag ai dispositivi.

Informazioni sui tag dispositivo

Kaspersky Security Center Cloud Console consente di eseguire il tagging dei dispositivi. Un *tag* è l'etichetta di un dispositivo che può essere utilizzato per raggruppare, descrivere o cercare i dispositivi. I tag assegnati ai dispositivi possono essere utilizzati per la creazione di selezioni, per il rilevamento dei dispositivi e per la distribuzione dei dispositivi tra i gruppi di amministrazione.

È possibile assegnare tag ai dispositivi in modalità manuale o automatica. È possibile utilizzare il tagging manuale quando si desidera assegnare tag a un singolo dispositivo. Il tagging automatico viene eseguito da Kaspersky Security Center Cloud Console in base alle regole di tagging specificate.

Ai dispositivi viene assegnato automaticamente un tag quando vengono soddisfatte le regole specificate. A ogni tag corrisponde una regola individuale. Le regole vengono applicate alle proprietà di rete del dispositivo, al sistema operativo, alle applicazioni installate nel dispositivo e ad altre proprietà del dispositivo. Se ad esempio la rete include dispositivi che eseguono Windows, Linux e macOS, è possibile configurare una regola che assegnerà il tag `[Linux]` a tutti i dispositivi basati su Linux. Sarà quindi possibile utilizzare il tag durante la creazione di una selezione dispositivi. Questo consentirà di ordinare tutti i dispositivi basati su Linux e di assegnare loro un'attività. Un tag viene rimosso automaticamente da un dispositivo nei seguenti casi:

- Quando il dispositivo smette di soddisfare le condizioni della regola per l'assegnazione del tag.
- Quando la regola per l'assegnazione del tag viene disabilitata o eliminata.

L'elenco dei tag e l'elenco delle regole in ciascun Administration Server sono indipendenti da tutti gli altri Administration Server, inclusi un Administration Server primario o gli Administration Server virtuali subordinati. Una regola viene applicata solo ai dispositivi nello stesso Administration Server in cui viene creata la regola.

Creazione di un tag dispositivo

Per creare un tag dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Fare clic su **Aggiungi**.
   Verrà visualizzata una finestra per il nuovo tag.
3. Nel campo **Tag** immettere il nome del tag.
4. Fare clic su **Salva** per salvare le modifiche.

Il nuovo tag verrà visualizzato nell'elenco dei tag dispositivo.

Ridenominazione di un tag dispositivo

Per rinominare un tag dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Fare clic sul nome del tag che si desidera rinominare.
   Verrà visualizzata una finestra delle proprietà del tag.
3. Nel campo **Tag** modificare il nome del tag.
4. Fare clic su **Salva** per salvare le modifiche.

Il tag aggiornato verrà visualizzato nell'elenco dei tag dispositivo.

Eliminazione di un tag dispositivo

Per eliminare un tag dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Selezionare dall'elenco il tag dispositivo da eliminare.
3. Fare clic sul pulsante **Elimina**.
4. Nella finestra visualizzata fare clic su **Sì**.

Il tag dispositivo verrà eliminato. Il tag eliminato viene rimosso automaticamente da tutti i dispositivi a cui è stato assegnato.

Il tag eliminato non viene rimosso automaticamente dalle regole di tagging automatico. Una volta eliminato, il tag verrà assegnato a un nuovo dispositivo solo quando il dispositivo soddisfa per la prima volta le condizioni di una regola per l'assegnazione del tag.

Il tag eliminato non viene rimosso automaticamente dal dispositivo se è assegnato al dispositivo da un'applicazione o da Network Agent. Per rimuovere il tag dal dispositivo, usare l'utilità klscflag.

Visualizzazione dei dispositivi a cui è assegnato un tag

Per visualizzare i dispositivi a cui è assegnato un tag:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Fare clic sul collegamento **Visualizza dispositivi** accanto al tag per cui si desidera visualizzare i dispositivi assegnati.

   L'elenco dei dispositivi visualizzato mostra solo i dispositivi a cui è assegnato il tag.

Per tornare all'elenco dei tag dispositivo, fare clic sul pulsante **Indietro** del browser.

Visualizzazione dei tag assegnati a un dispositivo

Per visualizzare i tag assegnati a un dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo di cui si desidera visualizzare i tag.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Tag**.

   Verrà visualizzato l'elenco dei tag assegnati al dispositivo selezionato.

È possibile assegnare un altro tag al dispositivo o rimuovere un tag già assegnato. È inoltre possibile visualizzare tutti i tag dispositivo presenti in Administration Server.

Assegnazione manuale di tag ai dispositivi

Per assegnare un tag a un dispositivo:

1. Visualizzare i tag assegnati al dispositivo a cui si desidera assegnare un altro tag.
2. Fare clic su **Aggiungi**.
3. Nella finestra visualizzata eseguire una delle seguenti operazioni:
   - Per creare e assegnare un nuovo tag, selezionare **Crea nuovo tag** e quindi specificare il nome del nuovo tag.
   - Per selezionare un tag esistente, selezionare **Assegna tag esistente** e quindi selezionare il tag desiderato nell'elenco a discesa.
4. Fare clic su **OK** per applicare le modifiche.

5. Fare clic su **Salva** per salvare le modifiche.

Il tag selezionato verrà assegnato al dispositivo.

Per assegnare un tag a diversi dispositivi:

1. Nel menu principale, accedere a **Risorse (dispositivi)** →**Dispositivi gestiti.**
2. Selezionare i dispositivi a cui si desidera assegnare un tag.
3. Fare clic su **Tag**, quindi selezionare **Assegna** nell'elenco a discesa.
4. Nella finestra visualizzata, selezionare un tag nell'elenco a discesa.
   Se necessario, è possibile selezionare più tag.
   È inoltre possibile procedere come segue:
   - Modificare il nome di un tag facendo clic sull'icona **Modifica** ( ).
     Specificare il nuovo nome del tag, quindi fare clic sul pulsante **Salva**.

     Si noti che il tag verrà rinominato anche nell'elenco dei tag del dispositivo.
   - Eliminare un tag facendo clic sull'icona **Elimina** ( ).
     Nella finestra visualizzata, fare clic su **Elimina**.

     Si noti che il tag verrà eliminato anche dall'Administration Server.
5. Fare clic sul pulsante **Salva**.

I tag verranno assegnati ai dispositivi selezionati. È possibile rimuovere i tag assegnati.

Rimozione dei tag assegnati dai dispositivi

Il tag del dispositivo di cui è stata annullata l'assegnazione non viene eliminato. Se si desidera, è possibile eliminarlo manualmente.

Non è possibile rimuovere manualmente i tag assegnati al dispositivo dalle applicazioni o da Network Agent. Per rimuovere questi tag, utilizzare l'utilità klscflag.

Per rimuovere un tag da un dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo di cui si desidera visualizzare i tag.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Tag**.
4. Selezionare la casella di controllo accanto al tag da rimuovere.

5. Nella parte superiore dell'elenco, fare clic sul pulsante **Annulla assegnazione tag**.
6. Nella finestra visualizzata fare clic su **Sì**.

Il tag viene rimosso dal dispositivo.

Per rimuovere i tag da più dispositivi:

1. Nel menu principale, accedere a **Risorse (dispositivi)** →**Dispositivi gestiti.**
2. Selezionare i dispositivi di cui si desidera rimuovere i tag.
3. Fare clic su **Tag**, quindi selezionare **Rimuovi** nell'elenco a discesa.
4. Nella finestra visualizzata, selezionare le caselle di controllo accanto ai tag che si desidera rimuovere.

   La finestra mostra tutti i tag assegnati a tutti i dispositivi selezionati nel passaggio 2.

5. Fare clic sul pulsante **Salva**.

I tag verranno rimossi dai dispositivi.

Visualizzazione delle regole per il tagging automatico dei dispositivi

Per visualizzare le regole per il tagging automatico dei dispositivi:

Eseguire una delle seguenti operazioni:

- Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Regole di tagging automatico**.
- Nel menu principale, passare a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**, quindi fare clic sul collegamento **Configura regole di tagging automatico**.
- Visualizzare i tag assegnati a un dispositivo e fare clic sul pulsante **Impostazioni**.

Verrà visualizzato l'elenco delle regole per il tagging automatico dei dispositivi.

Modifica di una regola per il tagging automatico dei dispositivi

Per modificare una regola per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Fare clic sul nome della regola che si desidera modificare.
   Verrà visualizzata una finestra delle impostazioni della regola.
3. Modificare le proprietà generali della regola:
   a. Nel campo **Nome regola** modificare il nome della regola.
      Il nome non può superare i 256 caratteri.

b. Eseguire una delle seguenti operazioni:

- Abilitare la regola spostando l'interruttore su **Regola abilitata**.
- Disabilitare la regola spostando l'interruttore su **Regola disabilitata**.

4. Eseguire una delle seguenti operazioni:

- Se si desidera aggiungere una nuova condizione, fare clic sul pulsante **Aggiungi** e specificare le impostazioni della nuova condizione nella finestra visualizzata.
- Per modificare una condizione esistente, fare clic sul nome della condizione che si desidera modificare, quindi modificare le impostazioni della condizione.
- Per eliminare una condizione, selezionare la casella di controllo accanto al nome della condizione da eliminare, quindi fare clic su **Elimina**.

5. Fare clic su **OK** nella finestra delle impostazioni delle condizioni.

6. Fare clic su **Salva** per salvare le modifiche.

La regola modificata verrà visualizzata nell'elenco.

Creazione di una regola per il tagging automatico dei dispositivi

Per creare una regola per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.

2. Fare clic su **Aggiungi**.

Verrà visualizzata una finestra delle impostazioni della nuova regola.

3. Configurare le proprietà generali della regola:

a. Nel campo **Nome regola** immettere il nome della regola.

Il nome non può superare i 256 caratteri.

b. Eseguire una delle seguenti operazioni:

- Abilitare la regola spostando l'interruttore su **Regola abilitata**.
- Disabilitare la regola spostando l'interruttore su **Regola disabilitata**.

c. Nel campo **Tag** immettere il nome del nuovo tag dispositivo o selezionare uno dei tag dispositivo esistenti dall'elenco.

Il nome non può superare i 256 caratteri.

4. Nella sezione delle condizioni fare clic sul pulsante **Aggiungi** per aggiungere una nuova condizione.

Verrà visualizzata una finestra delle impostazioni della nuova condizione.

5. Immettere il nome della condizione.

Il nome non può superare i 256 caratteri. Il nome deve essere univoco all'interno di una regola.

6. Configurare l'attivazione della regola in base alle seguenti condizioni. È possibile selezionare più condizioni.

   - **Rete** - Proprietà di rete del dispositivo, ad esempio il nome del dispositivo nella rete Windows o l'inclusione del dispositivo in un dominio o in una subnet IP.

     Se per il database utilizzato per Kaspersky Security Center Cloud Console sono impostate regole di confronto con distinzione tra maiuscole e minuscole, mantenere le maiuscole e le minuscole quando si specifica un nome DNS del dispositivo. In caso contrario, la regola di tagging automatico non funzionerà.

   - **Applicazioni** - Presenza di Network Agent nel dispositivo, tipo di sistema operativo, versione e architettura.
   - **Macchine virtuali** - Il dispositivo appartiene a un tipo specifico di macchina virtuale.
   - **Active Directory** - Presenza del dispositivo in un'unità organizzativa di Active Directory e appartenenza del dispositivo a un gruppo di Active Directory.
   - **Registro delle applicazioni** - Presenza di applicazioni di vari produttori nel dispositivo.

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

   Se necessario, è possibile impostare più condizioni per una singola regola. In questo caso, il tag verrà essere assegnato a un dispositivo se soddisfa almeno una condizione.

8. Fare clic su **Salva** per salvare le modifiche.

La nuova regola creata viene applicata ai dispositivi gestiti dall'Administration Server selezionato. Se le impostazioni di un dispositivo soddisfano le condizioni della regola, al dispositivo viene assegnato il tag.

Successivamente, la regola viene applicata nei seguenti casi:

- Automaticamente e periodicamente, a seconda del carico di lavoro del server
- Dopo aver modificato la regola
- Quando si esegue la regola manualmente
- Dopo che Administration Server rileva una modifica delle impostazioni di un dispositivo che soddisfa le condizioni della regola o delle impostazioni di un gruppo che contiene tale dispositivo

È possibile creare diverse regole di tagging. A un singolo dispositivo possono essere assegnati diversi tag se sono state create più regole di tagging e se vengono contemporaneamente soddisfatte le rispettive condizioni di tali regole. È possibile visualizzare l'elenco di tutti i tag assegnati nelle proprietà del dispositivo.

Esecuzione di regole per il tagging automatico dei dispositivi

Quando viene eseguita una regola, il tag specificato nelle proprietà di questa regola è assegnato ai dispositivi che soddisfano le condizioni specificate nelle proprietà della regola. È possibile eseguire solo regole attive.

Per eseguire le regole per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Selezionare le caselle di controllo accanto alle regole attive che si desidera eseguire.

3. Fare clic sul pulsante **Esegui regola**.

Le regole selezionate verranno eseguite.

Eliminazione di una regola per il tagging automatico dei dispositivi

Per eliminare una regola per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Selezionare la casella di controllo accanto alla regola che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Nella finestra visualizzata fare di nuovo clic su **Elimina**.

La regola selezionata verrà eliminata. L'assegnazione del tag specificato nelle proprietà di questa regola viene annullata da tutti i dispositivi a cui il tag è stato assegnato.

Il tag del dispositivo di cui è stata annullata l'assegnazione non viene eliminato. Se si desidera, è possibile eliminarlo manualmente.

Quarantena e Backup

Le applicazioni anti-virus Kaspersky installate nei dispositivi client possono spostare file in Quarantena o nella cartella Backup durante la scansione del dispositivo.

La *Quarantena* è uno speciale archivio per i file potenzialmente infetti da virus e per i file che non è possibile disinfettare al momento del rilevamento.

Backup archivia le copie di backup dei file che sono stati eliminati o modificati durante il processo di disinfezione.

Kaspersky Security Center Cloud Console crea un elenco di riepilogo dei file spostati in Quarantena o nella cartella Backup dalle applicazioni Kaspersky nei dispositivi. I Network Agent nei dispositivi client trasmettono le informazioni relative ai file in Quarantena e nella cartella Backup all'Administration Server.

Kaspersky Security Center Cloud Console non esegue la copia di file dagli archivi all'Administration Server. Tutti i file sono memorizzati negli archivi sui dispositivi.

Download di un file dagli archivi

Kaspersky Security Center Cloud Console consente di scaricare le copie dei file che sono state inserite in Quarantena o Backup su un dispositivo client da un'applicazione di protezione. I file vengono copiati nella destinazione specificata.

È possibile scaricare i file solo se vengono soddisfatte le seguenti condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo, è in uso un server push oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Per salvare una copia del file dalla cartella Quarantena o Backup sul disco rigido:

1. Eseguire una delle seguenti operazioni:
   - Se si desidera salvare una copia del file dalla Quarantena, nel menu principale passare a **Operazioni → Archivi → Quarantena**.
   - Se si desidera salvare una copia del file da Backup, nel menu principale passare a **Operazioni → Archivi → Backup**.
2. Nella finestra visualizzata selezionare un file che si desidera scaricare e fare clic su **Scarica**.

   Il download viene avviato. Una copia del file che era stato inserito in Quarantena nel dispositivo client viene salvata nella cartella specificata.

Eliminazione di file dagli archivi

Per eliminare un file dalla cartella Quarantena o Backup:

1. Eseguire una delle seguenti operazioni:
   - Se si desidera salvare una copia del file dalla Quarantena, nel menu principale passare a **Operazioni → Archivi → Quarantena**.
   - Se si desidera salvare una copia del file da Backup, nel menu principale passare a **Operazioni → Archivi → Backup**.
2. Nella finestra visualizzata selezionare un file che si desidera eliminare e fare clic su **Elimina**.
3. Confermare l'eliminazione del file.

   L'applicazione di protezione nel dispositivo client che aveva inserito i file nell'archivio (Quarantena o Backup) elimina tali file dall'archivio.

Diagnostica remota dei dispositivi client

È possibile utilizzare la diagnostica remota per l'esecuzione remota delle seguenti operazioni nei dispositivi client basati su Windows e basati su Linux:

- Abilitazione e disabilitazione del tracciamento, modifica del livello di traccia e download del file di traccia
- Download di informazioni sul sistema e impostazioni dell'applicazione

- Download dei registri eventi
- Generazione di un file di dump per un'applicazione
- Avvio della diagnostica e download dei rapporti
- Avvio, arresto e riavvio delle applicazioni

È possibile utilizzare i registri eventi e i rapporti di diagnostica scaricati da un dispositivo client per eseguire autonomamente la risoluzione dei problemi. Inoltre, se si contatta il Servizio di assistenza tecnica Kaspersky, uno specialista del Servizio di assistenza tecnica potrebbe richiedere di scaricare file di traccia, file di dump, registri eventi e rapporti di diagnostica da un dispositivo client per ulteriori analisi da parte di Kaspersky.

Apertura della finestra di diagnostica remota

Per eseguire la diagnostica remota in dispositivi client basati su Windows e basati su Linux, è prima necessario aprire la finestra di diagnostica remota.

Per aprire la finestra di diagnostica remota:

1. Per selezionare il dispositivo per cui si desidera aprire la finestra di diagnostica remota, eseguire una delle seguenti operazioni:
   - Se il dispositivo appartiene a un gruppo di amministrazione, nel menu principale passare a **Risorse (dispositivi)** → **Gruppi** → **<group name>** → **Dispositivi gestiti**.
   - Se il dispositivo appartiene al gruppo Dispositivi non assegnati, nel menu principale passare a **Individuazione e distribuzione** → **Dispositivi non assegnati**.
2. Fare clic sul nome del dispositivo desiderato.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Avanzate**.
4. Nella finestra visualizzata fare clic su **Diagnostica remota**.

   Viene aperta la finestra **Diagnostica remota** di un dispositivo client. Se la connessione tra Administration Server e il dispositivo client non viene stabilita, viene visualizzato il messaggio di errore.

In alternativa, se è necessario ottenere tutte le informazioni diagnostiche su un dispositivo client basato su Linux, è possibile eseguire lo script collect.sh in questo dispositivo.

Abilitazione e disabilitazione del tracciamento per le applicazioni

È possibile abilitare e disabilitare il tracciamento per le applicazioni, incluso il tracciamento Xperf.

Abilitazione e disabilitazione del tracciamento

Per abilitare o disabilitare il tracciamento in un dispositivo remoto:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.

3. Nell'elenco delle applicazioni selezionare l'applicazione per cui si desidera disabilitare il tracciamento.

   Si apre l'elenco delle opzioni di diagnostica remota.

4. Se si desidera abilitare il tracciamento:

   a. Nella sezione **Traccia**, fare clic su **Abilita traccia**.

   b. Nella finestra **Modifica livello di traccia** visualizzata è consigliabile mantenere i valori predefiniti delle impostazioni. Se necessario, uno specialista del Servizio di assistenza tecnica fornirà il supporto richiesto per il processo di configurazione. Sono disponibili le seguenti impostazioni:

   - **Livello di traccia**

     Il livello di traccia definisce la quantità di dettagli contenuti nel file di traccia.

   - **Traccia basata sulla rotazione**

     L'applicazione sovrascrive le informazioni di tracciamento per evitare un aumento eccessivo delle dimensioni del file di traccia. Specificare il numero massimo di file da utilizzare per archiviare le informazioni di tracciamento e la dimensione massima di ciascun file. Se viene eseguita la scrittura del numero massimo di file di traccia della dimensione massima, il file di traccia meno recente viene eliminato in modo da consentire la creazione di un nuovo file di traccia.

     Questa impostazione è disponibile solo per Kaspersky Endpoint Security.

   c. Fare clic su **Salva**.

   Il tracciamento è abilitato per l'applicazione selezionata. In alcuni casi, è necessario riavviare un'applicazione di protezione e la relativa attività per abilitare il tracciamento.

   Nei dispositivi client basati su Linux, il tracciamento per il componente Updater of Kaspersky Security Agent è regolata dalle impostazioni di Network Agent. Pertanto, le opzioni **Abilita traccia** e **Modifica livello di traccia** sono disabilitate per questo componente nei dispositivi client in cui viene eseguito Linux.

5. Se si desidera disabilitare il tracciamento per l'applicazione selezionata, fare clic su **Disabilita traccia**.

   Il tracciamento è disabilitato per l'applicazione selezionata.

Abilitazione del tracciamento Xperf

Per Kaspersky Endpoint Security, uno specialista del Servizio di assistenza tecnica può richiedere di abilitare il tracciamento Xperf per ottenere informazioni sulle prestazioni del sistema.

Per abilitare e configurare il tracciamento Xperf o disabilitarlo:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.

3. Nell'elenco delle applicazioni selezionare Kaspersky Endpoint Security for Windows.

   Viene visualizzato l'elenco delle opzioni di diagnostica remota per Kaspersky Endpoint Security for Windows.

4. Nella sezione **Traccia Xperf**, fare clic su **Abilita traccia Xperf**.

   Se il tracciamento Xperf è già abilitato, viene invece visualizzato il pulsante **Disabilita traccia Xperf**. Fare clic su questo pulsante se si desidera disabilitare il tracciamento Xperf per Kaspersky Endpoint Security for Windows.

5. Nella finestra **Modifica livello di traccia Xperf** visualizzata, a seconda di quanto richiesto dallo specialista del Servizio di assistenza tecnica, eseguire una delle seguenti azioni:

   a. Selezionare uno dei seguenti livelli di traccia:

   - **Livello superficiale**

     Un file di traccia di questo tipo contiene la quantità minima di informazioni sul sistema.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Livello approfondito**

     Un file di traccia di questo tipo contiene informazioni più dettagliate rispetto ai file di traccia di tipo *Superficiale* e può essere richiesto dagli specialisti del Servizio di assistenza tecnica quando un file di traccia di tipo *Superficiale* non è sufficiente per la valutazione delle prestazioni. Un file di traccia *Approfondito* contiene informazioni tecniche sul sistema, incluse informazioni su hardware, sistema operativo, elenco di processi e applicazioni avviati e arrestati, eventi utilizzati per la valutazione delle prestazioni ed eventi raccolti da Strumento Valutazione sistema Windows.

   b. Selezionare uno dei seguenti tipi di tracciamento Xperf:

   - **Tipologia di base**

     Le informazioni di tracciamento vengono ricevute durante l'esecuzione dell'applicazione Kaspersky Endpoint Security.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Tipologia al riavvio**

     Le informazioni di tracciamento vengono ricevute all'avvio del sistema operativo nel dispositivo gestito. Questo tipo di tracciamento è utile quando il problema che influisce sulle prestazioni del sistema si verifica dopo l'accensione del dispositivo e prima dell'avvio di Kaspersky Endpoint Security.

   Potrebbe anche essere necessario abilitare l'opzione **Dimensioni del file con rotazione (MB)** per impedire un aumento eccessivo delle dimensioni del file di traccia. Specificare quindi la dimensione massima del file di traccia. Quando il file raggiunge la dimensione massima, le informazioni di tracciamento meno recenti vengono sovrascritte da quelle nuove.

   c. Definire le dimensioni del file di rotazione.

   d. Fare clic su **Salva**.

Il tracciamento Xperf è abilitato e configurato.

6. Se si desidera disabilitare il tracciamento Xperf per Kaspersky Endpoint Security for Windows, fare clic su **Disabilita traccia Xperf** nella sezione **Traccia Xperf**.

   Il tracciamento Xperf è disabilitato.

Download dei file di traccia di un'applicazione

È possibile scaricare i file di traccia da un dispositivo client solo se viene soddisfatta una delle seguenti condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo, è in uso un server push oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Per scaricare un file di traccia di un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni, selezionare l'applicazione per la quale si desidera scaricare un file di traccia.
4. Nella sezione **Traccia** fare clic sul pulsante **File di traccia**.

   Viene aperta la finestra **Log di traccia del dispositivo**, dove viene visualizzato un elenco dei file di traccia.
5. Nell'elenco dei file di traccia, selezionare il file che si desidera scaricare.
6. Eseguire una delle seguenti operazioni:

   - Scaricare il file selezionato facendo clic su **Scarica**. È possibile selezionare uno o più file da scaricare.
   - Scaricare una parte del file selezionato:

     a. Fare clic su **Scarica una parte**.

        Non è possibile scaricare parti di più file contemporaneamente. Se si seleziona più di un file di traccia, il pulsante **Scarica una parte** sarà disabilitato.

     b. Nella finestra visualizzata specificare il nome e la parte del file da scaricare, in base alle esigenze.

        Per i dispositivi basati su Linux, la modifica del nome di parte del file non è disponibile.

     c. Fare clic su **Scarica.**

Il file selezionato, o la relativa parte, viene scaricato nella posizione specificata.

Eliminazione dei file di traccia

È possibile eliminare i file di traccia non più necessari.

Per eliminare un file di traccia:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra di diagnostica remota visualizzata, selezionare la scheda **Log eventi**.
3. Nella sezione **File di traccia**, fare clic su **Log di Windows Update** o **Log di installazione remota**, in base ai file di traccia che si desidera eliminare.

   Viene aperta la finestra **Log di traccia del dispositivo**, dove viene visualizzato un elenco dei file di traccia.
4. Nell'elenco dei file di traccia, selezionare uno o più file da eliminare.
5. Fare clic sul pulsante **Rimuovi**.

I file di traccia selezionati vengono eliminati.

Download delle impostazioni delle applicazioni

È possibile scaricare le impostazioni dell'applicazione da un dispositivo client solo se viene soddisfatta una delle seguenti condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo, è in uso un server push oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Per scaricare le impostazioni dell'applicazione da un dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.
3. Nella sezione **Impostazioni applicazione**. fare clic sul pulsante **Scarica** per scaricare le informazioni sulle impostazioni delle applicazioni installate nel dispositivo client.

L'archivio ZIP con le informazioni viene scaricato nella posizione specificata.

Download delle informazioni di sistema da un dispositivo client

È possibile scaricare le informazioni di sistema nel dispositivo da un dispositivo client solo se viene soddisfatta una delle seguenti condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo, è in uso un server push oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Per scaricare le informazioni di sistema da un dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Informazioni di sistema**.

3. Fare clic sul pulsante **Scarica** per scaricare le informazioni di sistema sul dispositivo client.

Il file con le informazioni viene scaricato nella posizione specificata.

Download dei registri eventi

È possibile scaricare i registri eventi nel dispositivo da un dispositivo client solo se viene soddisfatta una delle seguenti condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo, è in uso un server push oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Per scaricare un registro eventi da un dispositivo remoto:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, nella scheda **Log eventi**, fare clic su **Tutti i log del dispositivo**.
3. Nella finestra **Tutti i log del dispositivo**, selezionare uno o più log pertinenti.
4. Eseguire una delle seguenti operazioni:
   - Scaricare il log selezionato facendo clic su **Scarica l'intero file**.
   - Scaricare una parte del log selezionato:
     a. Fare clic su **Scarica una parte**.
        Non è possibile scaricare parti di più registri contemporaneamente. Se si seleziona più di un registro eventi, il pulsante **Scarica una parte** sarà disabilitato.
     b. Nella finestra visualizzata specificare il nome e la parte del registro da scaricare, in base alle esigenze.
     c. Fare clic su **Scarica**.

Il registro eventi selezionato, o la relativa parte, viene scaricato nella posizione specificata.

Avvio, arresto, riavvio dell'applicazione

È possibile avviare, arrestare e riavviare le applicazioni in un dispositivo client.

Per avviare, arrestare o riavviare un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.
   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni selezionare l'applicazione che si desidera avviare, arrestare o riavviare.

4. Selezionare un'azione facendo clic su uno dei seguenti pulsanti:

   - **Arresta applicazione**

     Questo pulsante è disponibile solo se l'applicazione è attualmente in esecuzione.

   - **Riavvia applicazione**

     Questo pulsante è disponibile solo se l'applicazione è attualmente in esecuzione.

   - **Avvia applicazione**

     Questo pulsante è disponibile solo se l'applicazione non è attualmente in esecuzione.

   A seconda dell'azione selezionata, l'applicazione richiesta viene avviata, arrestata o riavviata nel dispositivo client.

Se si riavvia Network Agent, viene visualizzato un messaggio che indica che la connessione corrente del dispositivo ad Administration Server andrà persa.

Esecuzione della diagnostica remota di un'applicazione e download dei risultati

Per avviare la diagnostica per un'applicazione in un dispositivo remoto e scaricarne i risultati:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.

3. Nell'elenco delle applicazioni selezionare l'applicazione per la quale si desidera eseguire la diagnostica remota.

   Si apre l'elenco delle opzioni di diagnostica remota.

4. Nella sezione **Rapporto di diagnostica**, fare clic sul pulsante **Esegui diagnostica**.

   In questo modo si avvia la procedura di diagnostica remota e si genera un rapporto di diagnostica. Al termine della procedura di diagnostica, il pulsante **Scarica il rapporto di diagnostica** diventa disponibile.

5. Fare clic sul pulsante **Scarica il rapporto di diagnostica** per scaricare il rapporto.

Il rapporto viene scaricato nella posizione specificata.

Esecuzione di un'applicazione in un dispositivo client

Potrebbe essere necessario eseguire un'applicazione nel dispositivo client, se richiesto da uno specialista dell'assistenza Kaspersky. Non è necessario installare l'applicazione nel dispositivo. Non è necessario installare l'applicazione nel dispositivo.

Per eseguire un'applicazione nel dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, selezionare la scheda **Esecuzione di un'applicazione remota**.

3. Nella sezione **File dell'applicazione**, fare clic sul pulsante **Sfoglia** per selezionare un archivio ZIP contenente l'applicazione che si desidera eseguire nel dispositivo client.

   L'archivio ZIP deve includere la cartella dell'utilità. Questa cartella contiene il file eseguibile da eseguire in un dispositivo remoto.

   È possibile specificare il nome del file eseguibile e gli argomenti della riga di comando, se necessario. A tale scopo, compilare i campi **Executable file in an archive to be run on a remote device** e **Argomenti della riga di comando**.

4. Facendo clic sul pulsante **Carica ed esegui** per eseguire l'applicazione specificata in un dispositivo client.

5. Seguire le istruzioni dell'esperto dell'Assistenza Kaspersky.

Generazione di un file di dump per un'applicazione

Un file di dump dell'applicazione consente di visualizzare i parametri dell'applicazione in esecuzione in un dispositivo client in un determinato momento. Questo file contiene anche informazioni sui moduli che sono stati caricati per un'applicazione.

La generazione di file dump è disponibile solo per i processi a 32 bit in esecuzione nei dispositivi client basati su Windows. Per i dispositivi client in cui viene eseguito Linux e per i processi a 64 bit, questa funzionalità non è supportata.

Per creare un file di dump per un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, selezionare la scheda **Esecuzione di un'applicazione remota**.

3. Nella sezione **Generazione del file di dump della memoria del processo in corso**, specificare il file eseguibile dell'applicazione per la quale si desidera generare un file dump.

4. Fare clic sul pulsante **Scarica** per salvare il file di dump per l'applicazione specificata.

   Se l'applicazione specificata non è in esecuzione nel dispositivo client, verrà visualizzato il messaggio di errore.

Connessione remota al desktop di un dispositivo client

È possibile ottenere l'accesso remoto al desktop di un dispositivo client tramite un Network Agent installato nel dispositivo client. La connessione remota a un dispositivo tramite Network Agent è possibile anche se le porte TCP e UDP del dispositivo client sono chiuse.

Dopo avere stabilito la connessione con il dispositivo, si ottiene l'accesso completo alle informazioni memorizzate in tale dispositivo ed è possibile gestire le applicazioni installate.

La connessione remota deve essere consentita nelle impostazioni del sistema operativo del dispositivo gestito di destinazione. Ad esempio, in Windows 10, questa opzione è denominata **Consenti connessioni di Assistenza remota al computer** (questa opzione è anche disponibile in **Pannello di controllo → Sistema e sicurezza → Sistema → Impostazioni di connessione remota**). Se si dispone di una licenza per la funzionalità Vulnerability e patch management, è possibile forzare l'abilitazione di questa opzione quando si stabilisce la connessione a un dispositivo gestito. Se non si dispone della licenza, abilitare questa opzione in locale nel dispositivo gestito di destinazione. Se questa opzione è disabilitata, la connessione remota non è possibile.

Per stabilire una connessione remota a un dispositivo, è necessario disporre di due utilità:

- Utilità Kaspersky denominata klsctunnel. Questa utilità deve essere archiviata nella workstation. Questa utilità viene utilizzata per eseguire il tunneling della connessione tra un dispositivo client e Administration Server.

  Kaspersky Security Center Cloud Console consente il tunneling delle connessioni TCP da Administration Console tramite l'Administration Server e quindi tramite Network Agent su una porta specificata in un dispositivo gestito. Il tunneling è progettato per la connessione di un'applicazione client su un dispositivo con Administration Console installato a una porta TCP in un dispositivo gestito, se non è possibile la connessione diretta tra Administration Console e il dispositivo di destinazione.

  Il tunneling della connessione tra un dispositivo client remoto e Administration Server è richiesto se la porta utilizzata per la connessione ad Administration Server non è disponibile nel dispositivo. La porta nel dispositivo potrebbe non essere disponibile nei seguenti casi:

  - Il dispositivo remoto è connesso a una rete locale che utilizza il meccanismo NAT.
  - Il dispositivo remoto fa parte della rete locale di Administration Server, ma la relativa porta è chiusa da un firewall.

- Componente standard di Microsoft Windows denominato Connessione Desktop remoto. La connessione a un desktop remoto viene stabilita attraverso l'utilità standard di Windows mstsc.exe in base alle impostazioni dell'utilità.

  La connessione alla sessione di desktop remoto corrente dell'utente viene stabilita senza che l'utente ne sia a conoscenza. Una volta che ci si connette alla sessione, l'utente del dispositivo viene disconnesso dalla sessione senza preavviso.

Per connettersi al desktop di un dispositivo client, deve essere soddisfatta una delle seguenti condizioni:

- Il dispositivo client è un membro di un gruppo di amministrazione che ha un punto di distribuzione con l'opzione **Non eseguire la disconnessione da Administration Server** abilitata.
- Nelle impostazioni del dispositivo client, l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata.

  Il numero massimo di dispositivi client in cui è possibile abilitare l'opzione **Non eseguire la disconnessione da Administration Server** è 300.

Per stabilire la connessione al desktop di un dispositivo client:

1. Nel menu principale accedere a **Risorse (dispositivi) → Dispositivi gestiti.**
2. Selezionare la casella di controllo accanto al nome del dispositivo a cui si desidera ottenere l'accesso.
3. Fare clic sul pulsante **Connetti a desktop remoto**

   Verrà aperta la finestra Desktop remoto (solo Windows).
4. Fare clic sul pulsante **Scarica** per scaricare l'utilità klsctunnel.

5. Fare clic sul pulsante **Copia negli Appunti** per copiare il testo dal campo di testo. Questo testo è un BLOB (Binary Large OBject) che contiene le impostazioni necessarie per stabilire una connessione tra Administration Server e il dispositivo gestito.

   Un BLOB è valido per 3 minuti. Se è scaduto, riaprire la finestra Desktop remoto (solo Windows) per generare un nuovo BLOB.

6. Eseguire l'utilità klsctunnel.

   Verrà visualizzata la finestra dell'utilità.

7. Incollare il testo copiato nel campo di testo.

8. Se si utilizza un server proxy, selezionare la casella di controllo **Usa server proxy**, quindi specificare le impostazioni di connessione del server proxy.

9. Fare clic sul pulsante **Apri porta**.

   Verrà visualizzata la finestra di accesso a Connessione Desktop remoto.

10. Specificare le credenziali dell'account con cui si è attualmente connessi a Kaspersky Security Center Cloud Console.

11. Fare clic sul pulsante **Connetti**.

Quando viene stabilita la connessione con il dispositivo, il desktop è disponibile nella finestra Connessione Desktop remoto di Microsoft Windows.

Connessione ai dispositivi tramite Condivisione desktop Windows

È possibile ottenere l'accesso remoto al desktop di un dispositivo client tramite un Network Agent installato nel dispositivo client. La connessione remota a un dispositivo tramite Network Agent è possibile anche se le porte TCP e UDP del dispositivo client sono chiuse.

È possibile connettersi a una sessione esistente in un dispositivo client senza disconnettere l'utente in questa sessione. In questo caso, l'utente e l'utente della sessione nel dispositivo condividono l'accesso al desktop.

Per stabilire una connessione remota a un dispositivo, è necessario disporre di due utilità:

- Utilità Kaspersky denominata klsctunnel. Questa utilità deve essere archiviata nella workstation. Questa utilità viene utilizzata per eseguire il tunneling della connessione tra un dispositivo client e Administration Server.

  Kaspersky Security Center Cloud Console consente il tunneling delle connessioni TCP da Administration Console tramite l'Administration Server e quindi tramite Network Agent su una porta specificata in un dispositivo gestito. Il tunneling è progettato per la connessione di un'applicazione client su un dispositivo con Administration Console installato a una porta TCP in un dispositivo gestito, se non è possibile la connessione diretta tra Administration Console e il dispositivo di destinazione.

  Il tunneling della connessione tra un dispositivo client remoto e Administration Server è richiesto se la porta utilizzata per la connessione ad Administration Server non è disponibile nel dispositivo. La porta nel dispositivo potrebbe non essere disponibile nei seguenti casi:

  - Il dispositivo remoto è connesso a una rete locale che utilizza il meccanismo NAT.

- Il dispositivo remoto fa parte della rete locale di Administration Server, ma la relativa porta è chiusa da un firewall.

- Condivisione desktop Windows. Quando ci si connette a una sessione esistente di desktop remoto, l'utente della sessione nel dispositivo riceve una richiesta per la connessione dall'utente. Nei rapporti creati da Kaspersky Security Center Cloud Console non sarà salvata alcuna informazione sull'attività remota nel dispositivo né sui relativi risultati.

  È possibile configurare un controllo dell'attività dell'utente in un dispositivo client remoto. Durante il controllo, l'applicazione salva le informazioni sui file nel dispositivo client che sono stati aperti e/o modificati dall'amministratore.

Per connettersi al desktop di un dispositivo client tramite Condivisione desktop Windows, devono essere soddisfatte le seguenti condizioni:

- Microsoft Windows Vista o versione successiva è installato nella workstation.

  Per verificare se la funzionalità Condivisione desktop Windows è inclusa nella versione di Windows in uso, assicurarsi che CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} sia incluso nel registro a 32 bit.

- Microsoft Windows Vista o versione successiva è installato nel dispositivo client.

- Kaspersky Security Center Cloud Console utilizza una licenza per Vulnerability e patch management.

- Il dispositivo client è un membro di un gruppo di amministrazione che dispone di un punto di distribuzione con l'opzione **Non eseguire la disconnessione da Administration Server** abilitata oppure questa opzione è abilitata nelle impostazioni del dispositivo client.

  Si noti che il numero massimo di dispositivi client in cui è possibile abilitare l'opzione **Non eseguire la disconnessione da Administration Server** è 300.

Per connettersi al desktop di un dispositivo client tramite Condivisione desktop Windows:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Selezionare la casella di controllo accanto al nome del dispositivo a cui si desidera ottenere l'accesso.
3. Fare clic sul pulsante **Condivisione desktop Windows**.

   Viene aperta la procedura guidata Condivisione desktop Windows.
4. Fare clic sul pulsante **Scarica** per scaricare l'utilità klsctunnel e attendere il completamento del processo di download.

   Se si dispone già dell'utilità klsctunnel, ignorare questo passaggio.
5. Fare clic sul pulsante **Avanti**.
6. Selezionare la sessione nel dispositivo a cui si desidera eseguire la connessione, quindi fare clic sul pulsante **Avanti**.
7. Nel dispositivo di destinazione, l'utente deve consentire una sessione di condivisione desktop nella finestra di dialogo visualizzata. In caso contrario, la sessione non è possibile.

   Dopo che l'utente del dispositivo ha confermato la sessione di condivisione del desktop, viene aperta la pagina successiva della procedura guidata.
8. Fare clic sul pulsante **Copia negli Appunti** per copiare il testo dal campo di testo. Questo testo è un BLOB (Binary Large OBject) che contiene le impostazioni necessarie per stabilire una connessione tra Administration Server e il dispositivo gestito.

Un BLOB è valido per 3 minuti. Se è scaduto, generare un nuovo BLOB.

9. Eseguire l'utilità klsctunnel.

   Verrà visualizzata la finestra dell'utilità.

10. Incollare il testo copiato nel campo di testo.

11. Se si utilizza un server proxy, selezionare la casella di controllo **Usa server proxy**, quindi specificare le impostazioni di connessione del server proxy.

12. Fare clic sul pulsante **Apri porta**.

    La condivisione del desktop viene avviata in una nuova finestra. Se si desidera interagire con il dispositivo, fare clic sull'icona Menu () nell'angolo superiore sinistro della finestra, quindi selezionare **Modalità interattiva**.

Attivazione delle regole in modalità Smart Training

Questa sezione fornisce informazioni sui rilevamenti eseguiti in base alle regole di Controllo adattivo delle anomalie in Kaspersky Endpoint Security for Windows nei dispositivi client.

Le regole rilevano i comportamenti anomali nei dispositivi client e possono bloccarli. Se le regole operano in modalità Smart Training, rilevano i comportamenti anomali e inviano i rapporti su ognuna di tali occorrenze all'Administration Server di Kaspersky Security Center Cloud Console. Queste informazioni sono archiviate come elenco nella sottocartella **Attivazione delle regole con stato Smart Training** della cartella **Archivi**. È possibile confermare i rilevamenti come corretti o aggiungerli come esclusioni, in modo che questo tipo di comportamento non venga più considerato anomalo.

Le informazioni sui rilevamenti vengono memorizzate nel registro eventi di Administration Server (insieme ad altri eventi) e nel rapporto di Controllo adattivo delle anomalie.

Per ulteriori informazioni su Controllo adattivo delle anomalie, le regole, le relative modalità e gli stati, fare riferimento alla Guida di Kaspersky Endpoint Security.

Visualizzazione dell'elenco dei rilevamenti eseguiti tramite Controllo adattivo delle anomalie

Per visualizzare l'elenco dei rilevamenti eseguiti tramite le regole di Controllo adattivo delle anomalie:

1. Nel menu principale, passare a **Operazioni** → **Archivi**.

2. Fare clic sul collegamento **Attivazione delle regole con stato Smart Training**.

   L'elenco visualizza le seguenti informazioni sui rilevamenti eseguiti tramite le regole di Controllo adattivo delle anomalie:

   - **Gruppo di amministrazione**

     Nome del gruppo di amministrazione a cui appartiene il dispositivo.

- **Nome dispositivo**

  Nome del dispositivo client a cui è stata applicata la regola.

- **Nome**

  Nome della regola che è stata applicata.

- **Stato**

  Esclusione in corso - Se l'amministratore ha elaborato questo elemento e lo ha aggiunto come un'esclusione alle regole. Questo stato rimane fino alla successiva sincronizzazione del dispositivo client con Administration Server. Dopo la sincronizzazione, l'elemento viene rimosso dall'elenco.

  Conferma in corso - Se l'amministratore ha elaborato e confermato questo elemento. Questo stato rimane fino alla successiva sincronizzazione del dispositivo client con Administration Server. Dopo la sincronizzazione, l'elemento viene rimosso dall'elenco.

  Vuoto - Se l'amministratore non ha elaborato questo elemento.

- **Nome utente**

  Nome dell'utente del dispositivo client che ha eseguito il processo che ha generato il rilevamento.

- **Elaborati**

  Data di rilevamento dell'anomalia.

- **Percorso del processo di origine**

  Percorso del processo di origine, ovvero del processo che esegue l'azione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Hash del processo di origine**

  Hash SHA-256 del file del processo di origine (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Percorso dell'oggetto di origine**

  Percorso dell'oggetto che ha avviato il processo (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Hash dell'oggetto di origine**

  Hash SHA-256 del file di origine (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Percorso del processo di destinazione**

Percorso del processo di destinazione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Hash del processo di destinazione**

  Hash SHA-256 del file di destinazione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Percorso dell'oggetto di destinazione**

  Percorso dell'oggetto di destinazione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Hash dell'oggetto di destinazione**

  Hash SHA-256 del file di destinazione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

Per visualizzare le proprietà di ogni elemento di informazioni:

1. Nel menu principale, passare a **Operazioni** → **Archivi**.
2. Fare clic sul collegamento **Attivazione delle regole con stato Smart Training**.
3. Nella finestra visualizzata selezionare l'oggetto desiderato.
4. Fare clic sul collegamento **Proprietà**.

   Verrà visualizzata la finestra delle proprietà dell'oggetto, in cui sono visualizzate le informazioni relative all'elemento selezionato.

È possibile confermare o aggiungere alle esclusioni qualsiasi elemento nell'elenco dei rilevamenti delle regole di Controllo adattivo delle anomalie.

Per confermare un elemento:

Selezionare uno o più elementi nell'elenco dei rilevamenti e fare clic sul pulsante **Conferma**.

Lo stato degli elementi verrà modificato in **Conferma in corso**.

La conferma dell'utente contribuisce alle statistiche utilizzate dalle regole (per ulteriori informazioni, fare riferimento alla documentazione di Kaspersky Endpoint Security for Windows).

Per aggiungere un elemento come un'esclusione:

Selezionare uno o più elementi nell'elenco dei rilevamenti e fare clic sul pulsante **Escludi**.

Verrà avviata l'Aggiunta guidata esclusioni. Seguire le istruzioni della procedura guidata.

Se si rifiuta o si conferma un elemento, questo verrà escluso dall'elenco dei rilevamenti dopo la successiva sincronizzazione del dispositivo client con Administration Server e non sarà più visualizzato nell'elenco.

Aggiunta di esclusioni dalle regole di Controllo adattivo delle anomalie

L'Aggiunta guidata esclusioni consente di aggiungere esclusioni dalle regole di Controllo adattivo delle anomalie per Kaspersky Endpoint Security for Windows.

Per avviare l'Aggiunta guidata esclusioni tramite il nodo Controllo adattivo delle anomalie:

1. Nel menu principale, passare a **Operazioni** → **Archivi** → **Attivazione delle regole con stato Smart Training**.
2. Nella finestra visualizzata, selezionare un elemento (o più elementi) nell'elenco dei rilevamenti, quindi fare clic sul pulsante **Escludi**.

   È possibile aggiungere fino a 1.000 esclusioni alla volta. Se si selezionano più elementi e si tenta di aggiungerli alle esclusioni, viene visualizzato un messaggio di errore.

Verrà avviata l'Aggiunta guidata esclusioni.

Criteri e profili criterio

In Kaspersky Security Center Cloud Console è possibile creare criteri per le applicazioni Kaspersky. Questa sezione descrive i criteri e i profili criterio e fornisce istruzioni per crearli e modificarli.

Informazioni sui criteri

Un *criterio* è un set di impostazioni dell'applicazione Kaspersky che vengono applicate a un gruppo di amministrazione e ai relativi sottogruppi. È possibile installare diverse applicazioni Kaspersky nei dispositivi di un gruppo di amministrazione. Kaspersky Security Center Cloud Console fornisce un singolo criterio per ogni applicazione Kaspersky in un gruppo di amministrazione. Un criterio ha uno dei seguenti stati (vedere la seguente tabella):

Lo stato del criterio

Stato	Descrizione
Attivo	Il criterio corrente applicato al dispositivo. Può essere attivo un solo criterio per un'applicazione Kaspersky in ogni gruppo di amministrazione. I dispositivi applicano i valori delle impostazioni di un criterio attivo per un'applicazione Kaspersky.
Inattivo	Un criterio che non è attualmente applicato a un dispositivo.
Fuori sede	Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.

I criteri funzionano secondo le seguenti regole:

- È possibile configurare diversi criteri con differenti impostazioni per una singola applicazione.
- Un solo criterio può essere attivo per l'applicazione corrente.

- È possibile attivare un criterio inattivo quando si verifica un evento specifico. È ad esempio possibile applicare impostazioni di protezione anti-virus più rigide durante le epidemie di virus.
- Un criterio può avere criteri figlio.

In generale è possibile utilizzare i criteri in preparazione a situazioni di emergenza, come un attacco virus. Ad esempio in caso di attacco tramite unità flash, è possibile attivare un criterio che blocca l'accesso alle unità flash. In questo caso il criterio attivo corrente diventa automaticamente inattivo.

Per evitare di dover gestire più criteri, ad esempio quando diverse occasioni presuppongono solo la modifica di più impostazioni, è possibile utilizzare i profili criterio.

Un *profilo criterio* è un sottoinsieme denominato di valori delle impostazioni dei criteri che sostituisce i valori delle impostazioni di un criterio. Un profilo criterio influisce sulla creazione delle impostazioni ottimizzate in un dispositivo gestito. Per *impostazioni effettive* si intende un insieme di impostazioni dei criteri, impostazioni dei profili criterio e impostazioni delle applicazioni locali attualmente applicate nel dispositivo.

I profili criterio funzionano secondo le seguenti regole:

- Un profilo criterio assume validità quando si verifica una condizione di attivazione specifica.
- I profili criterio contengono valori delle impostazioni che differiscono dalle impostazioni dei criteri.
- L'attivazione di un profilo criterio modifica le impostazioni effettive del dispositivo gestito.
- Un criterio può includere al massimo 100 profili criterio.

Non è possibile creare un criterio di Administration Server.

Informazioni su blocco e impostazioni bloccate

Ogni impostazione dei criteri ha un'icona a forma di lucchetto (). La tabella seguente mostra gli stati dei pulsanti a forma di lucchetto:

Stati dei pulsanti a forma di lucchetto

Stato	Descrizione
	Se accanto a un'impostazione viene visualizzato un lucchetto aperto e l'interruttore è disabilitato, l'impostazione non è specificata nel criterio. Un utente può modificare queste impostazioni nell'interfaccia dell'applicazione gestita. Questa tipologia di impostazioni è denominata *sbloccata*.
	Se accanto a un'impostazione viene visualizzato un lucchetto chiuso e l'interruttore è abilitato, l'impostazione viene applicata ai dispositivi ai quali si applica il criterio. Un utente non può modificare i valori di queste impostazioni nell'interfaccia dell'applicazione gestita. Questa tipologia di impostazioni è denominata *bloccata*.

È consigliabile bloccare le impostazioni dei criteri che si desidera applicare ai dispositivi gestiti. Le impostazioni dei criteri sbloccate possono essere riassegnate dalle impostazioni dell'applicazione Kaspersky in un dispositivo gestito.

È possibile utilizzare un pulsante a forma di lucchetto per eseguire le seguenti azioni:

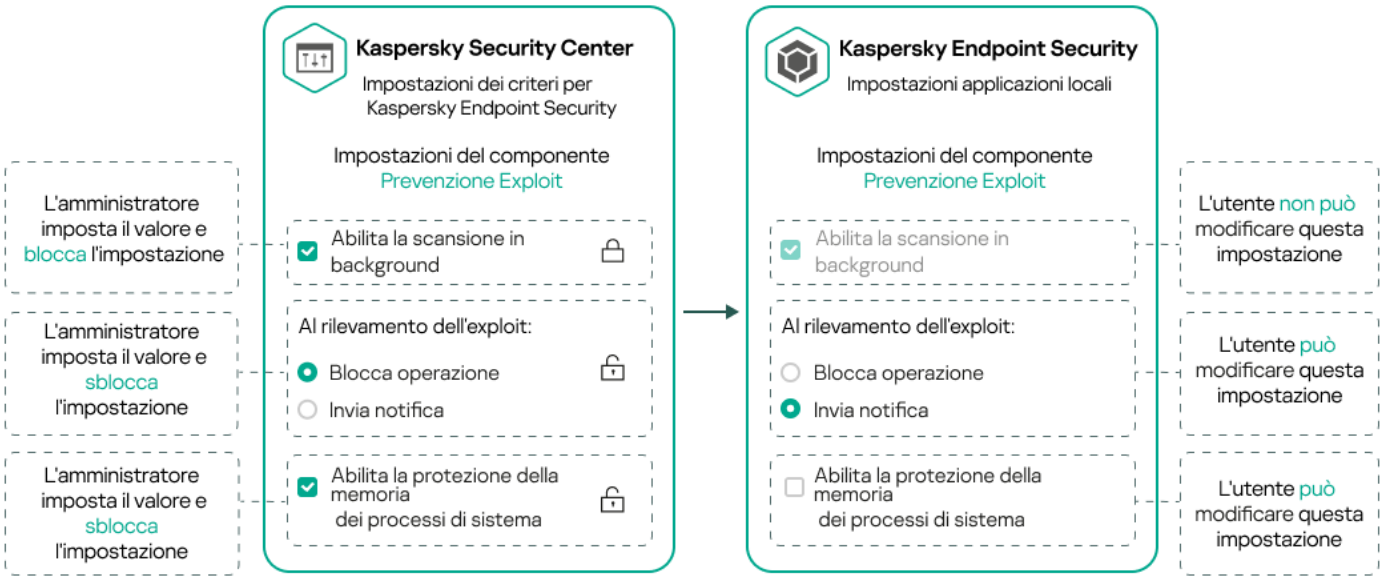
- Blocco delle impostazioni per il criterio di un sottogruppo di amministrazione
- Blocco delle impostazioni di un'applicazione Kaspersky in un dispositivo gestito

Un'impostazione bloccata viene pertanto utilizzata per implementare impostazioni ottimizzate in un dispositivo gestito.

Un processo di implementazione delle impostazioni ottimizzate include le seguenti azioni:

- Il dispositivo gestito applica i valori delle impostazioni dell'applicazione Kaspersky.
- Il dispositivo gestito applica i valori delle impostazioni bloccate di un criterio.

Un criterio e un'applicazione Kaspersky gestita contengono lo stesso set di impostazioni. Quando si configurano le impostazioni dei criteri, le impostazioni dell'applicazione Kaspersky assumono valori differenti in un dispositivo gestito. Non è possibile regolare le impostazioni bloccate in un dispositivo gestito (vedere la figura seguente):



Blocchi e impostazioni delle applicazioni Kaspersky

Ereditarietà di criteri e profili criterio

Questa sezione fornisce informazioni sulla gerarchia e sull'ereditarietà dei criteri e dei profili criterio.

Gerarchia dei criteri

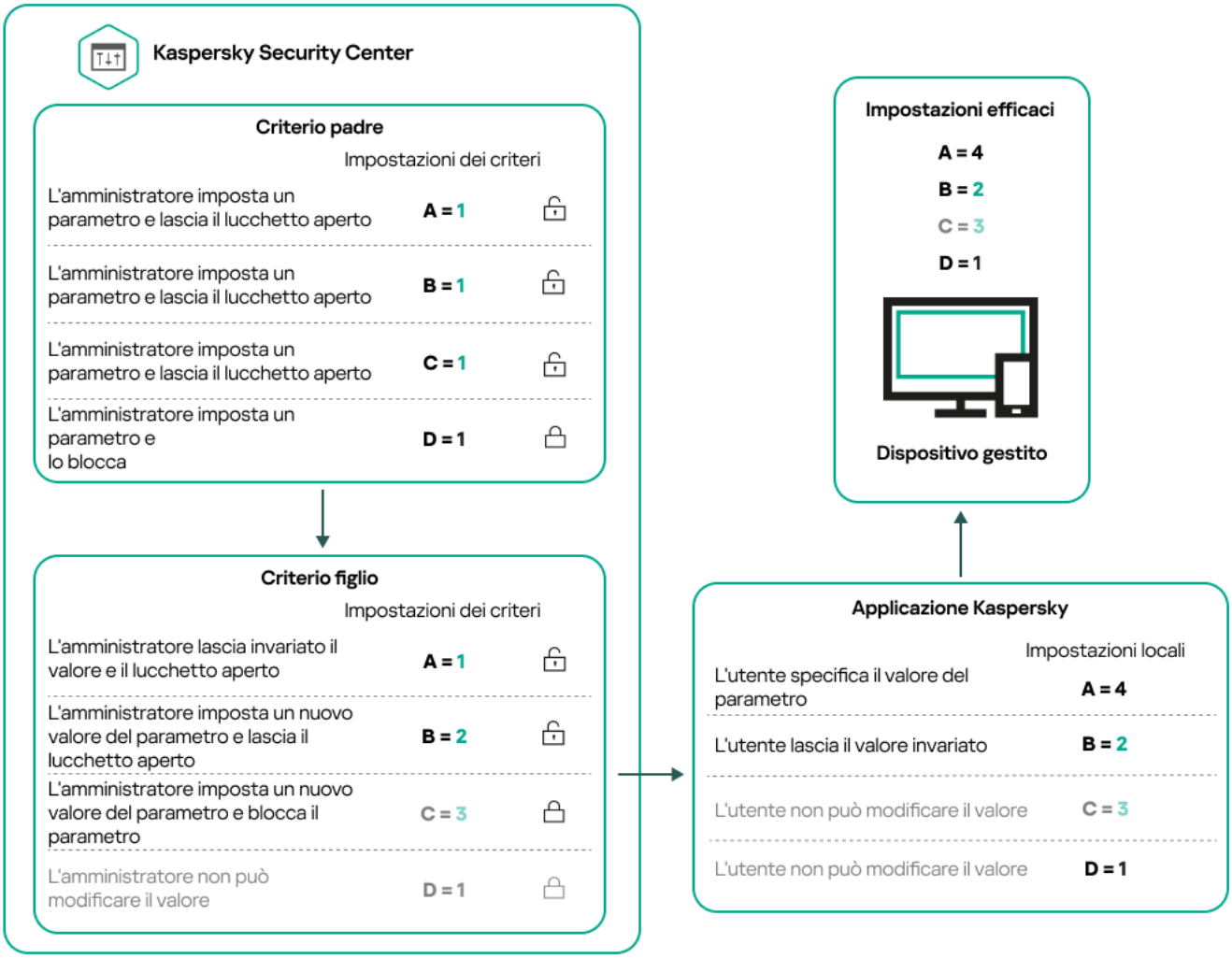
Se dispositivi diversi richiedono impostazioni diverse, è possibile organizzare i dispositivi in gruppi di amministrazione.

È possibile specificare un criterio per un singolo gruppo di amministrazione. Le impostazioni dei criteri possono essere *ereditate*. Ereditarietà significa ricevere i valori delle impostazioni dei criteri nei sottogruppi (gruppi figlio) di un criterio di un gruppo di amministrazione (padre) di livello superiore.

Da questo momento in poi, un criterio per un gruppo padre viene denominato anche *criterio padre*. Un criterio per un sottogruppo (gruppo figlio) viene inoltre denominato *criterio figlio*.

Per impostazione predefinita, esiste almeno un gruppo di dispositivi gestiti in Administration Server. Se si desidera creare gruppi personalizzati, questi vengono creati come sottogruppi (gruppi figlio) all'interno del gruppo di dispositivi gestiti.

I criteri della stessa applicazione si influenzano reciprocamente in base a una gerarchia di gruppi di amministrazione. Le impostazioni bloccate di un criterio di un gruppo di amministrazione di livello superiore (padre) riassegneranno i valori delle impostazioni dei criteri di un sottogruppo (vedere la figura seguente).

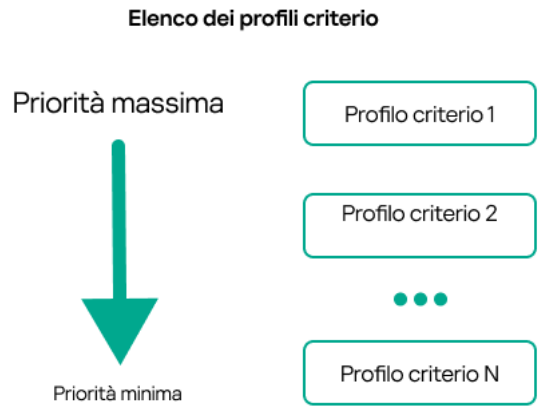


Gerarchia dei criteri

Profili criterio in una gerarchia di criteri

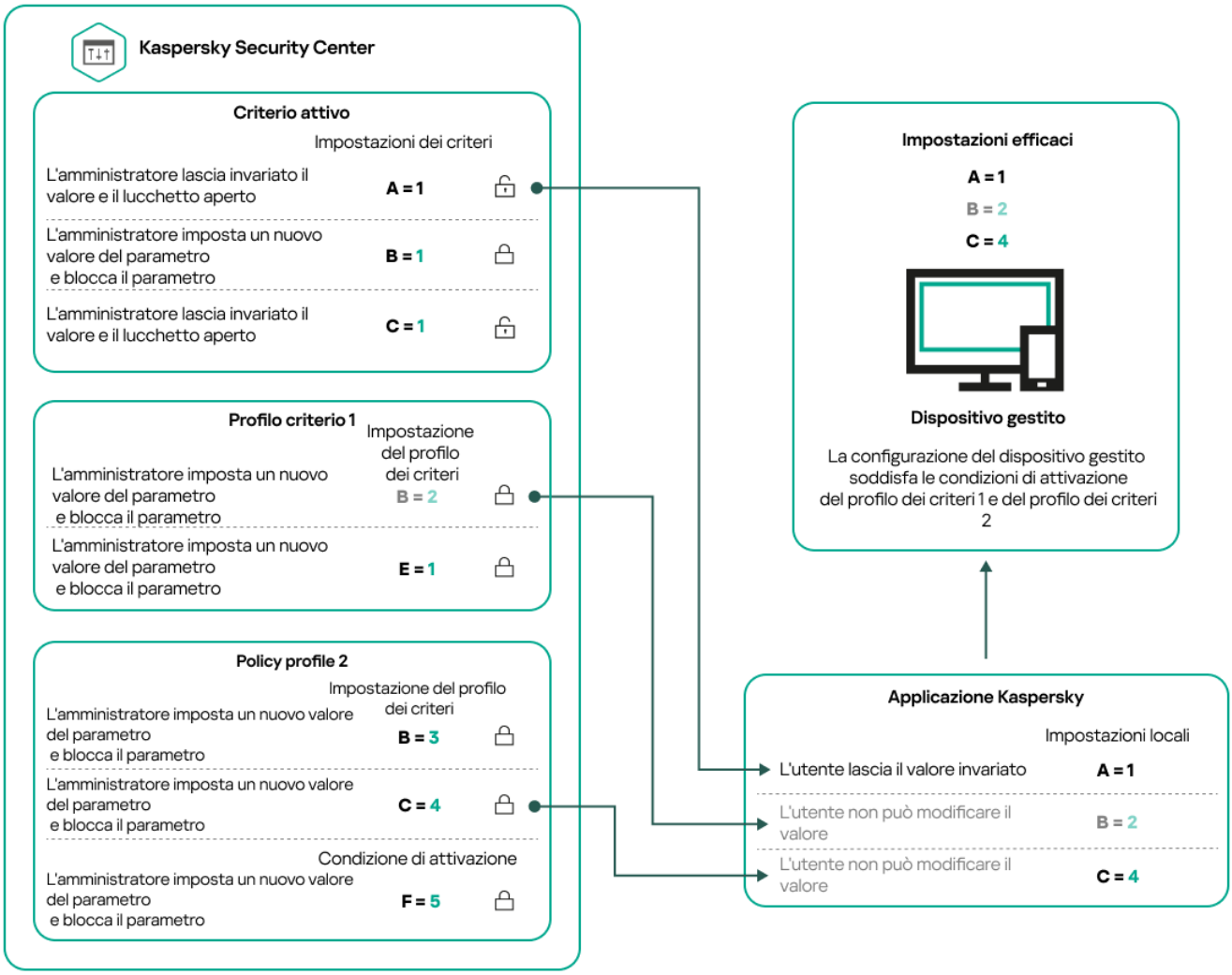
I profili criterio hanno le seguenti condizioni di assegnazione della priorità:

- La posizione di un profilo in un elenco di profili criterio indica la relativa priorità. È possibile modificare la priorità di un profilo criterio. La posizione più elevata in un elenco indica la massima priorità (vedere la figura seguente).



Definizione della priorità di un profilo criterio

- Le condizioni di attivazione dei profili criterio non dipendono l'una dall'altra. È possibile attivare più profili criterio contemporaneamente. Se più profili criterio influiscono sulla stessa impostazione, il dispositivo acquisisce il valore dell'impostazione dal profilo criterio con la priorità più elevata (vedere la figura seguente).

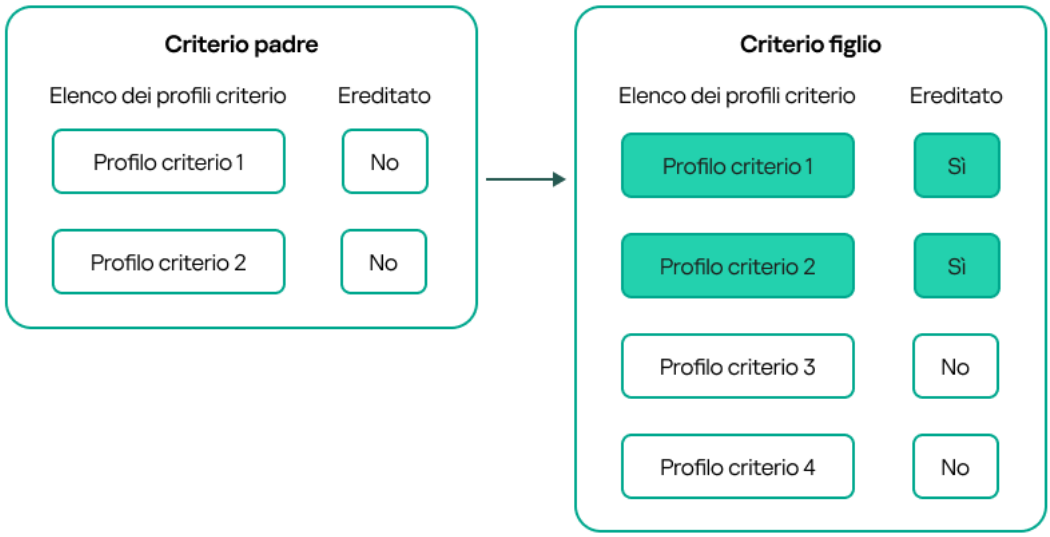


La configurazione del dispositivo gestito soddisfa le condizioni di attivazione di diversi profili criterio

Profili criterio in una gerarchia di ereditarietà

I profili criterio di diversi criteri di livello gerarchico soddisfano le seguenti condizioni:

- Un criterio di livello inferiore eredita i profili criterio da un criterio di livello superiore. Un profilo criterio ereditato da un criterio di livello superiore ottiene una priorità più elevata rispetto al livello del profilo criterio originale.
- Non è possibile modificare la priorità di un profilo criterio ereditato (vedere la figura seguente).

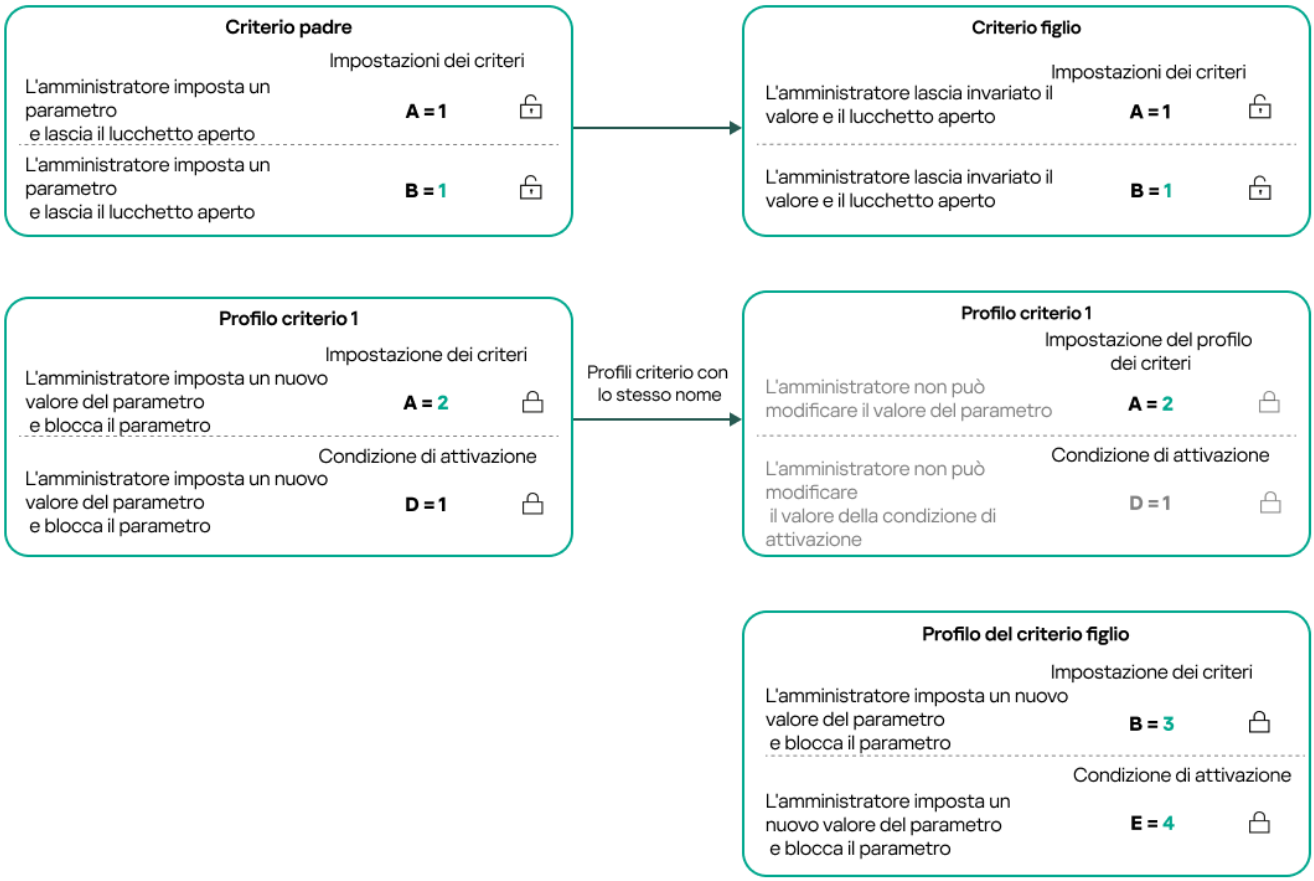


Ereditarietà dei profili criterio

Profili criterio con lo stesso nome

Se sono presenti due criteri con lo stesso nome in diversi livelli della gerarchia, questi criteri funzionano in base alle seguenti regole:

- Le impostazioni bloccate e la condizione di attivazione di un profilo criterio di livello superiore modificano le impostazioni e la condizione di attivazione di un profilo criterio di livello inferiore (vedere la figura seguente).



- Le impostazioni sbloccate e la condizione di attivazione di un profilo criterio di livello superiore non modificano le impostazioni e la condizione di attivazione di un profilo criterio di livello inferiore.

Modalità di implementazione delle impostazioni in un dispositivo gestito

L'implementazione di impostazioni ottimizzate in un dispositivo gestito può essere descritta come segue:

- I valori di tutte le impostazioni non bloccate vengono acquisiti dal criterio.
- Quindi vengono sovrascritti con i valori delle impostazioni dell'applicazione gestita.
- Vengono applicati i valori delle impostazioni bloccate del criterio ottimizzato. I valori delle impostazioni bloccate modificano i valori delle impostazioni ottimizzate sbloccate.

Gestione dei criteri

Questa sezione descrive i criteri di gestione e fornisce informazioni sulla visualizzazione dell'elenco dei criteri, sulla creazione di un criterio, sulla modifica di un criterio, sulla copia di un criterio, sullo spostamento di un criterio, sulla sincronizzazione forzata, sulla visualizzazione del grafico dello stato di distribuzione dei criteri e sull'eliminazione di un criterio.

Visualizzazione dell'elenco di criteri

È possibile visualizzare elenchi dei criteri creati per Administration Server o per qualsiasi gruppo di amministrazione.

Per visualizzare un elenco di criteri:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nella struttura dei gruppi di amministrazione selezionare il gruppo di amministrazione per cui si desidera visualizzare l'elenco di criteri.

   L'elenco di criteri viene visualizzato in formato di tabella. Se non sono presenti criteri, la tabella è vuota. È possibile mostrare o nascondere le colonne della tabella, modificarne l'ordine, visualizzare solo le righe che contengono un valore specificato o utilizzare la ricerca.

Creazione di un criterio

È possibile creare criteri, nonché modificare ed eliminare i criteri esistenti.

Non è possibile creare un criterio di Administration Server.

Per creare un profilo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic su **Aggiungi**.

   Verrà aperta la finestra **Selezionare l'applicazione**.
3. Selezionare l'applicazione per cui si desidera creare un criterio.
4. Fare clic su **Avanti**.

   Verrà visualizzata la finestra delle impostazioni del nuovo criterio, con la scheda **Generale** selezionata.
5. Se si desidera, modificare il nome predefinito, lo stato predefinito e le impostazioni di ereditarietà predefinite del criterio.
6. Fare clic sulla scheda **Impostazioni applicazione**.

   In alternativa, fare clic su **Salva** e uscire. Il criterio verrà visualizzato nell'elenco dei criteri e sarà possibile modificarne le impostazioni in un secondo momento.
7. Nella scheda **Impostazioni applicazione**, nel riquadro a sinistra selezionare la categoria desiderata e nel riquadro dei risultati a destra modificare le impostazioni del criterio. È possibile modificare le impostazioni del criterio in ciascuna categoria (sezione).

   Le impostazioni dell'applicazione dipendono dall'applicazione per cui si crea un criterio. Per i dettagli, fare riferimento ai seguenti elementi:

   - Configurazione di Administration Server
   - Impostazioni del criterio di Network Agent
   - Documentazione di Kaspersky Endpoint Security for Windows

   Per informazioni dettagliate sulle impostazioni delle altre applicazioni di protezione, fare riferimento alla documentazione relativa all'applicazione corrispondente.

   Quando si modificano le impostazioni, è possibile fare clic su **Annulla** per annullare l'ultima operazione.
8. Fare clic su **Salva** per salvare il criterio.

Il criterio verrà visualizzato nell'elenco dei criteri.

Modifica di un criterio

Per modificare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio che si desidera modificare.

   Verrà visualizzata la finestra delle impostazioni del criterio.
3. Specificare le impostazioni generali e le impostazioni dell'applicazione per cui si crea un criterio. Per i dettagli, fare riferimento ai seguenti elementi:

- Configurazione di Administration Server
- Impostazioni del criterio di Network Agent
- Documentazione di Kaspersky Endpoint Security for Windows

Per informazioni dettagliate sulle impostazioni delle altre applicazioni di protezione, fare riferimento alla documentazione relativa a tale applicazione.

4. Fare clic su **Salva**.

Le modifiche apportate al criterio saranno salvate nelle proprietà del criterio e verranno visualizzate nella sezione **Cronologia revisioni**.

Impostazioni generali dei criteri

Generale

Nella scheda **Generale** è possibile modificare lo stato del criterio e specificare l'ereditarietà delle impostazioni criterio:

- Nella sezione **Stato criterio** è possibile selezionare una modalità criterio:
  - **Attivo**
  - **Fuori sede**

    Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.
  - **Inattivo**

    Se questa opzione è selezionata, il criterio diventa inattivo, ma viene comunque salvato nella cartella **Criteri**. Se necessario, il criterio può essere attivato.
- Nel gruppo di impostazioni **Ereditarietà impostazioni** è possibile configurare l'ereditarietà del criterio:
  - **Eredita impostazioni dal criterio padre**

    Se questa opzione è abilitata, i valori delle impostazioni del criterio vengono ereditati dal criterio di gruppo di livello superiore e pertanto vengono bloccati.

    Per impostazione predefinita, questa opzione è abilitata.
  - **Forza ereditarietà impostazioni nei criteri figlio**

Se questa opzione è abilitata, una volta applicate le modifiche ai criteri, verranno eseguite le seguenti azioni:

- I valori delle impostazioni dei criteri saranno propagati ai criteri dei sottogruppi di amministrazione, ovvero ai criteri figlio.
- Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio figlio, l'opzione **Eredita impostazioni dal criterio padre** sarà abilitata automaticamente.

Se questa opzione è abilitata, le impostazioni dei criteri figlio vengono bloccate.

Per impostazione predefinita, questa opzione è disabilitata.

Configurazione eventi

La scheda **Configurazione eventi** consente di configurare la registrazione degli eventi e le notifiche degli eventi. Gli eventi vengono distribuiti nelle seguenti schede in base al livello di importanza:

- **Critico**

  La sezione **Critico** non è visualizzata nelle proprietà del criterio di Network Agent.
- **Errore funzionale**
- **Avviso**
- **Informazioni**

In ogni sezione, l'elenco mostra i tipi di eventi e il periodo di archiviazione predefinito per gli eventi in Administration Server (in giorni). Facendo clic su un tipo di evento, è possibile specificare le seguenti impostazioni:

- **Registrazione eventi**

  È possibile specificare per quanti giorni archiviare l'evento e selezionare dove archiviarlo:

  - **Archivia nel database di Administration Server per (giorni)**
  - **Archivia nel registro eventi del sistema operativo del dispositivo**
- **Notifiche eventi**

  È possibile selezionare se si desidera essere informati dell'evento tramite e-mail.

  Per impostazione predefinita, vengono utilizzate le impostazioni di notifica specificate nella scheda delle proprietà di Administration Server (ad esempio l'indirizzo del destinatario). Se si desidera, è possibile modificare queste impostazioni nella scheda **E-mail**.

Cronologia revisioni

La scheda **Cronologia revisioni** consente di visualizzare l'elenco delle revisioni del criterio ed eseguire il rollback delle modifiche apportate al criterio, se necessario.

Abilitazione e disabilitazione di un'opzione di ereditarietà dei criteri

Per abilitare o disabilitare l'opzione di ereditarietà in un criterio:

1. Aprire il criterio richiesto.
2. Aprire la scheda **Generale**.
3. Abilitare o disabilitare l'ereditarietà dei criteri:
   - Se si abilita **Eredita impostazioni dal criterio padre** in un criterio figlio e un amministratore blocca alcune impostazioni nel criterio padre, non è possibile modificare queste impostazioni nel criterio figlio.
   - Se si disabilita **Eredita impostazioni dal criterio padre** in un criterio figlio, è possibile modificare tutte le impostazioni nel criterio figlio, anche se alcune impostazioni sono bloccate nel criterio padre.
   - Se si abilita **Forza ereditarietà impostazioni nei criteri figlio** nel gruppo padre, viene abilitata l'opzione **Eredita impostazioni dal criterio padre** per tutti i criteri figlio. In questo caso, non è possibile disabilitare questa opzione per nessun criterio figlio. Tutte le impostazioni bloccate nel criterio padre vengono ereditate forzatamente nei gruppi figlio e non è possibile modificare queste impostazioni nei gruppi figlio.
4. Fare clic sul pulsante **Salva** per salvare le modifiche o fare clic sul pulsante **Annulla** per rifiutare le modifiche.

Per impostazione predefinita, l'opzione **Eredita impostazioni dal criterio padre** è abilitata per un nuovo criterio.

Se un criterio dispone di profili, tutti i criteri figlio ereditano tali profili.

Copia di un criterio

È possibile copiare i criteri da un gruppo di amministrazione a un altro.

Per copiare un criterio in un altro gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio (o ai criteri) che si desidera copiare.
3. Fare clic sul pulsante **Copia**.
   Sul lato destro dello schermo verrà visualizzata la struttura dei gruppi di amministrazione.
4. Nella struttura selezionare il gruppo di destinazione, ovvero il gruppo in cui si desidera copiare il criterio (o i criteri).
5. Fare clic sul pulsante **Copia** nella parte inferiore dello schermo.
6. Fare clic su **OK** per confermare l'operazione.

I criteri verranno copiati nel gruppo di destinazione con tutti i relativi profili. Lo stato di ciascun criterio copiato nel gruppo di destinazione sarà **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

Se un criterio con lo stesso nome del nuovo criterio spostato è già incluso nel gruppo di destinazione, al nome del nuovo criterio spostato viene aggiunto l'indice (<numero progressivo successivo>), ad esempio: (1).

Spostamento di un criterio

È possibile spostare i criteri da un gruppo di amministrazione a un altro. Ad esempio, si desidera eliminare un gruppo, ma utilizzare i relativi criteri per un altro gruppo. In questo caso, è possibile spostare il criterio dal gruppo precedente a quello nuovo prima di eliminare il gruppo precedente.

Per spostare un criterio in un altro gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio (o ai criteri) che si desidera spostare.
3. Fare clic sul pulsante **Sposta**.

   Sul lato destro dello schermo verrà visualizzata la struttura dei gruppi di amministrazione.
4. Nella struttura selezionare il gruppo di destinazione, ovvero il gruppo in cui si desidera spostare il criterio (o i criteri).
5. Fare clic sul pulsante **Sposta** nella parte inferiore dello schermo.
6. Fare clic su **OK** per confermare l'operazione.

   Se un criterio non è ereditato dal gruppo di origine, verrà spostato nel gruppo di destinazione con tutti i relativi profili. Lo stato del criterio nel gruppo di destinazione è **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

   Se un criterio è ereditato dal gruppo di origine, rimane nel gruppo di origine. Viene copiato nel gruppo di destinazione con tutti i relativi profili. Lo stato del criterio nel gruppo di destinazione è **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

Se un criterio con lo stesso nome del nuovo criterio spostato è già incluso nel gruppo di destinazione, al nome del nuovo criterio spostato viene aggiunto l'indice (<numero progressivo successivo>), ad esempio: (1).

Esportazione di un criterio

Kaspersky Security Center Cloud Console consente di salvare un criterio, le relative impostazioni e i profili dei criteri in un file KLP. È possibile utilizzare questo file KLP per importare il criterio salvato sia per Kaspersky Security Center Windows che per Kaspersky Security Center Linux.

Per esportare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio che si desidera esportare.

   Non è possibile esportare più criteri contemporaneamente. Se si selezionano più criteri, il pulsante **Esporta** verrà disabilitato.
3. Fare clic sul pulsante **Esporta**.

4. Nella finestra **Salva con nome** visualizzata, specificare il percorso e il nome del file di criteri. Fare clic sul pulsante **Salva**.

   La finestra **Salva con nome** viene visualizzata solo se si utilizza Google Chrome, Microsoft Edge oppure Opera. Se si utilizza un altro browser, il criterio di attività viene salvato automaticamente nella cartella **Download**.

Importazione di un criterio

Kaspersky Security Center Cloud Console consente di importare un criterio da un file KLP. Il file KLP contiene il criterio esportato, le relative impostazioni e i profili dei criteri.

Per importare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul pulsante **Importa**.
3. Fare clic sul pulsante **Sfoglia** per scegliere un file di criteri da importare.
4. Nella finestra visualizzata, specificare il percorso del file di criteri KLP, quindi fare clic sul pulsante **Apri**. Si noti che è possibile selezionare solo un file di criteri.

   Viene avviata l'elaborazione del criterio.
5. Dopo che il criterio è stato elaborato correttamente, selezionare il gruppo di amministrazione a cui si desidera applicare il criterio.
6. Fare clic sul pulsante **Completa** per completare l'importazione del criterio.

Viene visualizzata la notifica con i risultati dell'importazione. Se il criterio viene importato correttamente, è possibile fare clic sul collegamento **Dettagli** per visualizzare le proprietà del criterio.

Dopo un'importazione riuscita, il criterio viene visualizzato nell'elenco dei criteri. Vengono importati anche le impostazioni e i profili del criterio. Indipendentemente dallo stato del criterio selezionato durante l'esportazione, il criterio importato è inattivo. È possibile modificare lo stato del criterio nelle proprietà del criterio.

Se il criterio appena importato ha un nome identico a quello di un criterio esistente, il nome del criterio importato viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Visualizzazione del grafico dello stato di distribuzione dei criteri

In Kaspersky Security Center Cloud Console è possibile visualizzare lo stato dell'applicazione dei criteri in ogni dispositivo in un grafico sullo stato di distribuzione dei criteri.

Per visualizzare lo stato di distribuzione dei criteri in ogni dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al nome del criterio per cui si desidera visualizzare lo stato di distribuzione nei dispositivi.

3. Nel menu visualizzato, fare clic sul collegamento **Distribuzione**.

   Verrà visualizzata la finestra **Risultati della distribuzione di <Nome criterio>**.

4. Nella finestra **Risultati della distribuzione di <Nome criterio>** visualizzata viene visualizzata la **Descrizione dello stato (se disponibile)** del criterio.

È possibile modificare il numero di risultati visualizzati nell'elenco con la distribuzione dei criteri. Il numero massimo di dispositivi è 100.000.

Per modificare il numero dei dispositivi visualizzati nell'elenco con i risultati di distribuzione dei criteri:

1. Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Opzioni di interfaccia**.

2. In **Numero massimo di dispositivi visualizzati nei risultati di distribuzione criteri** immettere il numero di dispositivi (fino a 100.000).

   Il numero predefinito è 5000.

3. Fare clic su **Salva**.

Le impostazioni verranno salvate e applicate.

Attivazione automatica di un criterio quando si verifica un evento Epidemia di virus

Per attivare automaticamente un criterio quando si verifica un evento Epidemia di virus:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server, con la scheda **Generale** selezionata.

2. Selezionare la sezione **Epidemia di virus**.

3. Nel riquadro destro fare clic sul collegamento **Configura i criteri da attivare se si verifica un evento di epidemia di virus**.

   Verrà visualizzata la finestra **Attivazione dei criteri**.

4. Nella sezione relativa al componente per il rilevamento di un'epidemia di virus (Anti-Virus per workstation e file server, Anti-virus per i sistemi di posta o Anti-Virus per la difesa perimetrale) selezionare il pulsante di opzione accanto alla voce desiderata, quindi fare clic su **Aggiungi**.

   Verrà visualizzata una finestra con il gruppo di amministrazione **Dispositivi gestiti**.

5. Fare clic sull'icona di espansione (>) accanto a **Dispositivi gestiti**.

   Verrà visualizzata una gerarchia di gruppi di amministrazione, con i relativi criteri.

6. Nella gerarchia dei gruppi di amministrazione e dei relativi criteri fare clic sul nome di uno o più criteri attivati al rilevamento di un'epidemia di virus.

   Per selezionare tutti i criteri nell'elenco o in un gruppo, selezionare la casella di controllo accanto al nome desiderato.

7. Fare clic sul pulsante **Salva**.

La finestra con la gerarchia dei gruppi di amministrazione e dei relativi criteri verrà chiusa.

I criteri selezionati vengono aggiunti all'elenco dei criteri attivati quando viene rilevata un'epidemia di virus. I criteri selezionati vengono attivati al rilevamento di un'epidemia di virus, indipendentemente dal fatto che siano attivi o inattivi.

Se un criterio è stato attivato per l'evento Epidemia di virus, è possibile ripristinare il criterio precedente solo utilizzando la modalità manuale.

Sincronizzazione forzata

Anche se Kaspersky Security Center Cloud Console sincronizza automaticamente lo stato, le impostazioni, le attività e i criteri per i dispositivi gestiti, in alcuni casi è necessario sapere esattamente se in un dato momento la sincronizzazione è stata già eseguita per un dispositivo specifico.

Sincronizzazione di un singolo dispositivo

Per forzare la sincronizzazione tra Administration Server e un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo che si desidera sincronizzare con Administration Server.

   Verrà visualizzata una finestra delle proprietà con la sezione **Generale** selezionata.
3. Fare clic sul pulsante **Forza sincronizzazione**.

L'applicazione sincronizzerà il dispositivo selezionato con Administration Server.

Sincronizzazione di più dispositivi

Per forzare la sincronizzazione tra Administration Server e più dispositivi gestiti:

1. Aprire l'elenco dei dispositivi di un gruppo di amministrazione o una selezione dispositivi:
   - Nel menu principale, passare a **Risorse (dispositivi)** → **Dispositivi gestiti** → **Gruppi**, quindi selezionare il gruppo di amministrazione che contiene i dispositivi da sincronizzare.
   - Eseguire una selezione dei dispositivi per visualizzare l'elenco dei dispositivi.
2. Selezionare le caselle di controllo accanto ai dispositivi che si desidera sincronizzare con Administration Server.
3. Fare clic sul pulsante **Forza sincronizzazione**.

   L'applicazione sincronizzerà i dispositivi selezionati con Administration Server.
4. Nell'elenco dei dispositivi verificare che per i dispositivi selezionati l'ora dell'ultima connessione ad Administration Server sia cambiata all'ora corrente. Se l'ora non è cambiata, aggiornare il contenuto della pagina facendo clic sul pulsante **Aggiorna**.

I dispositivi selezionati vengono sincronizzati con Administration Server.

Visualizzazione dell'ora di invio di un criterio

Dopo aver modificato un criterio per un'applicazione Kaspersky sull'Administration Server, è possibile verificare se il criterio modificato è stato distribuito a uno specifico dispositivo gestito. Un criterio può essere distribuito durante una sincronizzazione periodica o una sincronizzazione forzata.

Per visualizzare la data e l'ora in cui un criterio dell'applicazione è stato distribuito a un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo che si desidera sincronizzare con Administration Server.

   Verrà visualizzata una finestra delle proprietà con la sezione **Generale** selezionata.
3. Fare clic sulla scheda **Applicazioni**.
4. Selezionare l'applicazione per cui si desidera visualizzare la data di sincronizzazione del criterio.

Verrà visualizzata la finestra del criterio dell'applicazione, con la sezione **Generale** selezionata e la data e l'ora di distribuzione del criterio visualizzate.

Eliminazione di un criterio

È possibile eliminare un criterio se non è più necessario. Può essere eliminato solo un criterio che non viene ereditato nel gruppo di amministrazione specificato. Se un criterio viene ereditato, è possibile eliminarlo solo nel gruppo di livello superiore per cui è stato creato.

Per eliminare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio che si desidera eliminare e fare clic su **Elimina**.

   Il pulsante **Elimina** diventa non disponibile (visualizzato in grigio) se si seleziona un criterio ereditato.
3. Fare clic su **OK** per confermare l'operazione.

Il criterio verrà eliminato insieme a tutti i relativi profili.

Gestione dei profili criterio

Questa sezione illustra la gestione dei profili criterio e fornisce informazioni sulla visualizzazione dei profili di un criterio, sulla modifica della priorità di un profilo criterio, sulla creazione di un profilo criterio, sulla modifica di un profilo criterio, sulla copia di un profilo criterio, sulla creazione di una regola di attivazione del profilo criterio e sull'eliminazione di un profilo criterio.

Visualizzazione dei profili di un criterio

Per visualizzare i profili di un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul nome del criterio di cui si desidera visualizzare i profili.

   Verrà visualizzata la finestra delle proprietà del criterio, con la scheda **Generale** selezionata.
3. Aprire la scheda **Profili criterio**.

L'elenco dei profili criterio viene visualizzato in formato di tabella. Se il criterio non dispone di profili, viene visualizzata una tabella vuota.

Modifica della priorità di un profilo criterio

Per modificare la priorità di un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.
2. Nella scheda **Profili criterio** selezionare la casella di controllo accanto al profilo criterio per cui si desidera modificare la priorità.
3. Impostare una nuova posizione del profilo criterio nell'elenco facendo clic su **Assegna priorità** o **Annulla priorità**.

   Più in alto è posizionato un profilo criterio nell'elenco, maggiore è la relativa priorità.
4. Fare clic sul pulsante **Salva**.

La priorità del profilo criterio selezionato verrà modificata e applicata.

Creazione di un profilo criterio

Per creare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio. Se il criterio non dispone di profili, viene visualizzata una tabella vuota.
2. Fare clic su **Aggiungi**.
3. Se si desidera, modificare il nome predefinito e le impostazioni di ereditarietà predefinite del profilo.
4. Selezionare la scheda **Impostazioni applicazione**.

   In alternativa, fare clic su **Salva** e uscire. Il profilo che è stato creato viene visualizzato nell'elenco dei profili criterio e sarà possibile modificarne le impostazioni in un secondo momento.
5. Nella scheda **Impostazioni applicazione**, nel riquadro a sinistra selezionare la categoria desiderata e nel riquadro dei risultati a destra modificare le impostazioni per il profilo. È possibile modificare le impostazioni del profilo

criterio in ciascuna categoria (sezione).

Quando si modificano le impostazioni, è possibile fare clic su **Annulla** per annullare l'ultima operazione.

6. Fare clic su **Salva** per salvare il profilo.

Il profilo verrà visualizzato nell'elenco dei profili criterio.

Modifica di un profilo criterio

La possibilità di modificare un profilo criterio è disponibile solo per i criteri di Kaspersky Endpoint Security for Windows.

Per modificare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.

2. Nella scheda **Profili criterio** fare clic sul profilo criterio che si desidera modificare.

   Verrà visualizzata la finestra delle proprietà del profilo criterio.

3. Configurare il profilo nella finestra delle proprietà:

   - Se necessario, nella scheda **Generale** modificare il nome del profilo e abilitare o disabilitare il profilo.
   - Modificare le regole di attivazione del profilo.
   - Modificare le impostazioni dell'applicazione.

   Per informazioni dettagliate sulle impostazioni delle applicazioni di protezione, consultare la documentazione dell'applicazione corrispondente.

4. Fare clic su **Salva**.

Le impostazioni modificate diventeranno effettive dopo la sincronizzazione del dispositivo con Administration Server (se il profilo criterio è attivo) o dopo l'esecuzione di una regola di attivazione (se il profilo criterio è inattivo).

Copia di un profilo criterio

È possibile copiare un profilo criterio nel criterio corrente o in un altro, ad esempio se si desidera avere profili identici per criteri diversi. È anche possibile utilizzare la copia per disporre di due o più profili che differiscono solo per un numero limitato di impostazioni.

Per copiare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio. Se il criterio non dispone di profili, viene visualizzata una tabella vuota.

2. Nella scheda **Profili criterio** selezionare il profilo criterio che si desidera copiare.
3. Fare clic su **Copia**.
4. Nella finestra visualizzata selezionare il criterio in cui si desidera copiare il profilo.

   È possibile copiare un profilo criterio nello stesso criterio o in un criterio specificato.
5. Fare clic su **Copia**.

Il profilo criterio verrà copiato nel criterio selezionato. Il nuovo profilo copiato ha la priorità più bassa. Se si copia il profilo nello stesso criterio, al nome del nuovo profilo copiato viene aggiunto l'indice (), ad esempio: (1), (2).

Successivamente, è possibile modificare le impostazioni del profilo, inclusi il nome e la priorità. In questo caso, il profilo criterio originale non verrà modificato.

Creazione di una regola di attivazione del profilo criterio

Per creare una regola di attivazione per un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.
2. Nella scheda **Profili criterio** fare clic sul profilo criterio per cui è necessario creare una regola di attivazione.

   Se l'elenco dei profili criterio è vuoto, è possibile creare un profilo criterio.
3. Nella scheda **Regole di attivazione** fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra con le regole di attivazione del profilo criterio.
4. Specificare un nome per la regola.
5. Selezionare le caselle di controllo accanto alle condizioni che devono determinare l'attivazione del profilo criterio che si sta creando:

   - **Regole generali per l'attivazione del profilo criterio**

     Selezionare questa casella di controllo per configurare le regole di attivazione del profilo criterio nel dispositivo in base allo stato della modalità offline del dispositivo, alla regola per la connessione ad Administration Server e ai tag assegnati al dispositivo.

     Per questa opzione, specificare al passaggio successivo:

     - **Stato dispositivo**

       Definisce la condizione per la presenza del dispositivo nella rete:
       - **Online** - Il dispositivo è presente nella rete, pertanto Administration Server è disponibile.
       - **Offline** - Il dispositivo si trova in una rete esterna, pertanto Administration Server non è disponibile.
       - **N/D** - Il criterio non verrà applicato.

- La regola per la connessione ad Administration Server è attiva su questo dispositivo

  Scegliere la condizione di attivazione del profilo criterio (se la regola viene eseguita o meno) e selezionare il nome della regola.

  La regola definisce il percorso di rete del dispositivo per la connessione ad Administration Server, le cui condizioni devono essere soddisfatte (o non devono essere soddisfatte) per l'attivazione del profilo criterio.

  È possibile creare o configurare una descrizione del percorso di rete dei dispositivi per la connessione a un Administration Server in una regola per il passaggio di Network Agent.

- **Regole per il proprietario di un dispositivo specifico**

  Per questa opzione, specificare al passaggio successivo:

  - Proprietario dispositivo

    Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al proprietario. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

    - Il dispositivo appartiene al proprietario specificato (segno "=").
    - Il dispositivo non appartiene al proprietario specificato (segno "≠").

      Si noti che l'elenco degli utenti viene filtrato e mostra i proprietari dei dispositivi che sono utenti interni.

      Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il proprietario dispositivo quando l'opzione è abilitata. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

  - Il proprietario dispositivo fa parte di un gruppo di protezione interno

    Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base all'appartenenza del proprietario a un gruppo di protezione interno di Kaspersky Security Center Cloud Console. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

    - Il proprietario dispositivo è un membro del gruppo di protezione specificato (segno "=").
    - Il proprietario dispositivo non è un membro del gruppo di protezione specificato (segno "≠").

      Si noti che l'elenco degli utenti viene filtrato e mostra i proprietari dei dispositivi che sono utenti interni.

      Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare un gruppo di protezione di Kaspersky Security Center Cloud Console. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- Regole per le specifiche hardware

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base al volume della memoria e al numero di processori logici.

Per questa opzione, specificare al passaggio successivo:

- **Dimensione RAM (MB)**

  Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al volume della RAM disponibile in tale dispositivo. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

  - Le dimensioni della RAM del dispositivo sono inferiori al valore specificato (segno "<").
  - Le dimensioni della RAM del dispositivo sono superiori al valore specificato (segno ">").

  Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il volume della RAM nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Numero di processori logici**

  Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al numero di processori logici nel dispositivo. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

  - Il numero di processori logici nel dispositivo è inferiore o uguale al valore specificato (segno "<").
  - Il numero di processori logici nel dispositivo è superiore o uguale al valore specificato (segno ">").

  Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il numero di processori logici nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Regole per l'assegnazione dei ruoli**

  Per questa opzione, specificare al passaggio successivo:

  Attiva il profilo criterio in base allo specifico ruolo del proprietario del dispositivo

  Selezionare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo a seconda del ruolo del proprietario. Aggiungere manualmente il ruolo dall'elenco dei ruoli esistenti.

  Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato.

- **Regole per l'utilizzo dei tag**

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base ai tag assegnati al dispositivo. È possibile attivare il profilo criterio nei dispositivi che dispongono o che non dispongono dei tag selezionati.

  Per questa opzione, specificare al passaggio successivo:

  - **Tag**

Nell'elenco di tag specificare una regola per l'inclusione dei dispositivi nel profilo criterio selezionando le caselle di controllo accanto ai tag appropriati.

È possibile aggiungere nuovi tag all'elenco immettendoli nel campo sopra l'elenco e facendo clic sul pulsante **Aggiungi**.

Il profilo criterio include i dispositivi con descrizioni che contengono tutti i tag selezionati. Se le caselle di controllo sono deselezionate, il criterio non viene applicato. Per impostazione predefinita, queste caselle di controllo sono deselezionate.

- Applica ai dispositivi senza i tag specificati

  Abilitare questa opzione se è necessario invertire la selezione di tag.

  Se questa opzione è abilitata, il profilo criterio include i dispositivi con descrizioni che non contengono alcuno dei tag selezionati. Se questa opzione è disabilitata, il criterio non viene applicato.

  Per impostazione predefinita, questa opzione è disabilitata.

- Regole per l'utilizzo di Active Directory

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base alla presenza del dispositivo in un'unità organizzativa di Active Directory o all'appartenenza del dispositivo (o del proprietario) a un gruppo di protezione di Active Directory.

  Per questa opzione, specificare al passaggio successivo:

  - Appartenenza del proprietario del dispositivo a un gruppo di protezione di Active Directory

    Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo il cui proprietario appartiene al gruppo di protezione specificato. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

  - Appartenenza del dispositivo al gruppo di protezione di Active Directory

    Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

  - Allocazione del dispositivo nell'unità organizzativa di Active Directory

    Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo incluso nell'unità organizzativa di Active Directory specificata. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato.

    Per impostazione predefinita, questa opzione è disabilitata.

Il numero delle pagine aggiuntive della procedura guidata dipende dalle impostazioni selezionate nel primo passaggio. È possibile modificare le regole di attivazione del profilo criterio in un secondo momento.

6. Controllare l'elenco dei parametri configurati. Se l'elenco è corretto, fare clic su **Crea**.

Il profilo verrà salvato. Il profilo sarà attivato nel dispositivo quando vengono attivate le regole di attivazione.

Le regole di attivazione del profilo criterio create per il profilo sono visualizzate nelle proprietà del profilo criterio nella scheda **Regole di attivazione**. È possibile modificare o rimuovere qualsiasi regola di attivazione del profilo criterio.

È possibile attivare contemporaneamente più regole di attivazione.

Eliminazione di un profilo criterio

Per eliminare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.

2. Nella scheda **Profili criterio** selezionare la casella di controllo accanto al profilo criterio da eliminare e fare clic su **Elimina**.

3. Nella finestra visualizzata fare di nuovo clic su **Elimina**.

   Il profilo criterio viene eliminato. Se il criterio è ereditato da un gruppo di livello inferiore, il profilo rimane in tale gruppo, ma diventa il profilo criterio di tale gruppo. Questo avviene per eliminare un cambiamento significativo nelle impostazioni delle applicazioni gestite installate nei dispositivi dei gruppi di livello inferiore.

Criptaggio e protezione dei dati

Il criptaggio dei dati riduce il rischio di divulgazione accidentale in caso di furto o smarrimento di un laptop o un disco rigido oppure qualora venga eseguito l'accesso da parte di utenti e applicazioni non autorizzati.

Le seguenti applicazioni Kaspersky supportano il criptaggio:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

È possibile mostrare o nascondere alcuni degli elementi dell'interfaccia relativi alla funzionalità di gestione del criptaggio utilizzando le impostazioni dell'interfaccia utente.

Criptaggio dei dati in Kaspersky Endpoint Security for Windows

È possibile gestire la tecnologia Crittografia unità BitLocker nei dispositivi in cui viene eseguito un sistema operativo Windows per server o workstation.

Utilizzando questi componenti di Kaspersky Endpoint Security for Windows è ad esempio possibile abilitare o disabilitare il criptaggio, visualizzare l'elenco delle unità criptate o generare e visualizzare rapporti sul criptaggio.

È possibile configurare il criptaggio definendo i criteri di Kaspersky Endpoint Security for Windows in Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security for Windows esegue il criptaggio e il decriptaggio in base al criterio attivo. Per istruzioni dettagliate su come configurare le regole e una descrizione delle funzionalità di criptaggio, consultare la Guida di Kaspersky Endpoint Security for Windows.

Criptaggio dei dati in Kaspersky Endpoint Security for Mac

È possibile utilizzare il criptaggio FileVault nei dispositivi che eseguono macOS. Durante l'utilizzo di Kaspersky Endpoint Security for Mac è possibile abilitare o disabilitare questo criptaggio.

È possibile configurare il criptaggio definendo i criteri di Kaspersky Endpoint Security for Mac in Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security for Mac esegue il criptaggio e il decriptaggio in base al criterio attivo. Per una descrizione dettagliata delle funzionalità di criptaggio, consultare la Guida di Kaspersky Endpoint Security for Mac.

Visualizzazione dell'elenco delle unità criptate

In Kaspersky Security Center Cloud Console, è possibile visualizzare i dettagli sulle unità criptate e sui dispositivi criptati a livello di unità. Una volta decriptate le informazioni in un'unità, l'unità viene automaticamente rimossa dall'elenco.

Per visualizzare l'elenco delle unità criptate:

Nel menu principale accedere a **Operazioni** → **Criptaggio e protezione dei dati** → **Unità criptate**.

Se la sezione non è visibile nel menu, significa che è nascosta. Nelle impostazioni dell'interfaccia utente. abilitare l'opzione **Mostra Criptaggio e protezione dei dati** per visualizzare la sezione.

È possibile esportare l'elenco delle unità criptate in un file CSV o TXT. A tale scopo, fare clic sul pulsante **Esporta in CSV** o **Esporta in TXT**.

Creazione e visualizzazione di rapporti sul criptaggio

È possibile generare i seguenti rapporti:

- Rapporto sullo stato di criptaggio dei dispositivi gestiti. Questo rapporto include informazioni dettagliate sul criptaggio dei dati di vari dispositivi gestiti. Il rapporto mostra ad esempio il numero di dispositivi a cui si applica il criterio con regole di criptaggio configurate. È inoltre possibile scoprire, ad esempio, quanti dispositivi devono essere riavviati. Il rapporto contiene inoltre le informazioni sulla tecnologia di criptaggio e sull'algoritmo di ogni dispositivo.
- Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa. Questo rapporto contiene informazioni simili a quelle del rapporto sullo stato di criptaggio dei dispositivi gestiti, ma fornisce solo i dati relativi a dispositivi di archiviazione di massa e unità rimovibili.
- Rapporto sui diritti di accesso alle unità criptate. Questo rapporto mostra quali account utente hanno accesso alle unità criptate.
- Rapporto sugli errori di criptaggio dei file. Questo rapporto contiene informazioni sugli errori che si sono verificati durante l'esecuzione delle attività di criptaggio o decriptaggio dei dati nei dispositivi.

- Rapporto sul blocco dell'accesso ai file criptati. Questo rapporto contiene informazioni sul blocco dell'accesso delle applicazioni ai file criptati. Questo rapporto è utile se un utente o un'applicazione non autorizzati tentano di accedere a unità o file criptati.

È possibile generare qualsiasi rapporto nella sezione **Monitoraggio e generazione dei rapporti** → **Rapporti**. In alternativa, nella sezione **Operazioni** → **Criptaggio e protezione dei dati**, è possibile generare i seguenti rapporti di criptaggio:

- Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa
- Rapporto sui diritti di accesso alle unità criptate
- Rapporto sugli errori di criptaggio dei file

*Per generare un rapporto sul criptaggio nella sezione **Criptaggio e protezione dei dati**:*

1. Assicurarsi di avere abilitato l'opzione **Mostra Criptaggio e protezione dei dati** in Opzioni di interfaccia.
2. Nel menu principale accedere a **Operazioni** → **Criptaggio e protezione dei dati**.
3. Aprire la sezione **Unità criptate** per generare il rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa o il rapporto sui diritti di accesso alle unità criptate.
4. Fare clic sul nome del rapporto che si desidera generare.

Verrà avviata la generazione del rapporto.

Concedere l'accesso a un'unità criptata in modalità offline

Un utente può richiedere l'accesso a un dispositivo criptato, ad esempio quando Kaspersky Endpoint Security for Windows non è installato nel dispositivo gestito. Dopo aver ricevuto la richiesta, è possibile creare un file della chiave di accesso e inviarlo all'utente. Tutti i casi di utilizzo e le istruzioni dettagliate sono disponibili nella Guida di Kaspersky Endpoint Security for Windows.

Per concedere l'accesso a un'unità criptata in modalità offline:

1. Ottenere un file della richiesta di accesso da un utente (un file con estensione FDERTC). Seguire le istruzioni contenute nella Guida di Kaspersky Endpoint Security for Windows per generare il file in Kaspersky Endpoint Security for Windows.
2. Nel menu principale accedere a **Operazioni** → **Criptaggio e protezione dei dati** → **Unità criptate**.

   Verrà visualizzato un elenco di unità criptate.
3. Selezionare l'unità a cui l'utente ha richiesto l'accesso.
4. Fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.
5. Nella finestra visualizzata selezionare il plug-in corrispondente all'applicazione Kaspersky utilizzata per criptare l'unità selezionata.

Se un'unità è criptata con un'applicazione Kaspersky non supportata da Kaspersky Security Center Cloud Console, utilizzare Administration Console basata su Microsoft Management Console per concedere l'accesso offline.

6. Seguire le istruzioni fornite nella Guida di Kaspersky Endpoint Security for Windows (vedere le parti espandibili alla fine della sezione).

Successivamente l'utente applica il file ricevuto per accedere all'unità criptata e leggere i dati archiviati nell'unità.

Utenti e ruoli utente

Questa sezione descrive gli utenti e i ruoli utente e fornisce istruzioni per la creazione e la modifica di questi elementi, per l'assegnazione di ruoli e gruppi agli utenti e per l'associazione dei profili criterio ai ruoli.

Informazioni sugli account utente

Kaspersky Security Center Cloud Console consente di gestire account utente e gruppi di account. L'applicazione supporta due tipi di account:

- Account dei dipendenti dell'organizzazione. Administration Server recupera i dati degli account degli utenti locali durante il polling della rete dell'organizzazione.
- Account di utenti interni di Kaspersky Security Center Cloud Console. È possibile creare account di utenti interni nel portale. Questi account vengono utilizzati solo all'interno di Kaspersky Security Center Cloud Console.

Per visualizzare le tabelle degli account utente e dei gruppi di protezione:

1. Nel menu principale accedere a **Utenti e ruoli** → **Utenti e gruppi**.
2. Selezionare la scheda **Utenti** o **Gruppi**.

Si apre la tabella degli utenti o dei gruppi di protezione. Per impostazione predefinita, la tabella aperta viene filtrata in base alle colonne **Sottotipo** e **Ha ruoli assegnati**. La tabella mostra gli utenti o i gruppi interni a cui sono stati assegnati ruoli.

Se si desidera visualizzare la tabella solo con gli account degli utenti locali, impostare i criteri del filtro **Sottotipo** su **Locale**.

Se si passa a un Administration Server secondario versione 14.2 o precedente e quindi si apre l'elenco di utenti o gruppi di sicurezza, la tabella aperta verrà filtrata solo in base alla colonna **Sottotipo**. Il filtro in base alla colonna **Ha ruoli assegnati** non verrà applicato per impostazione predefinita. La tabella filtrata conterrà tutti gli utenti interni o i gruppi di sicureza con e senza il ruolo assegnato.

Aggiunta di un account di un utente interno

Se lo si desidera, è possibile aggiungere utenti interni dell'area di lavoro nel portale. Dopo aver aggiunto un utente interno, è possibile assegnargli un ruolo in Kaspersky Security Center Cloud Console.

Informazioni sui ruoli utente

Un *ruolo utente* (anche denominato *ruolo*) è un oggetto contenente un set di diritti e privilegi. Un ruolo può essere associato alle impostazioni delle applicazioni Kaspersky installate in un dispositivo utente. È possibile assegnare un ruolo a un set di utenti o a un set di gruppi di protezione a qualsiasi livello nella gerarchia dei gruppi di amministrazione, di Administration Server o a livello di oggetti specifici.

Se i dispositivi vengono gestiti tramite una gerarchia di Administration Server che include Administration Server virtuali, si noti che è possibile creare, modificare o eliminare i ruoli utente solo da un Administration Server fisico. È quindi possibile propagare i ruoli utente agli Administration Server secondari, inclusi quelli virtuali.

È possibile associare i ruoli utente ai profili criterio. Se a un utente viene assegnato un ruolo, tale utente ottiene le impostazioni di protezione necessarie per eseguire le funzioni lavorative.

Un ruolo utente può essere associato agli utenti dei dispositivi in un gruppo di amministrazione specifico.

Ambito del ruolo utente

Un *ambito di un ruolo utente* è una combinazione di utenti e gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Vantaggi dell'utilizzo dei ruoli

Un vantaggio dell'utilizzo dei ruoli è che non è necessario specificare le impostazioni di protezione per ciascuno dei dispositivi gestiti o per ciascuno degli utenti separatamente. Il numero di utenti e dispositivi in un'azienda può essere piuttosto elevato, ma il numero delle diverse funzioni lavorative che richiedono differenti impostazioni di protezione è notevolmente inferiore.

Differenze rispetto all'utilizzo dei profili criterio

I profili criterio sono le proprietà di un criterio creato per ciascuna applicazione Kaspersky separatamente. Un ruolo è associato a molti profili criterio creati per diverse applicazioni. Pertanto, un ruolo è un metodo per riunire le impostazioni per un determinato tipo di utente in un'unica posizione.

Configurazione dei diritti di accesso alle funzionalità dell'applicazione. Controllo dell'accesso basato sui ruoli

Kaspersky Security Center Cloud Console offre l'accesso in base al ruolo alle funzionalità di Kaspersky Security Center Cloud Console e delle applicazioni Kaspersky gestite.

È possibile configurare i diritti di accesso alle funzionalità dell'applicazione per gli utenti di Kaspersky Security Center Cloud Console in uno dei seguenti modi:

- Attraverso la configurazione dei diritti per ciascun utente o gruppo di utenti singolarmente.

- Attraverso la creazione di ruoli utente standard con un set di diritti predefinito e l'assegnazione di tali ruoli agli utenti sulla base dell'ambito delle relative mansioni lavorative.

L'applicazione dei ruoli utente ha lo scopo di semplificare e abbreviare le procedure di routine per la configurazione dei diritti di accesso degli utenti alle funzionalità dell'applicazione. I diritti di accesso all'interno di un ruolo vengono configurati in base alle attività standard e all'ambito delle mansioni lavorative degli utenti.

Ai ruoli utente possono essere assegnati nomi corrispondenti ai rispettivi scopi. È possibile creare un numero illimitato di ruoli nell'applicazione.

È possibile utilizzare i ruoli utente predefiniti con un set di diritti già configurato oppure creare nuovi ruoli e configurare autonomamente i diritti richiesti.

Diritti di accesso alle funzionalità dell'applicazione

La tabella seguente mostra le funzionalità di Kaspersky Security Center Cloud Console con i diritti di accesso per gestire le attività, i rapporti e le impostazioni associati e per eseguire le azioni utente associate.

Per eseguire le azioni utente elencate nella tabella, un utente deve disporre del diritto specificato accanto all'azione.

I diritti **Lettura**, **Scrittura** ed **Esecuzione** sono applicabili a qualsiasi attività, rapporto o impostazione. Oltre a questi diritti, un utente deve disporre del diritto **Esegui operazioni per le selezioni di dispositivi** per gestire attività, rapporti o impostazioni relativi alle selezioni dispositivi.

Tutte le attività, i rapporti, le impostazioni e i pacchetti di installazione mancanti nella tabella appartengono all'area funzionale **Caratteristiche generali: Funzionalità di base**.

Diritti di accesso alle funzionalità dell'applicazione

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto
Caratteristiche generali: **Gestione dei gruppi di amministrazione**	**Scrittura**	• Aggiungere un dispositivo a un gruppo di amministrazione: **Scrittura** • Eliminare un dispositivo da un gruppo di amministrazione: **Scrittura** • Aggiungere un gruppo di amministrazione a un altro gruppo di amministrazione: **Scrittura** • Eliminare un gruppo di amministrazione	None	None

		da un altro gruppo di amministrazione: **Scrittura**		
Caratteristiche generali: **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi**	**Lettura**	Ottenere l'accesso in lettura a tutti gli oggetti: **Lettura**	None	None
Caratteristiche generali: **Funzionalità di base**	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Regole di spostamento dei dispositivi (creazione, modifica o eliminazione) per il server virtuale: **Scrittura**, **Esegui operazioni per le selezioni dispositivi** • Ottenere un certificato personalizzato per il protocollo Mobile (LWNGT): **Lettura** • Impostare un certificato personalizzato per il protocollo Mobile (LWNGT): **Scrittura** • Ottenere l'elenco di reti definito da NLA: **Lettura** • Aggiungere, modificare o eliminare l'elenco di reti definito da NLA: **Scrittura** • Visualizzare gli elenchi di controllo di accesso dei gruppi: **Lettura** • Visualizzare il registro eventi Kaspersky: **Lettura**	• "Scarica aggiornamenti nell'archivio di Administration Server" • "Invia rapporti" • "Distribuisci pacchetto di installazione" • "Installa l'applicazione negli Administration Server secondari in remoto"	• "Rapporto s stato della protezione" • "Rapporto s minacce" • "Rapporto s dispositivi p infetti" • "Rapporto s stato dei database ar virus" • "Rapporto s errori" • "Rapporto s attacchi di r • "Rapporto d riepilogo sul applicazioni protezione p sistema di p installate" • "Rapporto d riepilogo sul applicazioni difesa perim installate" • "Rapporto d riepilogo sui applicazioni installate" • "Rapporto s utenti dei dispositivi in • "Rapporto s problemi di

				sicurezza" • "Rapporto s eventi" • "Rapporto sull'attività c punti di distribuzion • "Rapporto s Administrati Server secc • "Rapporto s eventi di Controllo Dispositivi" • "Rapporto s vulnerabilità • "Rapporto s applicazioni proibite" • "Rapporto s Controllo W • "Rapporto s stato di criptaggio d dispositivi g • "Rapporto s stato di criptaggio d dispositivi d archiviazion massa" • "Rapporto s errori di criptaggio d • "Rapporto s blocco dell'accessc criptati" • "Rapporto s diritti di acc ai dispositiv criptati" • "Rapporto s autorizzazio utente effet

				• "Rapporto s diritti"
Caratteristiche generali: **Oggetti eliminati**	• **Lettura** • **Scrittura**	• Visualizzare gli oggetti eliminati nel Cestino: **Lettura** • Eliminare gli oggetti dal Cestino: **Scrittura**	None	None
Caratteristiche generali: **Elaborazione degli eventi**	• **Elimina eventi** • **Modifica impostazioni di notifica eventi** • **Modifica impostazioni registro eventi** • **Scrittura**	• Modificare le impostazioni di registrazione degli eventi: **Modifica impostazioni registro eventi** • Modificare le impostazioni di notifica degli eventi: **Modifica impostazioni di notifica eventi** • Eliminare gli eventi: **Elimina eventi**	None	None
Caratteristiche generali: **Distribuzione del software Kaspersky**	• **Gestisci patch di Kaspersky** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni**	Accettare o rifiutare l'installazione della patch: **Gestisci patch di Kaspersky**	None	• "Rapporto sull'utilizzo c chiavi di lice da parte dell'Administ Server virtu • "Rapporto s versioni del software Kaspersky"

	dispositivi			• "Rapporto s applicazioni incompatibi • "Rapporto s versioni deg aggiorname moduli softv Kaspersky" • "Rapporto s distribuzion protezione"
Caratteristiche generali: **Gestione delle chiavi di licenza**	• **Esporta file chiave** • **Scrittura**	• Esportare il file chiave: **Esporta file chiave** • Modificare le impostazioni della chiave di licenza di Administration Server: **Scrittura**	None	None
Caratteristiche generali: **Gestione dei rapporti forzata**	• **Lettura** • **Scrittura**	• Creare rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Scrittura** • Eseguire rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Lettura**	None	None
Caratteristiche generali: **Gerarchia di Administration Server**	**Configura gerarchia di Administration Server**	Registrare, aggiornare o eliminare gli Administration Server secondari: **Configura gerarchia di Administration Server**	None	None
Caratteristiche generali: **Autorizzazioni utente**	**Modifica elenchi di controllo degli accessi agli oggetti**	• Modificare le proprietà Protezione di qualsiasi oggetto: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire i ruoli utente: **Modifica elenchi di controllo**	None	None

		degli accessi agli oggetti • Gestire gli utenti interni: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire i gruppi di protezione: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire gli alias: **Modifica elenchi di controllo degli accessi agli oggetti**		
Caratteristiche generali: **Administration Server virtuali**	• **Gestisci Administration Server virtuali** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Ottenere l'elenco degli Administration Server virtuali: **Lettura** • Ottenere informazioni sull'Administration Server virtuale: **Lettura** • Creare, aggiornare o eliminare un Administration Server virtuale: **Gestisci Administration Server virtuali** • Spostare un Administration Server virtuale in un altro gruppo: **Gestisci Administration Server virtuali** • Impostare le autorizzazioni dei server virtuali: **Gestisci Administration Server virtuali**	None	"Rapporto sui ri dell'installazione aggiornamenti software di terz parti"
Caratteristiche generali: Gestione	**Scrittura**	Importazione delle chiavi di criptaggio: **Scrittura**	None	None

delle chiavi di criptaggio				
Gestione sistema: **Connettività**	• **Avvia sessioni RDP** • **Connetti a sessioni RDP esistenti** • **Avvia tunneling** • **Salva i file dei dispositivi nella workstation dell'amministratore** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Creare sessioni di condivisione desktop: **diritto di creare una sessione di condivisione desktop** • Creare una sessione RDP: **Connetti a sessioni RDP esistenti** • Creare un tunnel: **Avvia tunneling** • Salvare l'elenco della rete di contenuti: **Salva i file dei dispositivi nella workstation dell'amministratore**	None	"Rapporto sugli utenti dei dispo
Gestione sistema: **Inventario hardware**	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Ottenere o esportare un oggetto dell'inventario hardware: **Lettura** • Aggiungere, impostare o eliminare un oggetto dell'inventario hardware: **Scrittura**	None	• "Rapporto s registro hard • "Rapporto s modifiche d configurazio • "Rapporto sull'hardware
Gestione sistema: **Controllo accesso alla rete (NAC)**	• **Lettura** • **Scrittura**	• Visualizzare le impostazioni CISCO: **Lettura** • Modificare le impostazioni CISCO: **Scrittura**	None	None
Gestione sistema: **Distribuzione del sistema operativo**	• **Distribuisci server PXE** • **Lettura** • **Scrittura** • **Esecuzione**	• Distribuire server PXE: **Distribuisci server PXE** • Visualizzare un elenco di server PXE: **Lettura**	"Crea pacchetto installazione in base a immagine sistema operativo dispositivo di riferimento"	None

	• **Esegui operazioni per le selezioni dispositivi**	• Avviare o interrompere il processo di installazione nei client PXE: **Esecuzione** • Gestire i driver per WinPE e le immagini del sistema operativo: **Scrittura**		
Gestione sistema: **Vulnerability e Patch Management**	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Visualizzare le proprietà delle patch di terze parti: **Lettura** • Modificare le proprietà delle patch di terze parti: **Scrittura**	• "Esegui sincronizzazione di Windows Update" • "Installa aggiornamenti di Windows Update" • "Correggi vulnerabilità" • "Installa aggiornamenti richiesti e correggi vulnerabilità"	"Rapporto sugli aggiornamenti software"
Gestione sistema: **Installazione remota**	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Visualizzazione delle proprietà del pacchetto di installazione basato su Vulnerability e patch management di terzi: **Lettura** • Modifica delle proprietà del pacchetto di installazione basato su Vulnerability e patch management di terzi: **Scrittura**	None	None
Gestione sistema: **Inventario software**	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni**	None	None	• "Rapporto s applicazioni installate" • "Rapporto s cronologia c registro applicazioni"

	dispositivi			• "Rapporto s stato dei gr applicazioni concesse in licenza" • "Rapporto s chiavi di lice del software terze parti"

Ruoli utente predefiniti

I ruoli utente assegnati agli utenti di Kaspersky Security Center Cloud Console forniscono set di diritti di accesso alle funzionalità dell'applicazione.

Agli utenti creati in un server virtuale non può essere assegnato un ruolo in Administration Server.

È possibile utilizzare i ruoli utente predefiniti con un set di diritti già configurato oppure creare nuovi ruoli e configurare autonomamente i diritti richiesti. Alcuni dei ruoli utente predefiniti disponibili in Kaspersky Security Center Cloud Console possono essere associati a posizioni lavorative specifiche, ad esempio **Auditor**, **Security Officer** e **Supervisore** (questi ruoli sono presenti in Kaspersky Security Center Cloud Console a partire dalla versione 11). I diritti di accesso di questi ruoli sono preconfigurati in base alle attività standard e all'ambito delle mansioni lavorative delle posizioni associate. La tabella seguente illustra il modo in cui è possibile associare i ruoli a posizioni specifiche.

Esempi di ruoli per posizioni specifiche

Ruolo	Commento
Auditor	Consente tutte le operazioni con tutti i tipi di rapporti, tutte le operazioni di visualizzazione, inclusa la visualizzazione degli oggetti eliminati (concede le autorizzazioni di **lettura** e **scrittura** nell'area **Oggetti eliminati**). Non consente altre operazioni. È possibile assegnare questo ruolo a una persona che esegue il controllo dell'organizzazione.
Supervisore	Consente tutte le operazioni di visualizzazione; non consente le altre operazioni. È possibile assegnare questo ruolo a un security officer e ad altri manager responsabili della sicurezza IT dell'organizzazione.
Security Officer	Consente tutte le operazioni di visualizzazione e la gestione dei rapporti; concede autorizzazioni limitate per l'area **Gestione sistema**: **Connettività**. È possibile assegnare questo ruolo a un addetto responsabile della sicurezza IT dell'organizzazione.

La tabella seguente illustra i diritti di accesso assegnati a ciascun ruolo utente predefinito.

Diritti di accesso dei ruoli utente predefiniti

Ruolo	Descrizione

Amministratore Administration Server	Consente tutte le operazioni nelle seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Elaborazione degli eventi**

	• **Gerarchia di Administration Server** • **Administration Server virtuali** • **Gestione sistema**: • **Connettività** • **Inventario hardware** • **Inventario software** Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.
Operatore Administration Server	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali: • **Caratteristiche generali**: • **Funzionalità di base** • **Administration Server virtuali** • **Gestione sistema**: • **Connettività** • **Inventario hardware** • **Inventario software**
Auditor	Consente tutte le operazioni nelle seguenti aree funzionali, in **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Oggetti eliminati** • **Gestione dei rapporti forzata** È possibile assegnare questo ruolo a una persona che esegue il controllo dell'organizzazione.
Amministratore installazione	Consente tutte le operazioni nelle seguenti aree funzionali: • **Caratteristiche generali**: • **Funzionalità di base** • **Distribuzione del software Kaspersky** • **Gestione delle chiavi di licenza** • **Gestione sistema**: • **Distribuzione del sistema operativo** • **Vulnerability e patch management**

	• **Installazione remota** • **Inventario software** Concede i diritti **Lettura** ed **Esecuzione** nell'area funzionale **Caratteristiche generali: Administration Server virtuali**.

Operatore installazione	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Distribuzione del software Kaspersky** (concede anche il diritto **Gestisci patch di Kaspersky** in quest'area)
	  • **Administration Server virtuali**
	• **Gestione sistema**:
	  • **Distribuzione del sistema operativo**
	  • **Vulnerability e patch management**
	  • **Installazione remota**
	  • **Inventario software**

Amministratore Kaspersky Endpoint Security	Consente tutte le operazioni nelle seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • Area Kaspersky Endpoint Security, incluse tutte le funzionalità Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.
Operatore Kaspersky Endpoint Security	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • Area Kaspersky Endpoint Security, incluse tutte le funzionalità
Amministratore principale	Consente tutte le operazioni nelle aree funzionali, *ad eccezione* delle seguenti aree, **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Gestione dei rapporti forzata** Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.
Operatore principale	Concede i diritti **Lettura** ed **Esecuzione** (ove applicabile) in tutte le seguenti aree funzionali: • **Caratteristiche generali**: • **Funzionalità di base**

	• **Oggetti eliminati** • **Operazioni in Administration Server** • **Distribuzione del software Kaspersky** • **Administration Server virtuali** • **Mobile Device Management: Generale** • **Gestione sistema**, incluse tutte le funzionalità • Area Kaspersky Endpoint Security, incluse tutte le funzionalità
Amministratore Mobile Device Management	Consente tutte le operazioni nelle seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • **Mobile Device Management: Generale**
Operatore Mobile Device Management	Concede i diritti **Lettura** ed **Esecuzione** nell'area funzionale **Caratteristiche generali**: **Funzionalità di base**. Concede i diritti **Lettura** e **Invia solo comandi informativi ai dispositivi mobili** nell'area funzionale **Mobile Device Management**: **Generale**.
Security Officer	Consente tutte le operazioni nelle seguenti aree funzionali, in **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Gestione dei rapporti forzata** Concede i diritti **Lettura**, **Scrittura**, **Esecuzione**, **Salva i file dei dispositivi nella workstation dell'amministratore** ed **Esegui operazioni per le selezioni di dispositivi** nell'area funzionale **Gestione sistema: Connettività**. È possibile assegnare questo ruolo a un addetto responsabile della sicurezza IT dell'organizzazione.
Analista di sicurezza senior	Concede il diritto **Lettura** nell'area funzionale **Caratteristiche generali**: **Funzionalità di base**. Concede i diritti **Scrittura**, **Modifica**, **Esecuzione**, **Salva i file dei dispositivi nella workstation dell'amministratore** ed **Esegui operazioni per le selezioni dispositivi nell'area funzionale Gestione sistema**: **Connettività**. Concede i diritti di accesso alla soluzione Kaspersky Endpoint Detection and Response Expert.
Utente del Portale Self Service	Consente tutte le operazioni nell'area funzionale **Mobile Device Management: Portale Self Service**. Questa funzionalità non è supportata in Kaspersky Security Center 11 e versioni successive.
Supervisore	Concede il diritto **Lettura** nell'area funzionale **Caratteristiche generali**: **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** e **Caratteristiche generali**: **Gestione dei rapporti forzata**. È possibile assegnare questo ruolo a un security officer e ad altri manager responsabili della sicurezza IT dell'organizzazione.
Amministratore di Vulnerability e	Consente tutte le operazioni nelle aree funzionali **Caratteristiche generali**: **Funzionalità di base** e **Gestione sistema** (incluse tutte le funzionalità).

Patch Management	
Operatore di Vulnerability e Patch Management	Concede i diritti **Lettura** ed **Esecuzione** (ove applicabile) nelle aree funzionali **Caratteristiche generali**: **Funzionalità di base** e **Gestione sistema** (incluse tutte le funzionalità).

Assegnazione dei diritti di accesso a oggetti specifici

Oltre ad assegnare diritti di accesso a livello di server, è possibile configurare l'accesso a oggetti specifici, ad esempio a un'attività specifica. L'applicazione consente di specificare i diritti di accesso per i seguenti tipi di oggetti:

- Gruppi di amministrazione
- Attività
- Rapporti
- Selezioni dispositivi
- Selezioni eventi

Per assegnare i diritti di accesso a un oggetto specifico:

1. In base al tipo di oggetto, nel menu principale passare alla sezione corrispondente:
   - **Risorse (dispositivi) → Gerarchia dei gruppi**
   - **Risorse (dispositivi) → Attività**
   - **Monitoraggio e generazione dei rapporti → Rapporti**
   - **Risorse (dispositivi) → Selezioni dispositivi**
   - **Monitoraggio e generazione dei rapporti → Selezioni eventi**
2. Aprire le proprietà dell'oggetto per il quale si desidera configurare i diritti di accesso.

   Per aprire la finestra delle proprietà di un gruppo di amministrazione o di un'attività, fare clic sul nome dell'oggetto. È possibile aprire le proprietà di altri oggetti utilizzando il pulsante sulla barra degli strumenti.
3. Nella finestra delle proprietà, aprire la sezione **Diritti di accesso**.

   Verrà visualizzato l'elenco di utenti. Gli utenti e i gruppi di protezione elencati dispongono dei diritti di accesso all'oggetto. Per impostazione predefinita, se si utilizza una gerarchia di gruppi di amministrazione o server, l'elenco e i diritti di accesso vengono ereditati dal gruppo di amministrazione principale o dal server primario.
4. Per poter modificare l'elenco, abilitare l'opzione **Usa autorizzazioni personalizzate**.
5. Configurare i diritti di accesso:
   - Utilizzare i pulsanti **Aggiungi** ed **Elimina** per modificare l'elenco.

- Specificare i diritti di accesso per un utente o un gruppo di protezione. Eseguire una delle seguenti operazioni:
  - Se si desidera specificare i diritti di accesso manualmente, selezionare l'utente o il gruppo di protezione, fare clic sul pulsante **Diritti di accesso**, quindi specificare i diritti di accesso.
  - Se si desidera assegnare un ruolo utente all'utente o al gruppo di protezione, selezionare l'utente o il gruppo di protezione, fare clic sul pulsante **Ruoli** e selezionare il ruolo da assegnare.

6. Fare clic sul pulsante **Salva**.

I diritti di accesso all'oggetto sono configurati.

Assegnazione di un ruolo a un utente o un gruppo di protezione

Per assegnare un ruolo a un utente o un gruppo di protezione:

1. Nel menu principale, passare su **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti** o **Gruppi**.
2. Selezionare il nome dell'utente o del gruppo di protezione a cui assegnare un ruolo.

   È possibile selezionare più nomi.
3. Nella riga del menu fare clic sul pulsante **Assegna ruolo**.

   Verrà avviata l'Assegnazione guidata ruolo.
4. Seguire le istruzioni della procedura guidata: selezionare il ruolo che si desidera assegnare agli utenti o gruppi di protezione selezionati, quindi selezionare l'ambito del ruolo.

   Un *ambito di un ruolo utente* è una combinazione di utenti e gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Il ruolo con un set di diritti per l'utilizzo di Administration Server viene assegnato all'utente (o agli utenti o al gruppo di protezione). Nell'elenco degli utenti o dei gruppi di sicurezza, viene visualizzata una casella di controllo nella colonna **Ha ruoli assegnati**.

Creazione di un ruolo utente

Per creare un ruolo utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Nome nuovo ruolo** visualizzata immettere il nome del nuovo ruolo.
4. Fare clic su **OK** per applicare le modifiche.
5. Nella finestra delle proprietà del ruolo visualizzata modificare le impostazioni del ruolo:
   - Nella scheda **Generale** modificare il nome del ruolo.

Non è possibile modificare il nome di un ruolo predefinito.

- Nella scheda **Impostazioni** modificare l'ambito del ruolo, i criteri e i profili associati al ruolo.
- Nella scheda **Diritti di accesso** modificare i diritti per l'accesso alle applicazioni Kaspersky.

6. Fare clic su **Salva** per salvare le modifiche.

Il nuovo ruolo verrà visualizzato nell'elenco dei ruoli utente.

Modifica dei diritti di accesso di un utente

È possibile modificare i diritti di accesso degli utenti per i seguenti oggetti:

- Administration Server
- Gruppo di amministrazione
- Attività
- Rapporto
- Selezione eventi
- Selezione dispositivi

Per modificare i diritti di accesso di un utente:

1. Passare alla scheda **Diritti di accesso** dell'oggetto selezionato.
2. Selezionare un utente per il quale si desidera modificare i diritti di accesso.

   Se è stato selezionato il proprio account utente, non è possibile revocare i propri diritti di accesso. Le modifiche non verranno salvate.

3. Fare clic sul pulsante **Diritti di accesso**.
4. Nella finestra visualizzata modificare i diritti di accesso per l'utente selezionato.
5. Fare clic sul pulsante **OK**.

I diritti di accesso per questo utente sono stati modificati.

Modifica di un ruolo utente

Per modificare un ruolo utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic sul nome del ruolo che si desidera modificare.

3. Nella finestra delle proprietà del ruolo visualizzata modificare le impostazioni del ruolo:

   - Nella scheda **Generale** modificare il nome del ruolo.

     Non è possibile modificare il nome di un ruolo predefinito.

   - Nella scheda **Impostazioni** modificare l'ambito del ruolo, i criteri e i profili associati al ruolo.

   - Nella scheda **Diritti di accesso** modificare i diritti per l'accesso alle applicazioni Kaspersky.

4. Fare clic su **Salva** per salvare le modifiche.

Il ruolo aggiornato verrà visualizzato nell'elenco dei ruoli utente.

Modifica dell'ambito di un ruolo utente

Un *ambito di un ruolo utente* è una combinazione di utenti e gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Per aggiungere utenti, gruppi di utenti e gruppi di amministrazione all'ambito di un ruolo utente, è possibile utilizzare una dei seguenti metodi:

Metodo 1:

1. Nel menu principale, passare su **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti** o **Gruppi**.

2. Selezionare le caselle di controllo accanto agli utenti o ai gruppi di utenti che si desidera aggiungere all'ambito del ruolo utente.

3. Fare clic sul pulsante **Assegna ruolo**.

   Verrà avviata l'Assegnazione guidata ruolo. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Nella pagina **Selezionare un ruolo** della procedura guidata selezionare il ruolo utente che si desidera assegnare.

5. Nella pagina **Definire l'ambito** della procedura guidata selezionare il gruppo di amministrazione da aggiungere all'ambito del ruolo utente.

6. Fare clic sul pulsante **Assegna ruolo** per chiudere la finestra.

Gli utenti o i gruppi di utenti selezionati e il gruppo di amministrazione selezionato verranno aggiunti all'ambito del ruolo utente.

Metodo 2:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.

2. Fare clic sul nome del ruolo per cui si desidera definire l'ambito.

3. Nella finestra delle proprietà del ruolo visualizzata, selezionare la scheda **Impostazioni**.

4. Nella sezione **Ambito ruolo** fare clic su **Aggiungi**.

   Verrà avviata l'Assegnazione guidata ruolo. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

5. Nella pagina **Definire l'ambito** della procedura guidata selezionare il gruppo di amministrazione da aggiungere all'ambito del ruolo utente.

6. Nella pagina **Selezionare gli utenti** della procedura guidata, selezionare gli utenti e i gruppi di utenti che si desidera aggiungere all'ambito del ruolo utente.

7. Fare clic sul pulsante **Assegna ruolo** per chiudere la finestra.

8. Chiudere la finestra delle proprietà del ruolo.

Gli utenti o i gruppi di utenti selezionati e il gruppo di amministrazione selezionato verranno aggiunti all'ambito del ruolo utente.

Eliminazione di un ruolo utente

Per eliminare un ruolo utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.

2. Selezionare la casella di controllo accanto al nome del ruolo che si desidera eliminare.

3. Fare clic su **Elimina**.

4. Nella finestra visualizzata fare clic su **OK**.

Il ruolo utente verrà eliminato.

Associazione dei profili criterio ai ruoli

È possibile associare i ruoli utente ai profili criterio. In questo caso, la regola di attivazione per questo profilo criterio si basa sul ruolo: il profilo criterio diventa attivo per un utente che ha il ruolo specificato.

Il criterio vieta ad esempio un software di navigazione GPS in tutti i dispositivi in un gruppo di amministrazione. Il software di navigazione GPS è necessario in un solo dispositivo nel gruppo di amministrazione Utenti: quello di proprietà di un corriere. In questo caso, è possibile assegnare un ruolo "Corriere" al proprietario, quindi creare un profilo criterio che consente l'esecuzione del software di navigazione GPS solo nei dispositivi i cui proprietari hanno il ruolo "Corriere". Tutte le altre impostazioni del criterio vengono mantenute. Solo l'utente con il ruolo "Corriere" sarà autorizzato a eseguire il software di navigazione GPS. Se in seguito viene assegnato il ruolo "Corriere" a un altro dipendente, anche il nuovo dipendente potrà eseguire il software di navigazione nel dispositivo dell'organizzazione. L'esecuzione del software di navigazione GPS sarà ancora non consentita negli altri dispositivi dello stesso gruppo di amministrazione.

Per associare un ruolo a un profilo criterio:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.

2. Fare clic sul nome del ruolo che si desidera associare a un profilo criterio.

   Verrà visualizzata la finestra delle proprietà del ruolo, con la scheda **Generale** selezionata.

3. Selezionare la scheda **Impostazioni** e scorrere fino alla sezione **Criteri e profili**.

4. Fare clic su **Modifica**.

5. Per associare il ruolo a:

   - **Un profilo criterio esistente**: fare clic sull'icona della freccia di espansione (>) accanto al nome del criterio desiderato, quindi selezionare la casella di controllo accanto al profilo a cui associare il ruolo.

   - **Un nuovo profilo criterio**:

     a. Selezionare la casella di controllo accanto al criterio per cui si desidera creare un profilo.

     b. Fare clic su **Nuovo profilo criterio**.

     c. Specificare un nome per il nuovo profilo e configurare le impostazioni del profilo.

     d. Fare clic sul pulsante **Salva**.

     e. Selezionare la casella di controllo accanto al nuovo profilo.

6. Fare clic su **Assegna al ruolo**.

Il profilo verrà associato al ruolo e visualizzato nelle proprietà del ruolo. Il profilo si applica automaticamente a qualsiasi dispositivo il cui proprietario è assegnato al ruolo.

Creazione di un gruppo di protezione

Per creare un gruppo di protezione:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Gruppi**.

2. Fai clic su **Nuovo gruppo**.

3. Nella finestra **Nuovo gruppo**, specificare le seguenti impostazioni per il nuovo gruppo di sicurezza:

   - **Nome**

   - **Descrizione**

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

Un nuovo gruppo di protezione viene aggiunto all'elenco dei gruppi di sicurezza.

Modifica di un gruppo di protezione

Per modificare un gruppo di protezione:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Gruppi**.

2. Fare clic sul nome del gruppo di protezione che si desidera modificare.

3. Nella finestra delle impostazioni del gruppo visualizzata modificare le impostazioni del gruppo di protezione:

   - Nella scheda **Generale**, è possibile modificare le impostazioni **Nome** e **Descrizione**. Queste impostazioni sono disponibili solo per i gruppi di protezione interni.
   - Nella scheda **Utenti**, è possibile aggiungere utenti al gruppo di protezione. Questa impostazione è disponibile solo per utenti interni e gruppi di protezione interni.
   - Nella scheda **Ruoli**, è possibile assegnare un ruolo al gruppo di protezione.

4. Fare clic su **Salva** per salvare le modifiche.

Le modifiche vengono applicate al gruppo di protezione.

Aggiunta di account utente a un gruppo interno

È possibile aggiungere solo account di utenti interni a un gruppo interno.

Per aggiungere account utente a un gruppo interno:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Selezionare le caselle di controllo accanto agli account utente che si desidera aggiungere a un gruppo.
3. Fare clic sul pulsante **Assegna gruppo**.
4. Nella finestra **Assegna gruppo** visualizzata selezionare il gruppo a cui si desidera aggiungere gli account utente.
5. Fare clic sul pulsante **Assegna**.

Gli account utente verranno aggiunti al gruppo. È inoltre possibile aggiungere utenti interni a un gruppo utilizzando le impostazioni del gruppo.

Eliminazione di un gruppo di protezione

È possibile eliminare solo gruppi di protezione interni.

Per eliminare un gruppo di utenti:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Gruppi**.
2. Selezionare la casella di controllo accanto al gruppo di utenti che si desidera eliminare.
3. Fare clic su **Elimina**, quindi confermare l'eliminazione nella finestra aperta.

Il gruppo di utenti viene eliminato.

Configurazione dell'integrazione ADFS

Per consentire agli utenti registrati in Active Directory (AD) nell'organizzazione di accedere a Kaspersky Security Center Cloud Console, è necessario configurare l'integrazione con Active Directory Federation Services (ADFS).

Kaspersky Security Center Cloud Console supporta ADFS 3 (Windows Server 2016) o una versione successiva.

Per modificare le impostazioni di integrazione ADFS, è necessario disporre del diritto di accesso per modificare le autorizzazioni utente.

Prima di procedere, assicurarsi di aver completato il polling di Active Directory.

Per configurare l'integrazione ADFS:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome di Administration Server.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale**, selezionare la sezione **Impostazioni per l'integrazione ADFS**.

3. Copiare l'URL di callback.

   Questa URL sarà necessaria per configurare l'integrazione in Console di gestione di ADFS.

4. In Console di gestione di ADFS aggiungere un nuovo gruppo di applicazioni, quindi aggiungere una nuova applicazione selezionando il modello **Applicazione server** (i nomi degli elementi di interfaccia Microsoft sono disponibili in inglese).

   Console di gestione di ADFS genera l'ID client per la nuova applicazione. L'ID client sarà necessario per configurare l'integrazione in Kaspersky Security Center Cloud Console.

5. Come URI di reindirizzamento, specificare l'URL di callback copiata nella finestra delle proprietà di Administration Server.

6. Generare un segreto client. Il segreto client sarà necessario per configurare l'integrazione in Kaspersky Security Center Cloud Console.

7. Salvare le proprietà dell'applicazione aggiunta.

8. Aggiungere una nuova applicazione al gruppo di applicazioni creato. Questa volta selezionare il modello **API Web**.

9. Nella scheda **Identificatori**, nell'elenco **Identificatori componente** aggiungere l'ID client dell'applicazione server aggiunta in precedenza.

10. Nella scheda **Autorizzazioni client**, nell'elenco **Ambiti consentiti** selezionare gli ambiti **allatclaims** e **openid**.

11. Nella scheda **Regole di trasformazione rilascio** aggiungere una nuova regola selezionando il modello **Inviare attributi LDAP come attestazioni**:

    a. Assegnare un nome alla regola. È ad esempio possibile denominarla "SID gruppo".

b. Selezionare **Active Directory** come archivio di attributi, quindi eseguire il mapping di **Token-Groups come SID** come attributo LDAP su "SID gruppo" come tipo di attestazione in uscita.

12. Nella scheda **Regole di trasformazione rilascio** aggiungere una nuova regola selezionando il modello **Inviare attestazioni mediante una regola personalizzata**:

    a. Assegnare un nome alla regola. È ad esempio possibile denominarla "ActiveDirectoryUserSID".

    b. Nel campo **Regola personalizzata** digitare:

    ```
    c:[Type ==
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
    Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types =
    ("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query =
    ";objectSID;{0}", param = c.Value);
    ```

13. In Kaspersky Security Center Cloud Console aprire nuovamente la sezione **Impostazioni per l'integrazione ADFS**.

14. Spostare l'interruttore sulla posizione **Integrazione ADFS Abilitata**.

15. Fare clic sul collegamento **Impostazioni** e specificare il file contenente il certificato o più certificati per il server federativo.

16. Fare clic sul collegamento **Impostazioni per l'integrazione ADFS**, quindi specificare le seguenti impostazioni:

- **URL emittente**

  L'indirizzo URL del server federativo in uso nell'organizzazione.

  In particolare, Kaspersky Security Center Cloud Console aggiunge "/.well-known/openid-configuration" all'indirizzo URL dell'emittente e tenta di aprire l'indirizzo URL risultante (issuer_URL/.well-known/openid-configuration) per scoprire automaticamente la configurazione dell'emittente.

- **ID client**

  ID client generato dal server federativo per identificare Kaspersky Security Center Cloud Console. L'ID client è disponibile in Console di gestione di ADFS nella finestra delle proprietà dell'applicazione server corrispondente a Kaspersky Security Center Cloud Console.

- **Segreto client**

  Viene generato un segreto client in Console di gestione di ADFS quando vengono specificate le proprietà dell'applicazione server corrispondente a Kaspersky Security Center Cloud Console.

- **Dominio da cui autenticare gli utenti**

  I membri del dominio selezionato potranno accedere a Kaspersky Security Center Cloud Console con le credenziali dell'account di dominio. I nomi di dominio vengono visualizzati nell'elenco dopo il completamento del polling della rete.

- **Nome del campo per il SID dell'utente nel token ID**

Nome del campo che fa riferimento al SID utente nel token ID. Il nome del campo è necessario per identificare l'utente in Kaspersky Security Center Cloud Console. Per impostazione predefinita, questo campo nel token ID si chiama "primarysid".

- Nome del campo per l'array di SID dei gruppi di utenti nel token ID

  Nome del campo che fa riferimento all'array di SID dei gruppi di protezione di Active Directory in cui è incluso l'utente. Per impostazione predefinita, questo campo nel token ID si chiama "groupsid".

17. Fare clic sul pulsante **Salva**.

L'integrazione con ADFS è stata completata. Per accedere a Kaspersky Security Center Cloud Console con le credenziali di un account AD, utilizzare il collegamento disponibile nella sezione **Impostazioni per l'integrazione ADFS** (**Collegamento per l'accesso a Kaspersky Security Center Cloud Console con ADFS**).

Quando si accede a Kaspersky Security Center Cloud Console tramite ADFS per la prima volta, la console potrebbe rispondere con ritardo.

Assegnazione di un utente come proprietario dispositivo

Per informazioni sull'assegnazione di un utente come proprietario di un dispositivo mobile, vedere la Guida di Kaspersky Security for Mobile.

Per assegnare un utente come proprietario dispositivo:

1. Se si desidera assegnare un proprietario di un dispositivo connesso a un Administration Server virtuale, passare prima all'Administration Server virtuale:

   a. Nel menu principale, fare clic sull'icona a forma di freccia di espansione (>) a destra del nome corrente dell'Administration Server.

   b. Selezionare l'Administration Server desiderato.

2. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.

   Verrà visualizzato un elenco di utenti. Se si è attualmente connessi a un Administration Server virtuale, l'elenco include gli utenti dell'Administration Server virtuale corrente e dell'Administration Server primario.

3. Fare clic sul nome dell'account utente che si desidera assegnare come proprietario dispositivo.

4. Nella finestra delle impostazioni utente visualizzata, selezionare la scheda **Dispositivi**.

5. Fare clic su **Aggiungi**.

6. Dall'elenco dei dispositivi selezionare il dispositivo che si desidera assegnare all'utente.

7. Fare clic su **OK**.

Il dispositivo selezionato verrà aggiunto all'elenco dei dispositivi assegnati all'utente.

È possibile eseguire la stessa operazione in **Risorse (dispositivi)** → **Dispositivi gestiti**, facendo clic sul nome del dispositivo che si desidera assegnare e quindi facendo clic sul collegamento **Gestisci proprietario dispositivo**.

Gestione delle revisioni degli oggetti

Questa sezione contiene informazioni sulla gestione delle revisioni degli oggetti.

Gli oggetti che supportano la gestione delle revisioni includono:

- Administration Server
- Criteri
- Attività
- Gruppi di amministrazione
- Account utente
- Pacchetti di installazione

Informazioni sulle revisioni degli oggetti

Kaspersky Security Center Cloud Console consente di tenere traccia delle modifiche apportate agli oggetti. Ogni volta che si salvano le modifiche apportate a un oggetto, viene creata una *revisione*. Ogni revisione ha un numero.

È possibile eseguire le seguenti azioni sulle revisioni degli oggetti:

- Visualizzare una revisione selezionata
- Eseguire il rollback delle modifiche apportate a un oggetto a una revisione selezionata

Nella finestra delle proprietà di un oggetto che supporta la gestione delle revisioni, la sezione **Cronologia revisioni** visualizza un elenco delle revisioni degli oggetti con i seguenti dettagli:

- Numero di revisione dell'oggetto
- Data e ora di modifica dell'oggetto
- Nome dell'utente che ha modificato l'oggetto
- Azione eseguita sull'oggetto
- Descrizione della revisione relativa alla modifica apportata alle impostazioni dell'oggetto

  Per impostazione predefinita, la descrizione della revisione dell'oggetto è vuota. Per aggiungere una descrizione a una revisione, selezionare la revisione desiderata, quindi fare clic sul pulsante **Modifica descrizione**. Nella finestra visualizzata immettere il testo relativo alla descrizione della revisione.

Rollback delle modifiche

È possibile eseguire il rollback delle modifiche apportate a un oggetto, se necessario. Potrebbe ad esempio essere necessario ripristinare lo stato delle impostazioni di un criterio in una data specifica.

Per eseguire il rollback delle modifiche apportate a un oggetto:

1. Passare alla sezione **Cronologia revisioni** dell'oggetto.
2. Nell'elenco delle revisioni dell'oggetto selezionare il numero della revisione a cui eseguire il rollback delle modifiche.
3. Fare clic sul pulsante **Rollback**.

Verrà eseguito il rollback dell'oggetto alla revisione selezionata. L'elenco delle revisioni dell'oggetto visualizza un record dell'azione eseguita. La descrizione della revisione indica il numero della revisione a cui è stato riportato l'oggetto.

Aggiunta di una descrizione della revisione

È possibile aggiungere una descrizione per la revisione, in modo da semplificare la ricerca delle revisioni nell'elenco.

Per aggiungere una descrizione per una revisione:

1. Passare alla sezione **Cronologia revisioni** dell'oggetto.
2. Nell'elenco delle revisioni di un oggetto selezionare la revisione per cui è necessario aggiungere una descrizione.
3. Fare clic sul pulsante **Modifica descrizione**.
4. Nella finestra visualizzata immettere il testo relativo alla descrizione della revisione.
   Per impostazione predefinita, la descrizione della revisione dell'oggetto è vuota.
5. Fare clic su **Salva**.

La nuova descrizione viene visualizzata nella colonna **Descrizione** della tabella della cronologia delle revisioni.

Eliminazione di oggetti

È possibile eliminare oggetti come:

- Criteri
- Attività
- Pacchetti di installazione

- Administration Server virtuali
- Utenti
- Gruppi di protezione
- Gruppi di amministrazione

Quando si elimina un oggetto, le relative informazioni rimangono nel database. Il periodo di archiviazione per le informazioni sugli oggetti eliminati corrisponde al periodo di archiviazione per le revisioni degli oggetti (il periodo consigliato è di 90 giorni). È possibile modificare il periodo di archiviazione solo se si dispone dell'autorizzazione **Modifica** nell'area dei diritti **Oggetti eliminati**.

Informazioni sull'eliminazione dei dispositivi client

Quando si elimina un dispositivo gestito da un gruppo di amministrazione, l'applicazione sposta il dispositivo nel gruppo Dispositivi non assegnati. Dopo l'eliminazione del dispositivo, le applicazioni Kaspersky installate, Network Agent e qualsiasi applicazione di sicurezza, ad esempio Kaspersky Endpoint Security, rimangono nel dispositivo.

Kaspersky Security Center Cloud Console gestisce i dispositivi nel gruppo Dispositivi non assegnati in base alle seguenti regole:

- Se sono state configurate regole di spostamento dei dispositivi e un dispositivo soddisfa i criteri di una regola di spostamento, il dispositivo viene spostato automaticamente in un gruppo di amministrazione in base alla regola.
- Il dispositivo viene archiviato nel gruppo Dispositivi non assegnati e rimosso automaticamente dal gruppo in base alle regole di conservazione dei dispositivi.

  Le regole di conservazione dei dispositivi non influiscono sui dispositivi con una o più unità criptate con Criptaggio dell'intero disco. Tali dispositivi non vengono eliminati automaticamente; è possibile eliminarli solo manualmente. Se è necessario eliminare un dispositivo con un'unità criptata, decriptare prima l'unità, quindi eliminare il dispositivo.

  Quando si elimina un dispositivo con un'unità criptata, vengono eliminati anche i dati necessari per decriptare l'unità. In questo caso, per decriptare l'unità, devono essere soddisfatte le seguenti condizioni:

  - Il dispositivo viene riconnesso ad Administration Server al fine di ripristinare i dati necessari per decriptare l'unità.
  - L'utente del dispositivo ricorda la password di decriptaggio.
  - L'applicazione di sicurezza utilizzata per criptare l'unità, ad esempio Kaspersky Endpoint Security for Windows, è ancora installata nel dispositivo.

  Se l'unità è stata criptata con la tecnologia Criptaggio disco Kaspersky, è inoltre possibile provare a recuperare i dati utilizzando l'utilità di ripristino FDERT.

Quando si elimina manualmente un dispositivo dal gruppo Dispositivi non assegnati, l'applicazione rimuove il dispositivo dall'elenco. Dopo l'eliminazione del dispositivo, le eventuali applicazioni Kaspersky installate rimangono nel dispositivo. Quindi, se il dispositivo è ancora visibile in Administration Server ed è stato configurato il polling di rete periodico, Kaspersky Security Center Cloud Console rileva il dispositivo durante il polling di rete e lo aggiunge nuovamente al gruppo Dispositivi non assegnati. Pertanto, è ragionevole eliminare manualmente un dispositivo solo se il dispositivo è invisibile ad Administration Server.

Aggiornamento di database e applicazioni Kaspersky

Questa sezione descrive i passaggi da eseguire per aggiornare periodicamente i seguenti elementi:

- Database e moduli del software Kaspersky
- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center Cloud Console e le applicazioni di protezione

Scenario: Aggiornamento periodico di database e applicazioni Kaspersky

Questa sezione fornisce uno scenario per l'aggiornamento periodico dei database, dei moduli software e delle applicazioni Kaspersky. Dopo aver completato lo scenario di configurazione della protezione di rete, è necessario mantenere l'affidabilità del sistema di protezione. Questa manutenzione garantisce l'efficacia costante della protezione dei dispositivi gestiti contro un'ampia gamma di minacce, inclusi virus, attacchi di rete e attacchi di phishing.

Esistono diversi schemi che è possibile utilizzare per installare gli aggiornamenti dei componenti di Kaspersky Security Center Cloud Console e delle applicazioni di protezione. Scegliere uno o più schemi appropriati per i requisiti della rete.

Lo scenario seguente descrive lo schema di aggiornamento che implica il download degli aggiornamenti negli archivi dei punti di distribuzione. Se i dispositivi gestiti non dispongono di una connessione ai punti di distribuzione, valutare se eseguire l'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky manualmente o direttamente dai server di aggiornamento Kaspersky.

Al completamento di questo scenario, si ottengono i seguenti risultati:

- I componenti di Kaspersky Security Center Cloud Console vengono aggiornati automaticamente o solo quando si specifica lo stato *Approvato* per gli aggiornamenti.
- Le applicazioni di protezione Kaspersky, i database Kaspersky e i moduli software vengono aggiornati in base alla pianificazione specificata. Per impostazione predefinita, le applicazioni di protezione Kaspersky installano solo gli aggiornamenti approvati dall'utente.

È possibile configurare il processo di aggiornamento per scaricare e installare gli aggiornamenti in due modi:

- Automaticamente

  In questo caso è necessario eseguire questo scenario una sola volta. Sarà necessario pianificare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* (se presente) e le attività di aggiornamento per le applicazioni di protezione Kaspersky e mantenere le impostazioni di aggiornamento predefinite disponibili nelle proprietà di Network Agent.

- Manualmente

  È possibile configurare il processo di aggiornamento per eseguire l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* (se presente) e le attività di aggiornamento per le applicazioni di protezione Kaspersky manualmente. È inoltre possibile configurare Network Agent per l'installazione degli aggiornamenti per i componenti di Kaspersky Security Center Cloud Console solo quando si specifica lo stato *Approvato* per gli aggiornamenti.

Prerequisiti

Prima di iniziare, verificare di avere:

1. Distribuito le applicazioni di protezione Kaspersky nei dispositivi gestiti in base allo scenario di distribuzione delle applicazioni Kaspersky tramite Kaspersky Security Center Cloud Console. Durante l'esecuzione di questo scenario, è stato assegnato un numero appropriato di punti di distribuzione in base al numero di dispositivi gestiti e alla topologia della rete.

2. Creato e configurato tutti i criteri, i profili criterio e le attività richiesti in base allo scenario di configurazione della protezione di rete.

Passaggi

La configurazione dell'aggiornamento periodico dei database e delle applicazioni Kaspersky prevede diversi passaggi:

1. **Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione**

   Creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*. Durante l'esecuzione di questa attività, Kaspersky Security Center Cloud Console scarica gli aggiornamenti nei punti di distribuzione direttamente dai server di aggiornamento Kaspersky.

   Istruzioni dettagliate: Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione

2. **Configurazione dei punti di distribuzione**

   Assicurarsi che l'opzione **Distribuisci aggiornamenti** sia abilitata nelle proprietà di tutti i punti di distribuzione richiesti. Quando questa opzione è disabilitata per un punto di distribuzione, i dispositivi inclusi nell'ambito del punto di distribuzione possono scaricare gli aggiornamenti esclusivamente da una risorsa locale o direttamente dai server di aggiornamento Kaspersky.

   Se si desidera che i dispositivi gestiti ricevano gli aggiornamenti solo dai punti di distribuzione, abilitare l'opzione **Distribuisci i file solo tramite punti di distribuzione** nel criterio di Network Agent.

3. **Ottimizzazione del processo di aggiornamento utilizzando i file diff (opzionale)**

   Abilitando questa funzionalità si riduce il traffico tra i punti di distribuzione e i dispositivi gestiti. Per utilizzare questa funzionalità, abilitare l'opzione **Scarica file diff** nelle proprietà dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

   Istruzioni dettagliate: Utilizzo dei file diff per l'aggiornamento dei database e dei moduli del software Kaspersky

4. **Definizione degli aggiornamenti da installare**

   Per impostazione predefinita, gli aggiornamenti software scaricati hanno lo stato *Indefinito*. Modificare lo stato in *Approvato* o *Rifiutato* per definire se l'aggiornamento deve essere installato nei dispositivi della rete. Gli aggiornamenti approvati vengono sempre installati. Gli aggiornamenti indefiniti possono essere installati solo in Network Agent e negli altri componenti di Kaspersky Security Center Cloud Console in conformità con le impostazioni del criterio di Network Agent. Gli aggiornamenti per cui è stato impostato lo stato *Rifiutato* non verranno installati nei dispositivi.

   Istruzioni dettagliate:

   - Informazioni sugli stati degli aggiornamenti
   - Approvazione e rifiuto degli aggiornamenti software

5. **Configurazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center Cloud Console**

Per impostazione predefinita, gli aggiornamenti scaricati e le patch scaricate per Network Agent e altri componenti di Kaspersky Security Center Cloud Console vengono installati automaticamente. Se l'opzione **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito** è stata mantenuta abilitata nelle proprietà di Network Agent, tutti gli aggiornamenti verranno installati automaticamente dopo essere stati scaricati nell'archivio (o in diversi archivi). Se questa opzione è disabilitata, le patch di Kaspersky che sono state scaricate e contrassegnate con lo stato *Indefinito* saranno installate solo dopo che si modifica il relativo stato in *Approvato*.

Istruzioni dettagliate: Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center Cloud Console

6. **Configurazione dell'installazione automatica degli aggiornamenti per le applicazioni di protezione**

   Creare le attività di aggiornamento per le applicazioni gestite per garantire aggiornamenti tempestivi alle applicazioni, ai moduli software e ai database Kaspersky, inclusi i database anti-virus. È consigliabile selezionare l'opzione **Quando vengono scaricati nuovi aggiornamenti nell'archivio** durante la configurazione della pianificazione dell'attività. In questo modo i nuovi aggiornamenti verranno installati il prima possibile.

   Per impostazione predefinita, gli aggiornamenti per le applicazioni gestite vengono installati solo dopo aver modificato lo stato dell'aggiornamento in *Approvato*. Per Kaspersky Endpoint Security for Windows, è possibile modificare le impostazioni di aggiornamento nell'attività di aggiornamento.

   Se un aggiornamento richiede la visualizzazione e l'accettazione dei termini del Contratto di licenza con l'utente finale, è prima necessario accettare i termini. Successivamente, l'aggiornamento può essere propagato ai dispositivi gestiti.

   Istruzioni dettagliate: Installazione automatica degli aggiornamenti di Kaspersky Endpoint Security nei dispositivi

Al completamento dello scenario, è possibile procedere al monitoraggio dello stato della rete.

Informazioni sull'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky

Per assicurarsi che la protezione dei propri dispositivi gestiti sia aggiornata, è necessario garantire aggiornamenti tempestivi dei seguenti elementi:

- Database e moduli del software Kaspersky

  Prima di scaricare i database e i moduli software di Kaspersky, Kaspersky Security Center Cloud Console verifica se i server Kaspersky sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. Ciò è necessario per garantire che i database anti-virus siano aggiornati e per mantenere il livello di sicurezza per i dispositivi gestiti.

- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center Cloud Console e le applicazioni di protezione

In base alla configurazione della propria rete è possibile utilizzare i seguenti schemi di download e distribuzione degli aggiornamenti richiesti ai dispositivi gestiti:

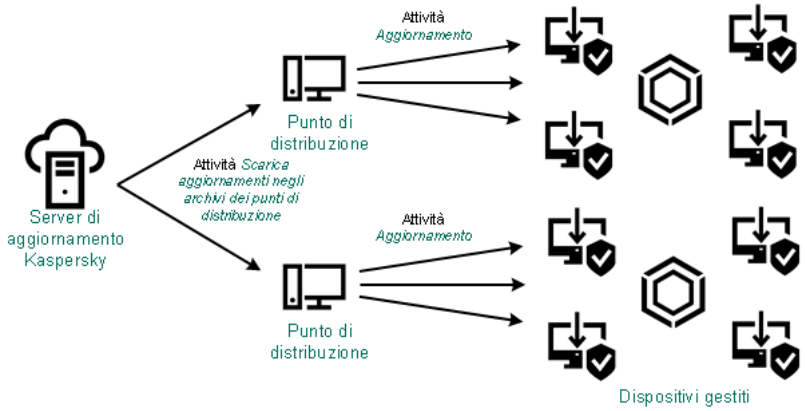
- Utilizzo dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*
- Manualmente attraverso una cartella locale, una cartella condivisa o un server FTP
- Direttamente dai server di aggiornamento Kaspersky alle applicazioni di protezione nei dispositivi gestiti

Utilizzo dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

In questo schema Kaspersky Security Center Cloud Console scarica gli aggiornamenti tramite l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*. I dispositivi gestiti inclusi nell'ambito di un punto di distribuzione scaricano gli aggiornamenti dall'archivio dei punti di distribuzione (vedere la figura di seguito).

I dispositivi dei punti di distribuzione che eseguono macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky.

Se uno o più dispositivi che eseguono macOS rientrano nell'ambito dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'attività viene completata con lo stato *Non riuscito*, anche se è stata completata correttamente in tutti i dispositivi Windows.



Aggiornamento utilizzando l'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

Al completamento dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, i seguenti aggiornamenti vengono scaricati nell'archivio dei punti di distribuzione:

- Moduli del software e database Kaspersky per le applicazioni di protezione nei dispositivi gestiti

  Questi aggiornamenti vengono installati tramite l'attività di aggiornamento per Kaspersky Endpoint Security for Windows.

- Aggiornamenti per i componenti di Kaspersky Security Center Cloud Console

  Per impostazione predefinita, questi aggiornamenti vengono installati automaticamente. È possibile modificare le impostazioni nel criterio di Network Agent.

- Aggiornamenti per le applicazioni di protezione

  Per impostazione predefinita, Kaspersky Endpoint Security for Windows installa solo gli aggiornamenti approvati dall'utente. Gli aggiornamenti vengono installati attraverso l'attività di aggiornamento e possono essere configurati nelle proprietà di questa attività.

Ogni applicazione Kaspersky richiede gli aggiornamenti necessari da Administration Server. Administration Server aggrega tali richieste e scarica negli archivi dei punti di distribuzione solo gli aggiornamenti che sono richiesti da un'applicazione. Questo garantisce che gli stessi aggiornamenti non vengano scaricati più volte e che gli aggiornamenti non necessari non vengano scaricati affatto. Durante l'esecuzione dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, Administration Server invia automaticamente le seguenti informazioni ai server di aggiornamento Kaspersky per garantire il download delle versioni appropriate dei moduli software e dei database Kaspersky:

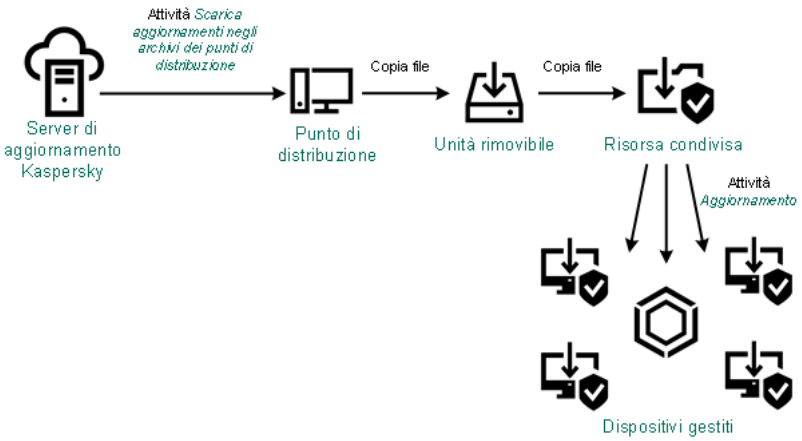
- Versione e ID applicazione
- ID di installazione dell'applicazione
- ID chiave attiva

- ID esecuzione attività di download

Le informazioni trasmesse non contengono dati personali o altri dati riservati. AO Kaspersky Lab protegge le informazioni in base ai requisiti previsti dalla legge.

Manualmente attraverso una cartella locale, una cartella condivisa o un server FTP

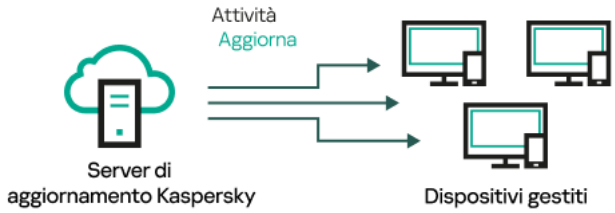
Se i dispositivi client non hanno una connessione a un punto di distribuzione, è possibile utilizzare una cartella locale o una risorsa condivisa come sorgente per l'aggiornamento di database, moduli software e applicazioni Kaspersky. In questo schema è necessario copiare gli aggiornamenti richiesti da un archivio dei punti di distribuzione in un'unità rimovibile, quindi copiare gli aggiornamenti nella cartella locale o nella risorsa condivisa specificata come sorgente aggiornamenti nelle impostazioni di Kaspersky Endpoint Security for Windows (vedere la figura di seguito).



Aggiornamento tramite una cartella locale, una cartella condivisa o un server FTP

Direttamente dai server di aggiornamento Kaspersky a Kaspersky Endpoint Security for Windows nei dispositivi gestiti

Nei dispositivi gestiti è possibile configurare Kaspersky Endpoint Security for Windows per ricevere gli aggiornamenti direttamente dai server di aggiornamento Kaspersky (vedere la figura di seguito).



Aggiornamento delle applicazioni di protezione direttamente dai server di aggiornamento Kaspersky

In questo schema l'applicazione di protezione non utilizza gli archivi forniti da Kaspersky Security Center Cloud Console. Per ricevere gli aggiornamenti direttamente dai server di aggiornamento Kaspersky, specificare i server di aggiornamento Kaspersky come sorgente aggiornamenti nell'interfaccia dell'applicazione di protezione. Per una descrizione completa di queste impostazioni, fare riferimento alla documentazione di Kaspersky Endpoint Security for Windows.

Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione

I dispositivi dei punti di distribuzione che eseguono macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky.

Se uno o più dispositivi che eseguono macOS rientrano nell'ambito dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'attività viene completata con lo stato *Non riuscito*, anche se è stata completata correttamente in tutti i dispositivi Windows.

È possibile creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per un gruppo di amministrazione. L'attività verrà eseguita per i punti di distribuzione inclusi nel gruppo di amministrazione specificato.

Questa attività è necessaria per scaricare gli aggiornamenti dai server di aggiornamento Kaspersky negli archivi dei punti di distribuzione. L'elenco degli aggiornamenti include:

- Aggiornamenti dei database e dei moduli software delle applicazioni di protezione Kaspersky
- Aggiornamenti dei componenti di Kaspersky Security Center Cloud Console
- Aggiornamenti delle applicazioni di protezione Kaspersky

Dopo aver scaricato gli aggiornamenti, questi possono essere propagati ai dispositivi gestiti.

*Per creare l'attività **Scarica aggiornamenti negli archivi dei punti di distribuzione** per un gruppo di amministrazione selezionato:*

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center Cloud Console, nel campo **Tipo di attività** selezionare **Scarica aggiornamenti negli archivi dei punti di distribuzione**.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare un pulsante di opzione per specificare il gruppo di amministrazione, la selezione dispositivi o i dispositivi a cui si applica l'attività.
6. Nel passaggio **Completa creazione attività**, se si abilita l'opzione **Apri i dettagli dell'attività al termine della creazione**, è possibile modificare le impostazioni predefinite dell'attività. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
7. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
8. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.
9. Nella scheda **Impostazioni applicazione** della finestra delle proprietà dell'attività specificare le seguenti impostazioni:
   - Sorgenti degli aggiornamenti

È possibile utilizzare le seguenti risorse come sorgenti degli aggiornamenti per il punto di distribuzione:

- Server degli aggiornamenti Kaspersky

  I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.

  Questa opzione è selezionata per impostazione predefinita.

- Administration Server primario

  Questa risorsa si applica alle attività create per un Administration Server secondario o virtuale.

- Cartella locale o di rete

  Un'unità locale o una cartella di rete che contiene gli aggiornamenti più recenti. Una cartella di rete può essere un server FTP o HTTP oppure una condivisione SMB. Se una cartella di rete richiede l'autenticazione, è supportato solo il protocollo SMB. Quando si seleziona una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server.

  Una cartella di rete o un server FTP o HTTP utilizzato da una sorgente aggiornamenti deve contenere una struttura di cartelle (con gli aggiornamenti) che corrisponde alla struttura creata durante l'utilizzo dei server di aggiornamento Kaspersky.

- **Cartella per l'archiviazione degli aggiornamenti**

  Il percorso della cartella specificata per l'archiviazione degli aggiornamenti salvati. È possibile copiare il percorso della cartella specificata negli appunti. Non è possibile modificare il percorso di una cartella specificata per un'attività di gruppo.

- **Scarica file diff**

  Questa opzione consente di abilitare la funzionalità di download dei file diff.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica gli aggiornamenti utilizzando lo schema precedente**

Kaspersky Security Center Cloud Console scarica gli aggiornamenti di database e moduli software utilizzando il nuovo schema. Affinché l'applicazione possa scaricare gli aggiornamenti utilizzando il nuovo schema, la sorgente aggiornamenti deve contenere i file di aggiornamento con i metadati compatibili con il nuovo schema. Se la sorgente aggiornamenti contiene i file di aggiornamento con i metadati compatibili solo con lo schema precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**. In caso contrario, l'attività di download degli aggiornamenti avrà esito negativo.

È ad esempio necessario abilitare questa opzione quando una cartella locale o di rete è specificata come sorgente aggiornamenti e i file di aggiornamento in questa cartella sono stati scaricati da una delle seguenti applicazioni:

- Kaspersky Update Utility

  Questa utilità scarica gli aggiornamenti utilizzando lo schema precedente.

- Kaspersky Security Center 13.2 o versione precedente

Un punto di distribuzione è ad esempio configurato per acquisire gli aggiornamenti da una cartella locale o di rete. In questo caso, è possibile scaricare gli aggiornamenti utilizzando un Administration Server dotato di una connessione Internet, quindi posizionare gli aggiornamenti nella cartella locale nel punto di distribuzione. Se la versione di Administration Server è la 13.2 o precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente** nell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

Per impostazione predefinita, questa opzione è disabilitata.

10. Creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Manualmente** (opzione selezionata per impostazione predefinita)

    L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N settimane**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

- **Giornaliera (ora legale non supportata)**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

  Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center Cloud Console.

  Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

- **Settimanale**

  L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è 18:00:00.

- **Durante un'epidemia di virus**

L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

- Anti-virus per workstation e file server
- Anti-virus per la difesa perimetrale
- Anti-virus per i sistemi di posta

Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

Può essere utile eseguire differenti attività a seconda del tipo di applicazione anti-virus che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

  L'attività corrente viene avviata dopo il completamento di un'altra attività. È possibile selezionare la modalità di completamento dell'attività precedente (correttamente o con errori) per l'attivazione dell'avvio dell'attività corrente. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus*. Questo parametro funziona solo se entrambe le attività sono assegnate agli stessi dispositivi.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, vengono eseguite solo le attività pianificate nei dispositivi client. Per le opzioni **Manualmente**, **Una sola volta** e **Immediatamente**, le attività sono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è abilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

11. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Oltre alle impostazioni specificate durante la creazione dell'attività, è possibile modificare altre proprietà di un'attività creata.

Quando si esegue l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, gli aggiornamenti dei database e dei moduli software vengono scaricati dalla sorgente degli aggiornamenti e archiviati nella cartella condivisa. Gli aggiornamenti scaricati verranno utilizzati solo dai punti di distribuzione inclusi nel gruppo di amministrazione specificato e che non hanno alcuna attività di download degli aggiornamenti esplicitamente configurata.

Configurazione dei dispositivi gestiti per la ricezione di aggiornamenti solo dai punti di distribuzione

I dispositivi gestiti possono recuperare gli aggiornamenti di database Kaspersky, moduli software e applicazioni Kaspersky da diverse origini: direttamente dai server di aggiornamento, dai punti di distribuzione oppure da una cartella locale o di rete. È possibile specificare i punti di distribuzione come l'unica sorgente possibile degli aggiornamenti.

Per configurare i dispositivi gestiti per la ricezione degli aggiornamenti solo dai punti di distribuzione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Network Agent.
3. Nella finestra delle proprietà del criterio aprire la scheda **Impostazioni applicazione**.
4. Nella sezione **Impostazioni** attivare l'interruttore **Distribuisci i file solo tramite punti di distribuzione**.
5. Impostare il lucchetto (🔒) per questo interruttore.
6. Fare clic sul pulsante **Salva**.

Il criterio verrà applicato ai dispositivi selezionati e i dispositivi riceveranno aggiornamenti solo dai punti di distribuzione.

Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center Cloud Console

L'installazione automatica degli aggiornamenti e delle patch per i componenti di Kaspersky Security Center Cloud Console è abilitata per impostazione predefinita durante l'installazione di Network Agent nel dispositivo. È possibile disabilitarla durante l'installazione di Network Agent o disabilitarla in un secondo momento utilizzando un criterio.

Per disabilitare l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center Cloud Console durante l'installazione locale di Network Agent in un dispositivo:

1. Avviare l'installazione locale di Network Agent nel dispositivo.
2. Durante il passaggio **Impostazioni avanzate** deselezionare la casella di controllo **Installa automaticamente gli aggiornamenti applicabili e le patch per i componenti con stato Indefinito**.
3. Seguire le istruzioni della procedura guidata.

Nel dispositivo verrà installato Network Agent con l'installazione automatica di aggiornamenti e patch disabilitata per i componenti di Kaspersky Security Center Cloud Console. È possibile abilitare l'installazione automatica di aggiornamenti e patch in un secondo momento utilizzando un criterio.

Per disabilitare l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center Cloud Console durante l'installazione di Network Agent nel dispositivo tramite un pacchetto di installazione:

1. Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.
2. Fare clic sul pacchetto **Kaspersky Security Center Network Agent <numero di versione>**.
3. Nella finestra delle proprietà selezionare la scheda **Impostazioni**.
4. Disattivare l'interruttore **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito**.

Network Agent con l'installazione automatica di aggiornamenti e patch disabilitata per i componenti di Kaspersky Security Center Cloud Console verrà installato da questo pacchetto. È possibile abilitare l'installazione automatica di aggiornamenti e patch in un secondo momento utilizzando un criterio.

Se la casella di controllo nel passaggio 4 è stata selezionata o deselezionata durante l'installazione di Network Agent nel dispositivo, successivamente è possibile abilitare (o disabilitare) l'aggiornamento automatico utilizzando il criterio di Network Agent.

Per abilitare o disabilitare l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center Cloud Console utilizzando il criterio di Network Agent:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Network Agent.
3. Nella finestra delle proprietà del criterio selezionare la scheda **Impostazioni applicazione**.
4. Nella sezione **Gestire patch e aggiornamenti** attivare o disattivare l'interruttore **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito** per abilitare o disabilitare, rispettivamente, l'applicazione automatica di aggiornamenti e patch.
5. Assicurarsi di impostare il lucchetto (**Applica**) (🔒) per questo interruttore.

Il criterio verrà applicato ai dispositivi selezionati e l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center Cloud Console verrà abilitata (o disabilitata) in tali dispositivi.

Installazione automatica degli aggiornamenti per Kaspersky Endpoint Security for Windows

È possibile configurare gli aggiornamenti automatici dei database e dei moduli software di Kaspersky Endpoint Security for Windows nei dispositivi client.

Per configurare il download e l'installazione automatica degli aggiornamenti di Kaspersky Endpoint Security for Windows nei dispositivi:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Endpoint Security for Windows, selezionare **Aggiornamento** come sottotipo di attività.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Scegliere l'ambito dell'attività.
6. Specificare il gruppo di amministrazione, la selezione dispositivi o i dispositivi a cui si applica l'attività.
7. Nel passaggio **Completa creazione attività**, se si abilita l'opzione **Apri i dettagli dell'attività al termine della creazione**, è possibile modificare le impostazioni predefinite dell'attività. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
8. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
9. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.
10. Nella scheda **Impostazioni applicazione** della finestra delle proprietà dell'attività definire le impostazioni dell'attività di aggiornamento in modalità locale o mobile:

    - **Modalità locale**: le impostazioni in questa scheda definiscono il modo in cui il dispositivo riceve gli aggiornamenti quando viene stabilita la connessione tra il dispositivo e l'Administration Server.
    - **Modalità mobile**: le impostazioni in questa scheda definiscono il modo in cui il dispositivo riceve gli aggiornamenti quando non viene stabilita alcuna connessione tra Kaspersky Security Center Cloud Console e il dispositivo (ad esempio quando il dispositivo non è connesso a Internet).
11. Abilitare le sorgenti aggiornamenti che si desidera utilizzare per aggiornare i database e i moduli dell'applicazione per Kaspersky Endpoint Security for Windows. Se necessario, modificare le posizioni delle sorgenti nell'elenco utilizzando i pulsanti **Sposta su** e **Sposta giù**. Se sono abilitate diverse sorgenti aggiornamenti, Kaspersky Endpoint Security for Windows tenta di connettersi a tali sorgenti una dopo l'altra, a partire a quella all'inizio dell'elenco, ed esegue l'attività di aggiornamento recuperando il pacchetto di aggiornamento dalla prima sorgente disponibile.

Quando Kaspersky Security Center Cloud Console è impostato come sorgente aggiornamenti, gli aggiornamenti vengono scaricati da un archivio del punto di distribuzione, non dall'archivio dell'Administration Server. Assicurarsi di aver assegnato i punti di distribuzione e creato l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

12. Abilitare l'opzione **Installa gli aggiornamenti approvati del modulo delle applicazioni** per scaricare e installare gli aggiornamenti dei moduli software oltre ai database dell'applicazione.

    Se l'opzione è abilitata, Kaspersky Endpoint Security for Windows invia una notifica all'utente per informarlo degli aggiornamenti dei moduli software disponibili e include gli aggiornamenti dei moduli software nel pacchetto di aggiornamento durante l'esecuzione dell'attività di aggiornamento. Kaspersky Endpoint Security for Windows installa solo gli aggiornamenti per cui è stato impostato lo stato *Approvato*. Verranno installati in locale tramite l'interfaccia dell'applicazione o tramite Kaspersky Security Center Cloud Console.

    È inoltre possibile abilitare l'opzione **Installa automaticamente gli aggiornamenti critici del modulo delle applicazioni**. Se sono disponibili aggiornamenti per i moduli software, Kaspersky Endpoint Security for Windows li installa automaticamente con lo stato *Critico*. Gli aggiornamenti rimanenti saranno installati dopo essere stati approvati dall'amministratore.

    Se l'aggiornamento dei moduli software richiede la visualizzazione e l'accettazione delle condizioni del Contratto di licenza e dell'Informativa sulla privacy, l'applicazione installa gli aggiornamenti dopo che le condizioni del Contratto di licenza e dell'Informativa sulla privacy sono state accettate dall'utente.

13. Selezionare la casella di controllo **Copia aggiornamenti nella cartella** per fare in modo che gli aggiornamenti scaricati vengano salvati in una cartella, quindi specificare il percorso della cartella.

14. Pianificare l'attività. Per garantire aggiornamenti tempestivi, è consigliabile selezionare l'opzione **Quando vengono scaricati nuovi aggiornamenti nell'archivio**.

15. Fare clic su **Salva**.

Quando è in esecuzione l'attività **Aggiornamento**, l'applicazione invia richieste ai server di aggiornamento Kaspersky.

Alcuni aggiornamenti richiedono l'installazione delle versioni più recenti dei plug-in di gestione.

Informazioni sugli stati degli aggiornamenti

Stato è un attributo degli aggiornamenti software che definisce se un determinato aggiornamento software deve essere installato in un dispositivo della rete.

Un aggiornamento può avere i seguenti stati:

- *Indefinito*

  Per impostazione predefinita, gli aggiornamenti software scaricati hanno lo stato *Indefinito*. Gli aggiornamenti indefiniti possono essere installati solo in Network Agent e negli altri componenti di Kaspersky Security Center Cloud Console in conformità con le impostazioni del criterio di Network Agent.

- *Approvato*

Gli aggiornamenti approvati vengono sempre installati. Se un aggiornamento richiede la visualizzazione e l'accettazione dei termini del Contratto di licenza con l'utente finale, è prima necessario accettare i termini.

- *Rifiutato*

  Gli aggiornamenti per cui è stato impostato lo stato *Rifiutato* non verranno installati nei dispositivi.

È possibile modificare gli stati degli aggiornamenti per il seguente software:

- Network Agent e altri componenti Kaspersky Security Center Cloud Console

  Per impostazione predefinita, gli aggiornamenti scaricati e le patch scaricate per i componenti di Kaspersky Security Center Cloud Console vengono installati automaticamente. Se l'opzione **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito** è stata mantenuta abilitata nelle proprietà di Network Agent, tutti gli aggiornamenti verranno installati automaticamente dopo essere stati scaricati nell'archivio (o in diversi archivi). Se questa opzione è disabilitata, le patch di Kaspersky che sono state scaricate e contrassegnate con lo stato *Indefinito* saranno installate solo dopo che si modifica il relativo stato in *Approvato*.

  Gli aggiornamenti per i componenti di Kaspersky Security Center Cloud Console non possono essere disinstallati, anche se si imposta lo stato *Rifiutato* per un aggiornamento.

- Applicazioni di protezione Kaspersky

  Per impostazione predefinita, gli aggiornamenti per le applicazioni gestite vengono installati solo dopo aver modificato lo stato dell'aggiornamento in *Approvato*. Se in precedenza era stato installato un aggiornamento rifiutato per un'applicazione di protezione, Kaspersky Security Center Cloud Console tenterà di disinstallare l'aggiornamento da tutti i dispositivi.

Approvazione e rifiuto degli aggiornamenti software

Le impostazioni di un'attività di installazione degli aggiornamenti possono richiedere l'approvazione degli aggiornamenti da installare. È possibile approvare gli aggiornamenti da installare e rifiutare quelli che non devono essere installati.

Ad esempio, potrebbe essere utile controllare prima l'installazione degli aggiornamenti in un ambiente di test e verificare che non interferiscano con l'utilizzo dei dispositivi e solo successivamente consentire l'installazione degli aggiornamenti nei dispositivi client.

Per approvare o rifiutare uno o più aggiornamenti:

1. Nel menu principale, passare a **Operazioni** → **Applicazioni Kaspersky** → **Aggiornamenti immediati**.

   Verrà visualizzato un elenco degli aggiornamenti disponibili.

   > Gli aggiornamenti delle applicazioni gestite potrebbero richiedere l'installazione di una versione minima specifica di Kaspersky Security Center. Se questa versione è successiva alla versione corrente, gli aggiornamenti vengono visualizzati ma non possono essere approvati. Inoltre, nessun pacchetto di installazione può essere creato da tali aggiornamenti finché non si esegue l'upgrade di Kaspersky Security Center. Viene richiesto di eseguire l'upgrade dell'istanza di Kaspersky Security Center alla versione minima richiesta.

2. Selezionare gli aggiornamenti che si desidera accettare o rifiutare.

3. Fare clic su **Approva** per approvare gli aggiornamenti selezionati o su **Rifiuta** per rifiutare gli aggiornamenti selezionati.

Il valore predefinito è *Indefinito*.

Gli aggiornamenti a cui è assegnato lo stato *Approvato* verranno inseriti in una coda per l'installazione.

Gli aggiornamenti a cui è assegnato lo stato *Rifiutato* verranno disinstallati (se possibile) da tutti i dispositivi in cui erano installati in precedenza. Inoltre, non verranno installati in altri dispositivi in futuro.

Alcuni aggiornamenti per le applicazioni Kaspersky non possono essere disinstallati. Se si imposta lo stato *Rifiutato* per tali aggiornamenti, Kaspersky Security Center Cloud Console non li disinstallerà dai dispositivi in cui erano installati in precedenza. Tuttavia, tali aggiornamenti non verranno installati in altri dispositivi in futuro.

Se si imposta lo stato *Rifiutato* per gli aggiornamenti software di terze parti, tali aggiornamenti non verranno installati nei dispositivi in cui l'installazione era stata pianificata ma non ancora eseguita. Gli aggiornamenti rimarranno nei dispositivi in cui erano già installati. Se è necessario eliminare gli aggiornamenti, è possibile eliminarli manualmente in locale.

Utilizzo dei file diff per l'aggiornamento dei database e dei moduli del software Kaspersky

Un file diff descrive le differenze tra due versioni di un file di un database o un modulo software. L'utilizzo dei file diff limita il traffico nella rete aziendale, poiché i file diff occupano meno spazio rispetto ai file completi di database e moduli software. Se è abilitata la funzionalità *Download dei file diff* in un punto di distribuzione, i file diff vengono salvati in questo punto di distribuzione. Come risultato, i dispositivi che recuperano gli aggiornamenti da questo punto di distribuzione possono utilizzare i file diff salvati per l'aggiornamento dei database e dei moduli software.

Per ottimizzare l'utilizzo dei file diff, è consigliabile sincronizzare la pianificazione di aggiornamento dei dispositivi con la pianificazione di aggiornamento del punto di distribuzione da cui i dispositivi recuperano gli aggiornamenti. Il traffico può comunque essere ridotto anche se i dispositivi vengono aggiornati con una frequenza notevolmente inferiore a quella del punto di distribuzione da cui i dispositivi recuperano gli aggiornamenti.

I punti di distribuzione non utilizzano la modalità IP multicast per la distribuzione automatica dei file diff.

Per abilitare la funzionalità Download dei file diff:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sull'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per aprire le proprietà dell'attività.
3. Nella scheda **Impostazioni applicazione**, abilitare l'opzione **Scarica file diff**.
4. Fare clic sul pulsante **Salva**.

La funzionalità Download dei file diff è abilitata. I file diff degli aggiornamenti verranno scaricati in aggiunta ai file di aggiornamento ogni volta che viene eseguita l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

Per verificare che la funzionalità Download dei file diff sia abilitata correttamente, è possibile misurare il traffico interno prima e dopo l'esecuzione dello scenario.

Aggiornamento dei database e dei moduli software Kaspersky nei dispositivi offline

L'aggiornamento dei database e dei moduli software Kaspersky nei dispositivi gestiti è un'attività importante per mantenere la protezione dei dispositivi da virus e altre minacce. Gli amministratori in genere configurano aggiornamenti periodici tramite gli archivi dei punti di distribuzione.

Quando è necessario aggiornare i database e i moduli software in un dispositivo (o un gruppo di dispositivi) che non è connesso a un punto di distribuzione o a Internet, è necessario utilizzare sorgenti degli aggiornamenti alternative, come un server FTP o una cartella locale. In questo caso, è necessario distribuire i file degli aggiornamenti richiesti utilizzando un dispositivo di archiviazione di massa, come un'unità flash o un disco rigido esterno.

È possibile copiare gli aggiornamenti richiesti dalle seguenti origini:

- Punto di distribuzione.

  Per essere certi che l'archivio del punto di distribuzione contenga gli aggiornamenti richiesti per l'applicazione di protezione installata in un dispositivo offline, in almeno uno dei dispositivi online gestiti nell'ambito del punto di distribuzione deve essere installata la stessa applicazione di protezione. Questa applicazione deve essere configurata per ricevere gli aggiornamenti dall'archivio del punto di distribuzione tramite l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

- Qualsiasi dispositivo in cui sia installata e configurata la stessa applicazione di protezione per la ricezione degli aggiornamenti dall'archivio di un punto di distribuzione o direttamente dai server di aggiornamento Kaspersky.

Di seguito è riportato un esempio di configurazione degli aggiornamenti dei database e dei moduli software copiandoli dall'archivio di un punto di distribuzione.

Per aggiornare i database e i moduli software Kaspersky nei dispositivi offline:

1. Collegare l'unità rimovibile al dispositivo del punto di distribuzione.

2. Copiare i file degli aggiornamenti nell'unità rimovibile.

   Per impostazione predefinita, gli aggiornamenti si trovano in: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\Updates.

3. Nei dispositivi offline configurare l'applicazione di protezione (ad esempio, Kaspersky Endpoint Security for Windows) per la ricezione degli aggiornamenti da una cartella locale o una risorsa condivisa, come un server FTP o una cartella condivisa.

4. Copiare i file degli aggiornamenti dall'unità rimovibile nella cartella locale o nella risorsa condivisa che si desidera utilizzare come sorgente aggiornamenti.

5. Nel dispositivo offline che richiede l'installazione degli aggiornamenti avviare l'attività di aggiornamento di Kaspersky Endpoint Security for Windows.

Al termine dell'attività di aggiornamento, i database e i moduli software Kaspersky sono aggiornati nel dispositivo.

Aggiornamento dei database di Kaspersky Security for Windows Server

È possibile installare Kaspersky Security for Windows Server nei dispositivi gestiti ed è consigliabile avviare l'attività Protezione in tempo reale di questa applicazione. Tuttavia, l'applicazione viene fornita senza i database necessari per il corretto funzionamento. I database vengono scaricati nel dispositivo gestito solo dopo il completamento dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

Se si desidera avviare l'attività Protezione in tempo reale in un dispositivo gestito subito dopo l'installazione di Kaspersky Security for Windows Server, è necessario assicurarsi che i database per tale applicazione siano stati scaricati e aggiornati. In caso contrario, l'attività potrebbe non funzionare correttamente.

Per assicurarsi che i database di Kaspersky Security for Windows Server siano aggiornati:

1. Verificare che l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* sia stata completata in Administration Server.

2. Eseguire una delle seguenti operazioni:

   - Nelle impostazioni dell'attività Protezione in tempo reale impostare l'avvio su *All'avvio dell'applicazione*, quindi riavviare il dispositivo gestito.

   - Nelle impostazioni dell'attività Protezione in tempo reale impostare manualmente l'ora di inizio sull'ora desiderata.

L'attività Protezione in tempo reale in Kaspersky Security for Windows Server è pronta per il corretto funzionamento.

Gestione delle applicazioni di terzi nei dispositivi client

Questa sezione descrive le funzionalità di Kaspersky Security Center Cloud Console correlate alla gestione delle applicazioni di terze parti installate nei dispositivi client.

Informazioni sulle applicazioni di terze parti

Kaspersky Security Center Cloud Console può aiutare ad aggiornare il software di terze parti installato nei dispositivi client e a correggere le vulnerabilità del software di terze parti. Kaspersky Security Center Cloud Console può aggiornare il software di terze parti solo dalla versione corrente alla versione più recente. L'elenco di seguito illustra il software di terze parti che è possibile aggiornare con Kaspersky Security Center Cloud Console:

L'elenco del software di terze parti può essere aggiornato ed esteso con nuove applicazioni. È possibile verificare se il software di terze parti (installato nei dispositivi degli utenti) può essere aggiornato con Kaspersky Security Center Cloud Console visualizzando l'elenco degli aggiornamenti disponibili in Kaspersky Security Center Cloud Console.

- 7-Zip Developers: 7-Zip
- Adobe Systems:
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC
  - Adobe Acrobat
  - Adobe Reader
  - Adobe Shockare Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander
- Apache Software Foundation: Apache Tomcat
- Apple:
  - Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.: Armory
- Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber
- Code Sector: TeraCopy

- Codec Guide:
  - K-Lite Codec Pack Basic
  - K-Lite Codec Pack Full
  - K-Lite Codec Pack Mega
  - K-Lite Codec Pack Standard
- DbVis Software AB: DbVisualizer
- Decho Corp.:
  - Mozy Enterprise
  - Mozy Home
  - Mozy Pro
- Dominik Reichl: KeePass Password Safe
- Don HO don.h@free.fr: Notepad++
- DoubleGIS: 2GIS
- Dropbox, Inc.: Dropbox
- EaseUs: EaseUS Todo Backup Free
- Electrum Technologies GmbH: Electrum
- Enter Srl: Iperius Backup
- Eric Lawrence: Fiddler
- EverNote: EverNote
- Exodus Movement Inc: Exodus
- EZB Systems: UltraISO
- Famatech:
  - Radmin
  - Remote Administrator
- Far Manager: FAR Manager
- FastStone Soft: FastStone Image Viewer
- FileZilla Project: FileZilla
- Firebird Developers: Firebird

- Foxit Corporation:
  - Foxit Reader
  - Foxit Reader Enterprise
- Free Download Manager.ORG: Free Download Manager
- GIMP project: GIMP
- GlavSoft LLC.: TightVNC
- GNU Project: Gpg4win
- Google:
  - Google Earth
  - Google Chrome
  - Google Chrome Enterprise
  - Google Earth Pro
- Inkscape Project: Inkscape
- IrfanView: IrfanView
- iterate GmbH: Cyberduck
- Logitech: SetPoint
- LogMeIn, Inc.:
  - LogMeIn
  - Hamachi
  - LogMeIn Rescue Technician Console
- Martin Prikryl: WinSCP
- Mozilla Foundation:
  - Mozilla Firefox
  - Mozilla Firefox ESR
  - Mozilla SeaMonkey
  - Mozilla Thunderbird
- New Cloud Technologies Ltd: MyOffice Standard. Home Edition
- OpenOffice.org: OpenOffice

- Opera Software: Opera
- Oracle Corporation:
  - Oracle Java JRE
  - Oracle VirtualBox
- PDF44: PDF24 MSI/EXE
- Piriform:
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql: PostgreSQL
- RealNetworks: RealPlayer Cloud
- RealVNC:
  - RealVNC Server
  - RealVNC Viewer
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Complete/Minimum)
- Simon Tatham: PuTTY
- Skype Technologies: Skype for Windows
- Sober Lemur S.a.s:
  - PDFsam Basic
  - PDFsam Visual
- Softland: FBackup
- Splashtop Inc.: Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP
- Sublime HQ Pty Ltd: Sublime Text
- TeamViewer GmbH:
  - TeamViewer Host
  - TeamViewer

- Telegram Messenger LLP: Telegram Desktop
- The Document Foundation:
  - LibreOffice
  - LibreOffice HelpPack
- The Git Development Community:
  - Git for Windows
  - Git LFS
- The Pidgin developer community: Pidgin
- TortoiseSVN Developers: TortoiseSVN
- VideoLAN: VLC media player
- VMware:
  - VMware Player
  - VMware Workstation
- WinRAR Developers: WinRAR
- WinZip: WinZip
- Wireshark Foundation: Wireshark
- Wrike: Wrike
- Zimbra: Zimbra Desktop

Limitazioni di Vulnerability e patch management

La funzionalità Vulnerability e patch management presenta una serie di limitazioni, a seconda della licenza utilizzata e della modalità di esecuzione di Kaspersky Security Center Cloud Console.

La funzionalità Vulnerability e patch management non è supportata dalle seguenti licenze:

- Kaspersky Endpoint Security for Business Select
- Kaspersky Hybrid Cloud Security

La funzionalità Vulnerability e patch management è supportata dalle seguenti licenze:

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Detection and Response Optimum

- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security Enterprise

Nella tabella seguente vengono confrontate le limitazioni di Kaspersky Security Center Cloud Console in modalità di prova, con licenze che non supportano Vulnerability e patch management e con licenze che supportano Vulnerability e patch management.

Limitazioni di Vulnerability e patch management

Limitazione	Modalità di prova	Modalità commerciale: licenze che non supportano Vulnerability e patch management	Modalità commerciale: licenze che supportano Vulnerability e Patch Management
Numero massimo di attività *Installa aggiornamenti di Windows Update* o di attività *Correggi vulnerabilità*	4	4	0 (non è possibile creare nuove attività di queste tipologie)
Numero massimo di attività *Installa aggiornamenti richiesti e correggi vulnerabilità*	2	Non supportato	4
Numero massimo di regole in tutte le attività *Installa aggiornamenti richiesti e correggi vulnerabilità*	10	Non supportato	50
Numero massimo di aggiornamenti software che possono avere contemporaneamente lo stato *Approvato*	100	Non supportato	1000
Numero massimo di aggiornamenti software che possono essere aggiunti manualmente a un'attività	500	1000	1000
Numero massimo di vulnerabilità del software che possono essere aggiunte manualmente a un'attività	500	1000	1000

Disponibilità delle funzionalità di Vulnerability e patch management in modalità di prova e commerciale e con varie opzioni di licenza

La disponibilità delle funzionalità di Vulnerability e patch management in Kaspersky Security Center Cloud Console dipende dall'utilizzo in modalità di prova o commerciale, nonché dall'opzione di licenza selezionata. Utilizzare la tabella per verificare quali funzionalità di Vulnerability e patch management sono disponibili.

Disponibilità delle funzionalità di Vulnerability e patch management

Funzionalità Vulnerability e patch management	Modalità di prova	Modalità commerciale: Kaspersky Endpoint Security for Business Select	Modalità Kaspersky Endpoint Secu Kaspersky Endpoint Detec Kaspersky Total S
Correzione manuale delle vulnerabilità nel software	✓	✓	

Microsoft nei dispositivi gestiti che eseguono Windows Creazione dell'attività *Correggi vulnerabilità*			
Installazione manuale degli aggiornamenti nel software Microsoft nei dispositivi gestiti che eseguono Windows Installazione di aggiornamenti software di terze parti tramite l'attività *Installa aggiornamenti di Windows Update*	–	✓	
Installazione automatica di aggiornamenti software di terze parti basata sulle regole e correzione delle vulnerabilità del software di terze parti Creazione dell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* e installazione degli aggiornamenti Aggiunta delle regole per l'installazione dell'aggiornamento	✓	–	

Installazione degli aggiornamenti software di terze parti

Questa sezione descrive le funzionalità di Kaspersky Security Center Cloud Console correlate all'installazione di aggiornamenti per le applicazioni di terze parti installate nei dispositivi client.

Scenario: Aggiornamento di software di terze parti

Questa sezione fornisce uno scenario per l'aggiornamento del software di terze parti installato nei dispositivi client. Il software di terze parti include le applicazioni Microsoft e di altri fornitori di software. Gli aggiornamenti per le applicazioni Microsoft sono forniti dal servizio Windows Update.

Passaggi

L'aggiornamento del software di terze parti prevede diversi passaggi:

1. **Ricerca degli aggiornamenti richiesti**

   Per trovare gli aggiornamenti software di terze parti richiesti per i dispositivi gestiti, eseguire l'attività *Trova vulnerabilità e aggiornamenti richiesti*. Al termine di questa attività, Kaspersky Security Center Cloud Console riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi specificati nelle proprietà dell'attività.

   L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Se non è stata eseguita la procedura guidata, creare l'attività o eseguire l'Avvio rapido guidato.

   Istruzioni dettagliate:

   - Creazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
   - Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

2. **Analisi dell'elenco degli aggiornamenti rilevati**

   Visualizzare l'elenco **Aggiornamenti software** e decidere quali aggiornamenti si desidera installare. Per visualizzare informazioni dettagliate su ciascun aggiornamento, fare clic sul nome dell'aggiornamento nell'elenco. Per ogni aggiornamento nell'elenco, è possibile visualizzare le statistiche sull'installazione dell'aggiornamento nei dispositivi gestiti. È ad esempio possibile visualizzare il numero di dispositivi in cui l'aggiornamento selezionato non è installato, verrà installato o in cui l'installazione dell'aggiornamento non è andata a buon fine.

   Istruzioni dettagliate: Visualizzazione delle informazioni sugli aggiornamenti software di terze parti disponibili

3. **Configurazione dell'installazione degli aggiornamenti**

   Quando Kaspersky Security Center Cloud Console ha ricevuto l'elenco degli aggiornamenti software di terze parti, è possibile installarli nei dispositivi client utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Installa aggiornamenti di Windows Update*. Creare una di queste attività. È possibile creare queste attività nella scheda **Attività** o utilizzando l'elenco **Aggiornamenti software**.

   L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per installare gli aggiornamenti per le applicazioni Microsoft, inclusi gli aggiornamenti forniti dal servizio Windows Update, e gli aggiornamenti dei prodotti di altri produttori.

   L'attività *Installa aggiornamenti di Windows Update* può essere utilizzata per installare solo gli aggiornamenti di Windows Update.

   Le attività di installazione degli aggiornamenti software prevedono una serie di limitazioni. Queste limitazioni dipendono dalla licenza con cui si utilizza Kaspersky Security Center Cloud Console e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

   Per installare alcuni aggiornamenti software, è necessario accettare il Contratto di licenza con l'utente finale (EULA) per il software da installare. Se non si accetta il Contratto di licenza con l'utente finale, l'aggiornamento software non verrà installato.

   Istruzioni dettagliate:

- Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità
- Creazione dell'attività Installa aggiornamenti di Windows Update
- Visualizzazione delle informazioni sugli aggiornamenti software di terze parti disponibili

4. **Pianificazione delle attività**

   Per assicurarsi che l'elenco degli aggiornamenti sia sempre aggiornato, pianificare l'attività *Trova vulnerabilità e aggiornamenti richiesti* affinché venga eseguita periodicamente in modo automatico. La frequenza predefinita è una volta alla settimana.

   Se è stata creata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile pianificarla in modo che venga eseguita con la stessa frequenza dell'attività *Trova vulnerabilità e aggiornamenti richiesti* o con una frequenza inferiore. Quando si pianifica l'attività *Installa aggiornamenti di Windows Update*, tenere presente che per questa attività è necessario definire l'elenco degli aggiornamenti ogni volta prima di avviare l'attività.

   Quando si pianificano le attività, assicurarsi che al termine dell'attività *Trova vulnerabilità e aggiornamenti richiesti* venga avviata un'attività per correggere la vulnerabilità.

   Istruzioni dettagliate: Impostazioni generali delle attività

5. **Approvazione e rifiuto degli aggiornamenti software (facoltativo)**

   Se è stata creata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile specificare le regole per l'installazione degli aggiornamenti nelle proprietà dell'attività. Se è stata creata l'attività *Installa aggiornamenti di Windows Update*, ignorare questo passaggio.

   Per ciascuna regola, è possibile definire gli aggiornamenti da installare in base allo stato dell'aggiornamento: *Indefinito*, *Approvato* o *Rifiutato*. Ad esempio, è possibile creare un'attività specifica per i server e impostare una regola per questa attività in modo da consentire l'installazione solo degli aggiornamenti di Windows Update e solo di quelli con stato *Approvato*. Successivamente, si imposta manualmente lo stato *Approvato* per gli aggiornamenti da installare. In questo caso, gli aggiornamenti di Windows Update con stato *Indefinito* o *Rifiutato* non verranno installati nei server specificati nell'attività.

   Per impostazione predefinita, gli aggiornamenti software scaricati hanno lo stato *Indefinito*. È possibile modificare lo stato in *Approvato* o *Rifiutato* nell'elenco **Aggiornamenti software** (**Operazioni** → **Gestione patch** → **Aggiornamenti software**).

   Istruzioni dettagliate: Approvazione e rifiuto degli aggiornamenti software di terze parti

6. **Esecuzione di un'attività di installazione degli aggiornamenti**

   Avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Installa aggiornamenti di Windows Update*. Quando si avviano queste attività, gli aggiornamenti vengono scaricati e installati nei dispositivi gestiti. Al termine dell'attività, assicurarsi che questa abbia lo stato *Completato* nell'elenco attività.

   Istruzioni dettagliate: Avvio manuale di un'attività

7. **Creare il rapporto sui risultati dell'installazione degli aggiornamenti del software di terze parti (facoltativo)**

   Per assicurarsi che l'attività venga creata e che gli aggiornamenti vengano installati, creare il **Rapporto sui risultati dell'installazione degli aggiornamenti software di terze parti** e visualizzare statistiche dettagliate sull'installazione degli aggiornamenti in questo rapporto.

   Istruzioni dettagliate: Generazione e visualizzazione di un rapporto

Informazioni sugli aggiornamenti software di terze parti

Kaspersky Security Center Cloud Console consente di gestire gli aggiornamenti del software di terze parti installato nei dispositivi gestiti e di correggere le vulnerabilità delle applicazioni Microsoft e di altri produttori di software tramite l'installazione degli aggiornamenti richiesti.

Kaspersky Security Center Cloud Console cerca gli aggiornamenti tramite l'attività *Trova vulnerabilità e aggiornamenti richiesti*. Al termine di questa attività, Administration Server riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi specificati nelle proprietà dell'attività. Dopo avere visualizzato le informazioni sugli aggiornamenti disponibili, è possibile installarli nei dispositivi.

Kaspersky Security Center Cloud Console aggiorna alcune applicazioni rimuovendo la versione precedente dell'applicazione e installando la nuova.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Per motivi di sicurezza, tutti gli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management vengono automaticamente analizzati alla ricerca di malware dalle tecnologie Kaspersky. Queste tecnologie vengono utilizzate per il controllo automatico dei file e includono la scansione virus, l'analisi statica, l'analisi dinamica, l'analisi del comportamento nell'ambiente sandbox e il machine learning.

Gli esperti Kaspersky non eseguono l'analisi manuale degli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management. Inoltre, gli esperti di Kaspersky non ricercano vulnerabilità (note o sconosciute) o funzionalità non documentate in tali aggiornamenti, né eseguono altri tipi di analisi degli aggiornamenti diversi da quelli specificati nel paragrafo precedente.

Attività per l'installazione degli aggiornamenti software di terze parti

Quando i metadati degli aggiornamenti software di terze parti vengono scaricati nell'archivio, è possibile installare gli aggiornamenti nei dispositivi client utilizzando le seguenti attività:

- L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*

  Questa attività viene utilizzata per installare gli aggiornamenti per le applicazioni Microsoft, inclusi gli aggiornamenti forniti dal servizio Windows Update, e gli aggiornamenti dei prodotti di altri produttori.

  Al termine di questa attività, gli aggiornamenti vengono installati automaticamente nei dispositivi gestiti. Quando i metadati dei nuovi aggiornamenti vengono scaricati nell'archivio dell'Administration Server, Kaspersky Security Center Cloud Console verifica se gli aggiornamenti soddisfano i criteri specificati nelle regole per gli aggiornamenti. Tutti i nuovi aggiornamenti che soddisfano i criteri verranno scaricati e installati automaticamente alla successiva esecuzione dell'attività.

- L'attività *Installa aggiornamenti di Windows Update*

  Questa attività può essere utilizzata per installare solo gli aggiornamenti di Windows Update.

  Al termine di questa attività, vengono installati solo gli aggiornamenti specificati nelle proprietà dell'attività. Se in seguito si desidera installare i nuovi aggiornamenti, è necessario aggiungere gli aggiornamenti richiesti all'elenco degli aggiornamenti nell'attività esistente o creare un'attività *Installa aggiornamenti di Windows Update*.

Le attività di installazione degli aggiornamenti software prevedono una serie di limitazioni. Queste limitazioni dipendono dalla licenza con cui si utilizza Kaspersky Security Center Cloud Console e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

Installazione degli aggiornamenti software di terze parti

È possibile installare gli aggiornamenti software di terze parti nei dispositivi gestiti creando ed eseguendo una delle seguenti attività:

- *Installa aggiornamenti richiesti e correggi vulnerabilità*

  È possibile utilizzare questa attività per installare sia gli aggiornamenti di Windows Update forniti da Microsoft sia gli aggiornamenti dei prodotti di altri fornitori.

- *Installa aggiornamenti di Windows Update*

  È possibile utilizzare questa attività solo per installare gli aggiornamenti di Windows Update.

Le attività di installazione degli aggiornamenti software prevedono una serie di limitazioni. Queste limitazioni dipendono dalla licenza con cui si utilizza Kaspersky Security Center Cloud Console e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Facoltativamente, è possibile creare un'attività per installare gli aggiornamenti richiesti nei seguenti modi:

- Aprendo l'elenco degli aggiornamenti e specificando quali aggiornamenti installare.

  Verrà creata una nuova attività per l'installazione degli aggiornamenti selezionati. Facoltativamente è possibile aggiungere gli aggiornamenti selezionati a un'attività esistente.

- Eseguendo l'Installazione guidata aggiornamenti.

  La disponibilità dell'Installazione guidata aggiornamenti dipende dalla modalità di Kaspersky Security Center Cloud Console e dalla licenza corrente.

  La procedura guidata semplifica la creazione e la configurazione di un'attività di installazione degli aggiornamenti e consente di eliminare la creazione di attività ridondanti che contengono gli stessi aggiornamenti da installare.

Installazione degli aggiornamenti software di terze parti tramite l'elenco degli aggiornamenti

Per installare aggiornamenti software di terze parti utilizzando l'elenco degli aggiornamenti:

1. Aprire uno degli elenchi di aggiornamenti:

   - Per aprire l'elenco generale degli aggiornamenti nel menu principale, passare a **Operazioni** → **Gestione patch** → **Aggiornamenti software**.

   - Per aprire l'elenco degli aggiornamenti per un dispositivo gestito nel menu principale, passare a **Risorse (dispositivi)** → **Dispositivi gestiti** → **<nome dispositivo>** → **Avanzate** → **Aggiornamenti disponibili**.

   - Per aprire l'elenco degli aggiornamenti per un'applicazione specifica nel menu principale, passare a **Operazioni** → **Applicazioni di terze parti** → **Registro delle applicazioni** → **<nome applicazione>** →

Aggiornamenti disponibili.

Verrà visualizzato un elenco degli aggiornamenti disponibili.

2. Selezionare le caselle di controllo accanto agli aggiornamenti che si desidera installare.

3. Fare clic sul pulsante **Installa aggiornamenti**.

   Per installare alcuni aggiornamenti software, è necessario accettare il Contratto di licenza con l'utente finale (EULA). Se non si accetta il Contratto di licenza con l'utente finale, l'aggiornamento software non verrà installato.

4. Selezionare una delle seguenti opzioni:

   - **Nuova attività**

     Verrà avviata la Creazione guidata nuova attività. L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Installa aggiornamenti di Windows Update* è preselezionata, a seconda della modalità di Kaspersky Security Center Cloud Console e della licenza corrente. Seguire i passaggi della procedura guidata per completare la creazione dell'attività.

   - **Installa aggiornamento (aggiungi regola all'attività specificata)**

     Selezionare un'attività a cui aggiungere gli aggiornamenti selezionati. Selezionare un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o un'attività *Installa aggiornamenti di Windows Update*. Se si seleziona un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, una nuova regola per installare gli aggiornamenti selezionati verrà automaticamente aggiunta all'attività selezionata. Se si seleziona un'attività *Installa aggiornamenti di Windows Update*, gli aggiornamenti selezionati verranno aggiunti alle proprietà dell'attività.

     Verrà visualizzata la finestra delle proprietà dell'attività. Fare clic sul pulsante **Salva** per applicare le modifiche.

   Se si è scelto di creare un'attività, l'attività viene creata e visualizzata nell'elenco delle attività in **Risorse (dispositivi)** → **Attività**. Se si è scelto di aggiungere gli aggiornamenti a un'attività esistente, gli aggiornamenti vengono salvati nelle proprietà dell'attività.

Per installare gli aggiornamenti software di terze parti, avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Installa aggiornamenti di Windows Update*. È possibile avviare queste attività manualmente o specificare le impostazioni di pianificazione nelle proprietà dell'attività avviata. Quando si specifica la pianificazione dell'attività, assicurarsi che l'attività di installazione degli aggiornamenti venga avviata dopo il completamento dell'attività *Trova vulnerabilità e aggiornamenti richiesti*.

Installazione degli aggiornamenti software di terze parti tramite l'Installazione guidata aggiornamenti

La disponibilità di questa funzionalità dipende dalla modalità di Kaspersky Security Center Cloud Console e dalla licenza corrente.

Per creare un'attività per l'installazione degli aggiornamenti software di terze parti utilizzando l'Installazione guidata aggiornamenti:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Aggiornamenti software**.

   Verrà visualizzato un elenco degli aggiornamenti disponibili.

2. Selezionare la casella di controllo accanto all'aggiornamento che si desidera installare.

3. Fare clic sul pulsante **Esegui Installazione guidata aggiornamenti**.

   Verrà avviata l'Installazione guidata aggiornamenti. La pagina **Selezionare un'attività per l'installazione dell'aggiornamento** mostra l'elenco di tutte le attività esistenti dei seguenti tipi:

   - *Installa aggiornamenti richiesti e correggi vulnerabilità*
   - *Installa aggiornamenti di Windows Update*
   - *Correggi vulnerabilità*

   Non è possibile modificare le attività degli ultimi due tipi per installare nuovi aggiornamenti. Per installare nuovi aggiornamenti, è possibile utilizzare solo le attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.

4. Se si desidera che la procedura guidata visualizzi solo le attività per l'installazione dell'aggiornamento selezionato, abilitare l'opzione **Mostra solo le attività che consentono di installare l'aggiornamento**.

5. Scegliere l'operazione da eseguire:

   - Per avviare un'attività, selezionare la casella di controllo accanto al nome dell'attività, quindi fare clic sul pulsante **Avvia**.
   - Per aggiungere una nuova regola a un'attività esistente:

     a. Selezionare la casella di controllo accanto al nome dell'attività, quindi fare clic sul pulsante **Aggiungi regola**.

     b. Nella pagina visualizzata configurare la nuova regola:

     - Regola di installazione per gli aggiornamenti di questo livello di importanza

       Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

       Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore alla criticità dell'aggiornamento selezionato (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

       Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

       Per impostazione predefinita, questa opzione è disabilitata.

     - Regola di installazione per gli aggiornamenti di questo livello di importanza in base a MSRC (disponibile solo per gli aggiornamenti di Windows Update)

Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

Se questa opzione è abilitata (disponibile solo per gli aggiornamenti di Windows Update), gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Microsoft Security Response Center (MSRC) è uguale o superiore al valore selezionato nell'elenco (**Basso**, **Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

Per impostazione predefinita, questa opzione è disabilitata.

- Regola di installazione per gli aggiornamenti in base a questo produttore (disponibile solo per gli aggiornamenti di applicazioni di terze parti)

  Questa opzione è disponibile solo per gli aggiornamenti di applicazioni di terze parti. Kaspersky Security Center Cloud Console installa solo gli aggiornamenti relativi alle applicazioni sviluppate dallo stesso produttore dell'aggiornamento selezionato. Gli aggiornamenti rifiutati e gli aggiornamenti per le applicazioni sviluppate da altri produttori non vengono installati.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Regola di installazione per gli aggiornamenti del tipo**
- **Regola di installazione per l'aggiornamento selezionato**
- Approvare gli aggiornamenti selezionati

  L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

  Per impostazione predefinita, questa opzione è disabilitata.

- Installa automaticamente tutti gli aggiornamenti precedenti dell'applicazione necessari per l'installazione degli aggiornamenti selezionati

  Mantenere abilitata questa opzione se si desidera consentire l'installazione delle versioni intermedie delle applicazioni quando questa operazione è necessaria per l'installazione degli aggiornamenti selezionati.

  Se questa opzione è disabilitata, vengono installate solo le versioni delle applicazioni selezionate. Disabilitare questa opzione se si desidera aggiornare le applicazioni in modo diretto, senza tentare di installare le versioni successive in modo incrementale. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

  Si supponga di avere la versione 3 di un'applicazione installata in un dispositivo e di voler eseguire l'aggiornamento alla versione 5, ma la versione 5 di questa applicazione può essere installata solo sulla versione 4. Se questa opzione è abilitata, il software installa prima la versione 4 e quindi la versione 5. Se questa opzione è disabilitata, il software non riesce a eseguire l'aggiornamento l'applicazione.

  Per impostazione predefinita, questa opzione è abilitata.

c. Fare clic sul pulsante **Aggiungi**.

- Per creare un'attività:

a. Fare clic sul pulsante **Nuova attività**.

b. Nella pagina visualizzata configurare la nuova regola:

- Regola di installazione per gli aggiornamenti di questo livello di importanza

  Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

  Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore alla criticità dell'aggiornamento selezionato (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

  Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

  Per impostazione predefinita, questa opzione è disabilitata.

- Regola di installazione per gli aggiornamenti di questo livello di importanza in base a MSRC (disponibile solo per gli aggiornamenti di Windows Update)

  Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

  Se questa opzione è abilitata (disponibile solo per gli aggiornamenti di Windows Update), gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Microsoft Security Response Center (MSRC) è uguale o superiore al valore selezionato nell'elenco (**Basso**, **Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

  Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

  Per impostazione predefinita, questa opzione è disabilitata.

- Regola di installazione per gli aggiornamenti in base a questo produttore (disponibile solo per gli aggiornamenti di applicazioni di terze parti)

  Questa opzione è disponibile solo per gli aggiornamenti di applicazioni di terze parti. Kaspersky Security Center Cloud Console installa solo gli aggiornamenti relativi alle applicazioni sviluppate dallo stesso produttore dell'aggiornamento selezionato. Gli aggiornamenti rifiutati e gli aggiornamenti per le applicazioni sviluppate da altri produttori non vengono installati.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Regola di installazione per gli aggiornamenti del tipo**
- **Regola di installazione per l'aggiornamento selezionato**
- Approvare gli aggiornamenti selezionati

L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

Per impostazione predefinita, questa opzione è disabilitata.

- **Installa automaticamente tutti gli aggiornamenti precedenti dell'applicazione necessari per l'installazione degli aggiornamenti selezionati**

  Mantenere abilitata questa opzione se si desidera consentire l'installazione delle versioni intermedie delle applicazioni quando questa operazione è necessaria per l'installazione degli aggiornamenti selezionati.

  Se questa opzione è disabilitata, vengono installate solo le versioni delle applicazioni selezionate. Disabilitare questa opzione se si desidera aggiornare le applicazioni in modo diretto, senza tentare di installare le versioni successive in modo incrementale. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

  Si supponga di avere la versione 3 di un'applicazione installata in un dispositivo e di voler eseguire l'aggiornamento alla versione 5, ma la versione 5 di questa applicazione può essere installata solo sulla versione 4. Se questa opzione è abilitata, il software installa prima la versione 4 e quindi la versione 5. Se questa opzione è disabilitata, il software non riesce a eseguire l'aggiornamento l'applicazione.

  Per impostazione predefinita, questa opzione è abilitata.

c. Fare clic sul pulsante **Aggiungi**.

Se è stato scelto di avviare un'attività, è possibile chiudere la procedura guidata. L'attività verrà completata in background. Non sono necessarie ulteriori operazioni.

Se si è scelto di aggiungere una regola a un'attività esistente, verrà visualizzata la finestra delle proprietà dell'attività. La nuova regola è già stata aggiunta alle proprietà dell'attività. È possibile visualizzare o modificare la regola o altre impostazioni dell'attività. Fare clic sul pulsante **Salva** per applicare le modifiche.

Se è stato scelto di creare un'attività, continuare a creare l'attività nella Creazione guidata nuova attività. La nuova regola aggiunta nell'Installazione guidata aggiornamenti viene visualizzata nella Creazione guidata nuova attività. Al termine della Creazione guidata nuova attività, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* verrà aggiunta all'elenco delle attività.

Creazione dell'attività Trova vulnerabilità e aggiornamenti richiesti

Tramite l'attività Trova vulnerabilità e aggiornamenti richiesti, Kaspersky Security Center Cloud Console riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi gestiti.

L'attività Trova vulnerabilità e aggiornamenti richiesti viene creata automaticamente durante l'esecuzione dell'Avvio rapido guidato. Se la procedura guidata non è stata eseguita, è possibile creare l'attività manualmente.

Per creare l'attività Trova vulnerabilità e aggiornamenti richiesti:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

3. Per l'applicazione Kaspersky Security Center Cloud Console, selezionare il tipo di attività **Trova vulnerabilità e aggiornamenti richiesti**.

4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

5. Selezionare i dispositivi a cui assegnare l'attività.

6. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completa creazione attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

7. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.

8. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

9. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività.

10. Nella scheda **Impostazioni applicazione** specificare le seguenti impostazioni:

    - **Cerca vulnerabilità e aggiornamenti elencati da Microsoft**

      Durante la ricerca di vulnerabilità e aggiornamenti, Kaspersky Security Center Cloud Console utilizza le informazioni sugli aggiornamenti Microsoft applicabili della sorgente degli aggiornamenti di Microsoft e disponibili al momento.

      È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft e gli aggiornamenti delle applicazioni di terze parti.

      Per impostazione predefinita, questa opzione è abilitata.

    - **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati**

Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft. I seguenti server possono operare come sorgente degli aggiornamenti Microsoft:

- L'Administration Server di Kaspersky Security Center Cloud Console (vedere le impostazioni del criterio di Network Agent)
- Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione
- Server degli aggiornamenti Microsoft

Se questa opzione è abilitata, Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft per aggiornare le informazioni sugli aggiornamenti di Microsoft Windows applicabili.

Se questa opzione è disabilitata, Windows Update Agent in un dispositivo gestito utilizza le informazioni sugli aggiornamenti di Microsoft Windows applicabili ricevuti dalla sorgente degli aggiornamenti Microsoft in precedenza e archiviati nella cache del dispositivo.

La connessione alla sorgente degli aggiornamenti Microsoft può comportare un notevole utilizzo di risorse. Potrebbe essere necessario disabilitare questa opzione se è stata impostata una connessione standard a questa sorgente degli aggiornamenti in un'altra attività o nelle proprietà del criterio Network Agent, nella sezione **Vulnerabilità e aggiornamenti software**. Se non si desidera disabilitare questa opzione, per ridurre l'overload del Server è possibile configurare la pianificazione delle attività in modo da utilizzare il ritardo casuale per l'avvio delle attività entro 360 minuti.

Per impostazione predefinita, questa opzione è abilitata.

La combinazione delle seguenti opzioni delle impostazioni del criterio di Network Agent definisce il modo in cui si ottengono gli aggiornamenti:

- Windows Update Agent in un dispositivo gestito si connette al server di aggiornamento per ottenere gli aggiornamenti solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è abilitata e l'opzione **Attiva**, nel gruppo di impostazioni **Modalità di ricerca di Windows Update**, è selezionata.
- Windows Update Agent in un dispositivo gestito utilizza le informazioni sugli aggiornamenti di Microsoft Windows applicabili ricevuti dalla sorgente degli aggiornamenti Microsoft in precedenza e archiviati nella cache del dispositivo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è abilitata e l'opzione **Passiva**, nel gruppo di impostazioni **Modalità di ricerca di Windows Update**, è selezionata oppure se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è disabilitata e l'opzione **Attiva**, nel gruppo di impostazioni **Modalità di ricerca di Windows Update**, è selezionata.
- Indipendentemente dallo stato dell'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** (abilitata o disabilitata), se l'opzione **Disabilitata** nel gruppo di impostazioni **Modalità di ricerca di Windows Update** è selezionata, Kaspersky Security Center Cloud Console non richiede informazioni sugli aggiornamenti.

- Cerca vulnerabilità e aggiornamenti di terze parti elencati da Kaspersky

Se questa opzione è abilitata, Kaspersky Security Center Cloud Console esegue la ricerca delle vulnerabilità e degli aggiornamenti richiesti per le applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) nel Registro di sistema di Windows e nelle cartelle specificate con **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**. L'elenco completo delle applicazioni di terze parti supportate è gestito da Kaspersky.

Se questa opzione è disabilitata, Kaspersky Security Center Cloud Console non esegue la ricerca di vulnerabilità e aggiornamenti richiesti per le applicazioni di terze parti. È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft Windows e gli aggiornamenti delle applicazioni di terze parti.

Per impostazione predefinita, questa opzione è abilitata.

- **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**

  Cartelle in cui Kaspersky Security Center Cloud Console esegue la ricerca delle applicazioni di terze parti che richiedono la correzione delle vulnerabilità e l'installazione di aggiornamenti. È possibile utilizzare le variabili di sistema.

  Specificare le cartelle in cui sono installate le applicazioni. Per impostazione predefinita, l'elenco è vuoto.

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive le tracce anche se il tracciamento è disabilitato per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center Cloud Console. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center Cloud Console. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

11. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Se i risultati dell'attività contengono l'avviso 0x80240033 "Errore di Windows Update Agent 80240033 ("Non è stato possibile scaricare le condizioni di licenza")", è possibile risolvere questo problema tramite il Registro di sistema di Windows.

Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente durante l'esecuzione dell'Avvio rapido guidato. Se la procedura guidata non è stata eseguita, è possibile creare l'attività manualmente.

Oltre alle impostazioni generali delle attività, è possibile specificare le seguenti impostazioni durante la creazione dell'attività *Trova vulnerabilità e aggiornamenti richiesti* o in un secondo momento, quando si configurano le proprietà dell'attività creata:

- **Cerca vulnerabilità e aggiornamenti elencati da Microsoft**

  Durante la ricerca di vulnerabilità e aggiornamenti, Kaspersky Security Center Cloud Console utilizza le informazioni sugli aggiornamenti Microsoft applicabili della sorgente degli aggiornamenti di Microsoft e disponibili al momento.

  È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft e gli aggiornamenti delle applicazioni di terze parti.

  Per impostazione predefinita, questa opzione è abilitata.

- **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati**

Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft. I seguenti server possono operare come sorgente degli aggiornamenti Microsoft:

- L'Administration Server di Kaspersky Security Center Cloud Console (vedere le impostazioni del criterio di Network Agent)
- Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione
- Server degli aggiornamenti Microsoft

Se questa opzione è abilitata, Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft per aggiornare le informazioni sugli aggiornamenti di Microsoft Windows applicabili.

Se questa opzione è disabilitata, Windows Update Agent in un dispositivo gestito utilizza le informazioni sugli aggiornamenti di Microsoft Windows applicabili ricevuti dalla sorgente degli aggiornamenti Microsoft in precedenza e archiviati nella cache del dispositivo.

La connessione alla sorgente degli aggiornamenti Microsoft può comportare un notevole utilizzo di risorse. Potrebbe essere necessario disabilitare questa opzione se è stata impostata una connessione standard a questa sorgente degli aggiornamenti in un'altra attività o nelle proprietà del criterio Network Agent, nella sezione **Vulnerabilità e aggiornamenti software**. Se non si desidera disabilitare questa opzione, per ridurre l'overload del Server è possibile configurare la pianificazione delle attività in modo da utilizzare il ritardo casuale per l'avvio delle attività entro 360 minuti.

Per impostazione predefinita, questa opzione è abilitata.

La combinazione delle seguenti opzioni delle impostazioni del criterio di Network Agent definisce il modo in cui si ottengono gli aggiornamenti:

- Windows Update Agent in un dispositivo gestito si connette al server di aggiornamento per ottenere gli aggiornamenti solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è abilitata e l'opzione **Attiva**, nel gruppo di impostazioni **Modalità di ricerca di Windows Update**, è selezionata.
- Windows Update Agent in un dispositivo gestito utilizza le informazioni sugli aggiornamenti di Microsoft Windows applicabili ricevuti dalla sorgente degli aggiornamenti Microsoft in precedenza e archiviati nella cache del dispositivo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è abilitata e l'opzione **Passiva**, nel gruppo di impostazioni **Modalità di ricerca di Windows Update**, è selezionata oppure se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è disabilitata e l'opzione **Attiva**, nel gruppo di impostazioni **Modalità di ricerca di Windows Update**, è selezionata.
- Indipendentemente dallo stato dell'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** (abilitata o disabilitata), se l'opzione **Disabilitata** nel gruppo di impostazioni **Modalità di ricerca di Windows Update** è selezionata, Kaspersky Security Center Cloud Console non richiede informazioni sugli aggiornamenti.

- Cerca vulnerabilità e aggiornamenti di terze parti elencati da Kaspersky

Se questa opzione è abilitata, Kaspersky Security Center Cloud Console esegue la ricerca delle vulnerabilità e degli aggiornamenti richiesti per le applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) nel Registro di sistema di Windows e nelle cartelle specificate con **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**. L'elenco completo delle applicazioni di terze parti supportate è gestito da Kaspersky.

Se questa opzione è disabilitata, Kaspersky Security Center Cloud Console non esegue la ricerca di vulnerabilità e aggiornamenti richiesti per le applicazioni di terze parti. È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft Windows e gli aggiornamenti delle applicazioni di terze parti.

Per impostazione predefinita, questa opzione è abilitata.

- **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**

  Cartelle in cui Kaspersky Security Center Cloud Console esegue la ricerca delle applicazioni di terze parti che richiedono la correzione delle vulnerabilità e l'installazione di aggiornamenti. È possibile utilizzare le variabili di sistema.

  Specificare le cartelle in cui sono installate le applicazioni. Per impostazione predefinita, l'elenco è vuoto.

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive le tracce anche se il tracciamento è disabilitato per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center Cloud Console. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center Cloud Console. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

Raccomandazioni relative alla pianificazione delle attività

Durante la pianificazione dell'attività *Trova vulnerabilità e aggiornamenti richiesti*, verificare che le due opzioni **Esegui attività non effettuate** e **Usa automaticamente il ritardo casuale per l'avvio delle attività** siano abilitate.

Per impostazione predefinita, l'attività *Trova vulnerabilità e aggiornamenti richiesti* è impostata per l'avvio alle 18:00. Se le regole dell'organizzazione per l'ambiente di lavoro prevedono lo spegnimento di tutti i dispositivi in tale orario, l'attività *Trova vulnerabilità e aggiornamenti richiesti* verrà eseguita dopo la riaccensione dei dispositivi, la mattina del giorno successivo. Un'attività di questo tipo potrebbe essere indesiderabile perché una Scansione vulnerabilità può aumentare il carico sui sottosistemi del disco e della CPU. È necessario impostare la pianificazione appropriata per l'attività in base alle regole per l'ambiente di lavoro adottate nell'organizzazione.

Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità

La disponibilità dell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* dipende dalla modalità di Kaspersky Security Center Cloud Console e dalla licenza corrente.

L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per aggiornare e correggere le vulnerabilità nel software di terze parti, incluso il software Microsoft, installato nei dispositivi gestiti. Questa attività consente di installare più aggiornamenti e correggere più vulnerabilità in base a determinate regole.

Per installare aggiornamenti o correggere vulnerabilità utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile effettuare una delle seguenti operazioni:

- Eseguire l'Installazione guidata aggiornamenti o la Correzione guidata vulnerabilità.
- Creare un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.
- Aggiungere una regola per l'installazione dell'aggiornamento a un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* esistente.

Le attività di installazione degli aggiornamenti software prevedono una serie di limitazioni. Queste limitazioni dipendono dalla licenza con cui si utilizza Kaspersky Security Center Cloud Console e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

Per creare un'attività Installa aggiornamenti richiesti e correggi vulnerabilità:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center Cloud Console, selezionare il tipo di attività **Installa aggiornamenti richiesti e correggi vulnerabilità**.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare i dispositivi a cui assegnare l'attività.
6. Specificare le regole per l'installazione dell'aggiornamento, quindi specificare le seguenti impostazioni:
   - **Avvia l'installazione al riavvio o all'arresto del dispositivo**

Se questa opzione è abilitata, gli aggiornamenti vengono installati al riavvio o all'arresto del dispositivo. In caso contrario, gli aggiornamenti vengono installati in base a una pianificazione.

Utilizzare questa opzione se l'installazione degli aggiornamenti può influire sulle prestazioni del dispositivo.

Per impostazione predefinita, questa opzione è disabilitata.

- **Installa i componenti generali del sistema richiesti**

  Se questa opzione è abilitata, prima di installare un aggiornamento l'applicazione installa automaticamente tutti i componenti di sistema generali (prerequisiti) richiesti per installare l'aggiornamento. Questi prerequisiti possono ad esempio essere aggiornamenti del sistema operativo.

  Se questa opzione è disabilitata, può essere necessario installare manualmente i prerequisiti.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Consenti l'installazione di nuove versioni dell'applicazione durante gli aggiornamenti**

  Se questa opzione è abilitata, gli aggiornamenti sono consentiti se implicano l'installazione di una nuova versione di un'applicazione software.

  Se questa opzione è disabilitata, l'upgrade del software non viene eseguito. È quindi possibile installare le nuove versioni del software manualmente o tramite un'altra attività. È ad esempio possibile utilizzare questa opzione se l'infrastruttura aziendale non è supportata da una nuova versione del software o se si desidera verificare un aggiornamento in un'infrastruttura di test.

  Per impostazione predefinita, questa opzione è abilitata.

  L'upgrade dell'applicazione può causare un malfunzionamento delle applicazioni dipendenti installate nei dispositivi client.

- **Scarica gli aggiornamenti nel dispositivo senza installarli**

  Se questa opzione è abilitata, l'applicazione scarica gli aggiornamenti nel dispositivo client ma non li installa automaticamente. È quindi possibile installare manualmente gli aggiornamenti scaricati.

  Gli aggiornamenti Microsoft vengono scaricati nell'archiviazione di sistema di Windows. Gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) vengono scaricati nella cartella specificata nel campo **Scarica aggiornamenti in**.

  Se questa opzione è disabilitata, gli aggiornamenti vengono installati automaticamente nel dispositivo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Cartella per il download degli aggiornamenti**

  Questa cartella viene utilizzata per scaricare gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft).

- **Abilita diagnostica avanzata**

Se questa funzionalità è abilitata, Network Agent scrive le tracce anche se il tracciamento è disabilitato per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center Cloud Console. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center Cloud Console. Non viene eseguita la scrittura di ulteriori tracce.

Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

7. Specificare le impostazioni per il riavvio del sistema operativo:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

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

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ripeti la richiesta ogni (min.)**

Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

- **Riavvia dopo (min.)**

  Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

  Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Tempo di attesa prima della chiusura forzata delle applicazioni nelle sessioni bloccate (min.)**

  Viene forzata la chiusura delle applicazioni quando il dispositivo dell'utente viene bloccato (automaticamente dopo un intervallo di inattività specificato o manualmente).

  Se questa opzione è abilitata, viene forzata la chiusura delle applicazioni nel dispositivo bloccato alla scadenza dell'intervallo di tempo specificato nel campo di immissione.

  Se questa opzione è disabilitata, le applicazioni nel dispositivo bloccato non vengono chiuse.

  Per impostazione predefinita, questa opzione è disabilitata.

8. Se nella pagina **Completa creazione attività** si abilita l'opzione **Apri i dettagli dell'attività al termine della creazione**, è possibile modificare le impostazioni predefinite dell'attività. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

9. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.

10. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

11. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

12. Fare clic sul pulsante **Salva**.

    L'attività verrà creata e configurata.

Se i risultati dell'attività contengono l'avviso 0x80240033 "Errore di Windows Update Agent 80240033 ("Non è stato possibile scaricare le condizioni di licenza")", è possibile risolvere questo problema tramite il Registro di sistema di Windows.

Aggiunta delle regole per l'installazione dell'aggiornamento

La disponibilità di questa funzionalità dipende dalla modalità di Kaspersky Security Center Cloud Console e dalla licenza corrente.

Durante l'installazione di aggiornamenti software o la correzione di vulnerabilità del software tramite l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è necessario specificare le regole per l'installazione degli aggiornamenti. Queste regole determinano gli aggiornamenti da installare e le vulnerabilità da correggere.

Le esatte impostazioni dipendono dall'esigenza di aggiungere una regola per tutti gli aggiornamenti, per gli aggiornamenti di Windows Update o per gli aggiornamenti di applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft). Durante l'aggiunta di una regola per gli aggiornamenti di Windows Update o per gli aggiornamenti di applicazioni di terze parti, è possibile selezionare le specifiche applicazioni e versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Durante l'aggiunta di una regola per tutti gli aggiornamenti, è possibile selezionare gli specifici aggiornamenti da installare e le vulnerabilità che si desidera correggere tramite l'installazione degli aggiornamenti.

È possibile aggiungere una regola per l'installazione degli aggiornamenti nei modi seguenti:

- Aggiungendo una regola durante la creazione di una nuova attività Installa aggiornamenti richiesti e correggi vulnerabilità.
- Aggiungendo una regola nella scheda **Impostazioni applicazione** nella finestra delle proprietà di un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* esistente.
- Tramite l'Installazione guidata aggiornamenti o la Correzione guidata vulnerabilità.

Per aggiungere una nuova regola per tutti gli aggiornamenti:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per tutti gli aggiornamenti**.

3. Nella pagina **Criteri generali** utilizzare gli elenchi a discesa per specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Aggiornamenti** selezionare gli aggiornamenti da installare:

- **Installa tutti gli aggiornamenti appropriati**

  Installa tutti gli aggiornamenti software che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

- **Installa solo gli aggiornamenti nell'elenco**

  Installa solo gli aggiornamenti software che selezionati manualmente dall'elenco. Questo elenco contiene tutti gli aggiornamenti software disponibili.

  Ad esempio, è possibile selezionare aggiornamenti specifici nei seguenti casi: per verificarne l'installazione in un ambiente di test, per aggiornare solo le applicazioni critiche o per aggiornare solo specifiche applicazioni.

- **Installa automaticamente tutti gli aggiornamenti precedenti dell'applicazione necessari per l'installazione degli aggiornamenti selezionati**

  Mantenere abilitata questa opzione se si desidera consentire l'installazione delle versioni intermedie delle applicazioni quando questa operazione è necessaria per l'installazione degli aggiornamenti selezionati.

  Se questa opzione è disabilitata, vengono installate solo le versioni delle applicazioni selezionate. Disabilitare questa opzione se si desidera aggiornare le applicazioni in modo diretto, senza tentare di installare le versioni successive in modo incrementale. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

  Si supponga di avere la versione 3 di un'applicazione installata in un dispositivo e di voler eseguire l'aggiornamento alla versione 5, ma la versione 5 di questa applicazione può essere installata solo sulla versione 4. Se questa opzione è abilitata, il software installa prima la versione 4 e quindi la versione 5. Se questa opzione è disabilitata, il software non riesce a eseguire l'aggiornamento l'applicazione.

  Per impostazione predefinita, questa opzione è abilitata.

5. Nella pagina **Vulnerabilità** selezionare le vulnerabilità da correggere tramite l'installazione degli aggiornamenti selezionati:

- **Correggi tutte le vulnerabilità che corrispondono ad altri criteri**

  Verranno corrette tutte le vulnerabilità che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

- Correggi solo le vulnerabilità nell'elenco

  Verranno corrette solo le vulnerabilità selezionate manualmente dall'elenco. Questo elenco contiene tutte le vulnerabilità rilevate.

  Ad esempio, è possibile selezionare vulnerabilità specifiche nei seguenti casi: per verificarne la correzione in un ambiente di test, per correggere solo le vulnerabilità di applicazioni critiche o per correggere le vulnerabilità solo in specifiche applicazioni.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Per aggiungere una nuova regola per gli aggiornamenti di Windows Update:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per Windows Update**.

3. Nella finestra **Criteri generali** specificare le seguenti impostazioni:

   - Set di aggiornamenti da installare

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - Correggi le vulnerabilità con un livello di criticità uguale o superiore a

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

   - Correggi le vulnerabilità con un livello di criticità MSRC uguale o superiore a

Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Microsoft Security Response Center (MSRC) è uguale o superiore al valore selezionato nell'elenco (**Basso**, **Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Categorie di aggiornamenti** selezionare le categorie di aggiornamenti da installare. Queste categorie sono identiche a quelle del catalogo di Microsoft Update. Per impostazione predefinita, tutte le categorie sono selezionate.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Per aggiungere una nuova regola per gli aggiornamenti delle applicazioni di terze parti:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per gli aggiornamenti di terze parti**.

3. Nella finestra **Criteri generali** specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione Impostazioni della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Creazione dell'attività Installa aggiornamenti di Windows Update

L'attività Installa aggiornamenti di Windows Update consente di installare gli aggiornamenti software forniti dal servizio Windows Update nei dispositivi client.

Le attività di installazione degli aggiornamenti software prevedono una serie di limitazioni. Queste limitazioni dipendono dalla licenza con cui si utilizza Kaspersky Security Center Cloud Console e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

Per creare l'attività Installa aggiornamenti di Windows Update:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Per l'applicazione Kaspersky Security Center Cloud Console, selezionare il tipo di attività **Installa aggiornamenti di Windows Update**.

4. Specificare il nome dell'attività che si intende creare.

   Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

5. Selezionare i dispositivi a cui assegnare l'attività.

6. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzato l'elenco degli aggiornamenti.

7. Selezionare gli aggiornamenti di Windows Update che si desidera installare, quindi fare clic su **OK**.

8. Specificare le impostazioni per il riavvio del sistema operativo:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

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

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ripeti la richiesta ogni (min.)**

  Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

  Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

- **Riavvia dopo (min.)**

  Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

  Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

9. Specificare le impostazioni per l'account:

- **Account predefinito**

  L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

  Per impostazione predefinita, questa opzione è selezionata.

- **Specifica account**

  Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

- **Account**

  Account tramite il quale viene eseguita l'attività.

- **Password**

  Password dell'account con cui verrà eseguita l'attività.

10. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completa creazione attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

11. Fare clic sul pulsante **Fine**.

    L'attività verrà creata e visualizzata nell'elenco delle attività.

12. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

13. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

14. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Visualizzazione delle informazioni sugli aggiornamenti software di terze parti disponibili

È possibile visualizzare l'elenco degli aggiornamenti disponibili per il software di terze parti, incluso il software Microsoft, installato nei dispositivi client.

Per visualizzare un elenco degli aggiornamenti disponibili per le applicazioni di terze parti installate nei dispositivi client:

Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Aggiornamenti software**.

Verrà visualizzato un elenco degli aggiornamenti disponibili.

È possibile specificare un filtro per visualizzare l'elenco degli aggiornamenti software. Fare clic sull'icona **Filtro** ( ) nell'angolo superiore destro dell'elenco degli aggiornamenti software per gestire il filtro. È anche possibile selezionare uno dei filtri preimpostati dall'elenco a discesa **Filtri preimpostati** sopra l'elenco delle vulnerabilità del software.

Per visualizzare le proprietà di un aggiornamento:

1. Fare clic sul nome dell'aggiornamento software richiesto.
2. Verrà visualizzata la finestra delle proprietà dell'aggiornamento, in cui sono visualizzate informazioni raggruppate nelle seguenti schede:

   - **Generale**

     Questa scheda mostra i dettagli generali dell'aggiornamento selezionato:

     - Stato di approvazione dell'aggiornamento. (può essere modificato manualmente selezionando un nuovo stato nell'elenco a discesa)
     - Categoria WSUS (Windows Server Update Services) a cui appartiene l'aggiornamento
     - Data e ora di registrazione dell'aggiornamento
     - Data e ora di creazione dell'aggiornamento
     - Livello di importanza dell'aggiornamento
     - Requisiti di installazione imposti dall'aggiornamento
     - Famiglia di applicazioni a cui appartiene l'aggiornamento
     - Applicazione a cui si applica l'aggiornamento
     - Numero di revisione dell'aggiornamento

   - **Attributi**

Questa scheda visualizza un set di attributi che è possibile utilizzare per ottenere ulteriori informazioni sull'aggiornamento selezionato. Questo set varia a seconda che l'aggiornamento sia pubblicato da Microsoft o da un fornitore di terze parti.

La scheda visualizza le seguenti informazioni per un aggiornamento Microsoft:

- Livello di importanza dell'aggiornamento secondo Microsoft Security Response Center (MSRC)
- Collegamento all'articolo nella Microsoft Knowledge Base in cui viene descritto l'aggiornamento
- Collegamento all'articolo nel Bollettino Microsoft sulla sicurezza in cui viene descritto l'aggiornamento
- ID di aggiornamento

La scheda visualizza le seguenti informazioni per un aggiornamento di terze parti:

- Se l'aggiornamento è una patch o un pacchetto di distribuzione completo
- Lingua di localizzazione dell'aggiornamento
- Se l'aggiornamento viene installato automaticamente o manualmente
- Se l'aggiornamento è stato revocato dopo l'applicazione
- Collegamento per scaricare l'aggiornamento

- **Dispositivi**

  Questa scheda visualizza un elenco di dispositivi in cui è stato installato l'aggiornamento selezionato.

- **Vulnerabilità risolte**

  Questa scheda visualizza un elenco di vulnerabilità che l'aggiornamento selezionato è in grado di correggere.

- **Crossover degli aggiornamenti**

  Questa scheda visualizza i possibili crossover tra i vari aggiornamenti pubblicati per la stessa applicazione, ovvero se l'aggiornamento selezionato può sostituire altri aggiornamenti o, viceversa, essere sostituito da altri aggiornamenti (disponibile solo per gli aggiornamenti Microsoft).

- **Attività per l'installazione dell'aggiornamento**

  Questa scheda visualizza un elenco di attività il cui ambito include l'installazione dell'aggiornamento selezionato. La scheda consente inoltre di creare una nuova attività di installazione remota per l'aggiornamento.

Per visualizzare le statistiche relative all'installazione di un aggiornamento:

1. Selezionare la casella di controllo accanto all'aggiornamento software richiesto.

2. Fare clic sul pulsante **Statistiche degli stati di installazione aggiornamenti**.

   Verrà visualizzato il diagramma degli stati di installazione dell'aggiornamento. Facendo clic su uno stato, viene aperto un elenco dei dispositivi in cui l'aggiornamento ha lo stato selezionato.

È possibile visualizzare le informazioni sugli aggiornamenti software disponibili per il software di terze parti, incluso il software Microsoft, installato nel dispositivo gestito selezionato che esegue Windows.

Per visualizzare un elenco degli aggiornamenti disponibili per il software di terze parti installato nel dispositivo gestito selezionato:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo per cui si desidera visualizzare gli aggiornamenti software di terze parti.

   Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.

3. Nella finestra delle proprietà del dispositivo selezionato selezionare la scheda **Avanzate**.

4. Nel riquadro sinistro selezionare la sezione **Aggiornamenti disponibili**. Per visualizzare solo gli aggiornamenti installati, abilitare l'opzione **Mostra aggiornamenti installati**.

Verrà visualizzato l'elenco degli aggiornamenti software di terze parti disponibili per il dispositivo selezionato.

Esportazione dell'elenco degli aggiornamenti software disponibili in un file

È possibile esportare l'elenco degli aggiornamenti per il software di terze parti, incluso il software Microsoft, che viene attualmente visualizzato nei file CSV o TXT. È ad esempio possibile utilizzare questi file per inviarli al responsabile della sicurezza delle informazioni o per archiviarli a fini statistici.

Per esportare in un file di testo l'elenco degli aggiornamenti disponibili per il software di terze parti installato in tutti i dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Aggiornamenti software**.

   La pagina visualizza un elenco degli aggiornamenti disponibili per il software di terze parti installato in tutti i dispositivi gestiti.

2. Fare clic sul pulsante **Esporta in TXT** o **Esporta in CSV**, a seconda del formato preferito per l'esportazione.

Il file contenente l'elenco degli aggiornamenti disponibili per il software di terze parti, incluso il software Microsoft, verrà scaricato nel dispositivo in uso.

Per esportare in un file di testo l'elenco degli aggiornamenti disponibili per il software di terze parti installato nel dispositivo gestito selezionato:

1. Aprire l'elenco degli aggiornamenti software di terze parti disponibili nel dispositivo gestito selezionato.

2. Selezionare gli aggiornamenti software da esportare.

   Ignorare questo passaggio se si desidera esportare un elenco completo degli aggiornamenti software.

Se si desidera esportare un elenco completo degli aggiornamenti software, verranno esportati solo gli aggiornamenti visualizzati nella pagina corrente.

Per esportare solo gli aggiornamenti installati, selezionare la casella di controllo **Mostra aggiornamenti installati**.

3. Fare clic sul pulsante **Esporta in TXT** o **Esporta in CSV**, a seconda del formato preferito per l'esportazione.

Il file contenente l'elenco degli aggiornamenti per il software di terze parti, incluso il software Microsoft, installati nel dispositivo gestito selezionato verrà scaricato nel dispositivo in uso.

Approvazione e rifiuto degli aggiornamenti software di terze parti

Quando si configura l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile creare una regola che richiede uno stato specifico degli aggiornamenti che devono essere installati. Ad esempio, una regola di aggiornamento può consentire l'installazione dei seguenti elementi:

- Solo gli aggiornamenti approvati
- Solo gli aggiornamenti approvati e non definiti
- Tutti gli aggiornamenti, indipendentemente dai relativi stati

È possibile approvare gli aggiornamenti da installare e rifiutare quelli che non devono essere installati.

L'utilizzo dello stato *Approvato* per gestire l'installazione degli aggiornamenti è efficace per una piccola quantità di aggiornamenti. Per installare più aggiornamenti, utilizzare le regole che è possibile configurare nell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. È consigliabile impostare lo stato *Approvato* solo per gli aggiornamenti specifici che non soddisfano i criteri specificati nelle regole. Quando si approva manualmente una grande quantità di aggiornamenti, le prestazioni di Administration Server si riducono e questo può causare un sovraccarico di Administration Server.

Per approvare o rifiutare uno o più aggiornamenti:

1. Nel menu principale accedere a **Operazioni → Gestione patch → Aggiornamenti software**.

   Verrà visualizzato un elenco degli aggiornamenti disponibili.

2. Selezionare gli aggiornamenti che si desidera accettare o rifiutare.

3. Fare clic su **Approva** per approvare gli aggiornamenti selezionati o su **Rifiuta** per rifiutare gli aggiornamenti selezionati.

   Il valore predefinito è *Indefinito*.

Gli aggiornamenti selezionati hanno gli stati che sono stati definiti.

Facoltativamente è possibile modificare lo stato di approvazione nelle proprietà di un aggiornamento specifico.

Per approvare o rifiutare un aggiornamento nelle relative proprietà:

1. Nel menu principale accedere a **Operazioni → Gestione patch → Aggiornamenti software**.

   Verrà visualizzato un elenco degli aggiornamenti disponibili.

2. Fare clic sul nome dell'aggiornamento che si desidera approvare o rifiutare.

Verrà visualizzata la finestra delle proprietà dell'aggiornamento.

3. Nella sezione **Generale** selezionare uno stato per l'aggiornamento modificando l'opzione **Stato di approvazione dell'aggiornamento**. È possibile selezionare lo stato *Approvato*, *Rifiutato* o *Indefinito*.

4. Fare clic sul pulsante **Salva** per applicare le modifiche.

L'aggiornamento selezionato ha lo stato che è stato definito.

Se si imposta lo stato **Rifiutato** per gli aggiornamenti software di terze parti, tali aggiornamenti non verranno installati nei dispositivi in cui l'installazione era stata pianificata ma non ancora eseguita. Gli aggiornamenti rimarranno nei dispositivi in cui erano già installati. Se è necessario eliminarli, è possibile eliminarli manualmente in locale.

Aggiornamento automatico delle applicazioni di terze parti

Alcune applicazioni di terze parti possono essere aggiornate automaticamente. Il fornitore dell'applicazione definisce se l'applicazione supporta o meno la funzionalità di aggiornamento automatico. Se un'applicazione di terze parti installata in un dispositivo gestito supporta l'aggiornamento automatico, è possibile specificare l'impostazione di aggiornamento automatico nelle proprietà dell'applicazione. Dopo aver modificato l'impostazione di aggiornamento automatico, i Network Agent applicano la nuova impostazione in ogni dispositivo gestito in cui è installata l'applicazione.

L'impostazione di aggiornamento automatico è indipendente dagli altri oggetti e dalle impostazioni della funzionalità Vulnerability e patch management. Questa impostazione non dipende ad esempio da uno stato di approvazione degli aggiornamenti o dalle attività di installazione degli aggiornamenti, come *Installa aggiornamenti richiesti e correggi vulnerabilità*, *Installa aggiornamenti di Windows Update* e *Correggi vulnerabilità*.

Per configurare l'impostazione di aggiornamento automatico per un'applicazione di terze parti:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Registro delle applicazioni**.

2. Fare clic sul nome dell'applicazione per la quale si desidera modificare l'impostazione di aggiornamento automatico.

   Per semplificare la ricerca, è possibile filtrare l'elenco in base alla colonna **Stato degli aggiornamenti automatici**.

   Verrà visualizzata la finestra delle proprietà dell'applicazione.

3. Nella sezione **Generale** selezionare un valore per la seguente impostazione:

   Stato degli aggiornamenti automatici

Selezionare una delle seguenti opzioni:

- **Indefinito**

  La funzionalità di aggiornamento automatico è disabilitata. Kaspersky Security Center Cloud Console installa gli aggiornamenti delle applicazioni di terze parti utilizzando le attività: *Installa aggiornamenti richiesti e correggi vulnerabilità*, *Installa aggiornamenti di Windows Update* e *Correggi vulnerabilità*.

- **Consentito**

  Dopo che il fornitore rilascia un aggiornamento per l'applicazione, questo aggiornamento viene installato automaticamente nei dispositivi gestiti. Non sono necessarie operazioni aggiuntive.

- **Bloccato**

  Questi aggiornamenti dell'applicazione non vengono installati automaticamente. Kaspersky Security Center Cloud Console installa gli aggiornamenti delle applicazioni di terze parti utilizzando le attività: *Installa aggiornamenti richiesti e correggi vulnerabilità*, *Installa aggiornamenti di Windows Update* e *Correggi vulnerabilità*.

4. Fare clic sul pulsante **Salva** per applicare le modifiche.

L'impostazione di aggiornamento automatico viene applicata all'applicazione selezionata.

Correzione delle vulnerabilità del software di terze parti

Questa sezione descrive le funzionalità di Kaspersky Security Center Cloud Console relative alla correzione delle vulnerabilità nel software installato nei dispositivi gestiti.

Scenario: Ricerca e la correzione delle vulnerabilità del software

Questa sezione fornisce uno scenario per individuare e correggere le vulnerabilità nei dispositivi gestiti che eseguono Windows. È possibile individuare e correggere le vulnerabilità del software nel sistema operativo e nel software di terze parti, incluso il software Microsoft.

Prerequisiti

- Kaspersky Security Center Cloud Console viene distribuito nell'organizzazione.
- Nell'organizzazione sono presenti dispositivi gestiti che eseguono Windows.

Passaggi

L'individuazione e la correzione delle vulnerabilità del software prevede diversi passaggi:

1. **Ricerca delle vulnerabilità nel software installato nei dispositivi client**

Per individuare le vulnerabilità nel software installato nei dispositivi gestiti, eseguire l'attività *Trova vulnerabilità e aggiornamenti richiesti*. Al termine di questa attività, Kaspersky Security Center Cloud Console riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi specificati nelle proprietà dell'attività.

L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center Cloud Console. Se la procedura guidata non è stata eseguita, avviarla ora o creare l'attività manualmente.

Istruzioni dettagliate: Creazione dell'attività Trova vulnerabilità e aggiornamenti richiesti

2. **Analisi dell'elenco delle vulnerabilità del software rilevate**

Visualizzare l'elenco **Vulnerabilità del software** e decidere quali vulnerabilità devono essere corrette. Per visualizzare informazioni dettagliate su ciascuna vulnerabilità, fare clic sul nome della vulnerabilità nell'elenco. Per ogni vulnerabilità nell'elenco, è anche possibile visualizzare le statistiche sulla vulnerabilità nei dispositivi gestiti.

Istruzioni dettagliate:

- Visualizzazione delle informazioni sulle vulnerabilità del software
- Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti

3. **Configurazione della correzione delle vulnerabilità**

Quando vengono rilevate le vulnerabilità del software, è possibile correggere le vulnerabilità del software nei dispositivi gestiti utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità*.

L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per aggiornare e correggere le vulnerabilità nel software di terze parti, incluso il software Microsoft, installato nei dispositivi gestiti. Questa attività consente di installare più aggiornamenti e correggere più vulnerabilità in base a determinate regole. La disponibilità di questa attività dipende dalla modalità di Kaspersky Security Center Cloud Console e dalla licenza corrente. Per correggere le vulnerabilità del software l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* utilizza gli aggiornamenti software consigliati.

L'attività *Correggi vulnerabilità* utilizza le correzioni consigliate per il software Microsoft.

È possibile avviare la Correzione guidata vulnerabilità che crea automaticamente una di queste attività oppure è possibile creare una di queste attività manualmente.

Istruzioni dettagliate: Correzione delle vulnerabilità nel software di terze parti, Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità

4. **Pianificazione delle attività**

Per assicurarsi che l'elenco delle vulnerabilità sia sempre aggiornato, pianificare l'attività *Trova vulnerabilità e aggiornamenti richiesti* affinché venga eseguita periodicamente in modo automatico. La frequenza media consigliata è una volta alla settimana.

Se è stata creata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile pianificarla in modo che venga eseguita con la stessa frequenza dell'attività *Trova vulnerabilità e aggiornamenti richiesti* o con una frequenza inferiore. Quando si pianifica l'attività *Correggi vulnerabilità*, tenere presente che è necessario selezionare le correzioni per il software Microsoft ogni volta prima di avviare l'attività.

Quando si pianificano le attività, assicurarsi che al termine dell'attività *Trova vulnerabilità e aggiornamenti richiesti* venga avviata un'attività per correggere la vulnerabilità.

5. **Ignorare le vulnerabilità del software (facoltativo)**

Se lo si desidera, è possibile ignorare le vulnerabilità del software da correggere in tutti i dispositivi gestiti o solo nei dispositivi gestiti selezionati.

Istruzioni dettagliate: Ignorare le vulnerabilità del software

6. **Esecuzione di un'attività di correzione della vulnerabilità**

Avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità*. Al termine dell'attività, assicurarsi che questa abbia lo stato *Completato* nell'elenco attività.

7. **Creare il rapporto sui risultati della correzione delle vulnerabilità del software (facoltativo)**

   Per visualizzare le statistiche dettagliate sulla correzione delle vulnerabilità, generare il Rapporto sulle vulnerabilità. Il rapporto visualizza informazioni sulle vulnerabilità del software che non sono state corrette. In tal modo è possibile avere un'idea sulla ricerca e la correzione delle vulnerabilità nel software di terze parti, incluso il software Microsoft, presente nell'organizzazione.

   Istruzioni dettagliate: Generazione e visualizzazione di un rapporto

8. **Verifica della configurazione e individuazione e correzione delle vulnerabilità nel software di terze parti**

   Assicurarsi di quanto segue:

   - L'elenco delle vulnerabilità del software nei dispositivi gestiti non è vuoto.
   - Un'attività per correggere le vulnerabilità è nell'elenco delle attività.
   - Le attività per individuare e correggere le vulnerabilità del software vengono pianificate in modo che vengano avviate in sequenza. Visualizzare le proprietà di queste attività e confrontare la relativa pianificazione.
   - L'attività per correggere le vulnerabilità del software è stata completata correttamente. Visualizzare le informazioni nella scheda **Risultati** della finestra delle proprietà dell'attività.

Risultati

Se è stata creata e configurata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, le vulnerabilità vengono corrette automaticamente nei dispositivi gestiti. Quando viene eseguita, l'attività collega l'elenco degli aggiornamenti software disponibili alle regole specificate nelle impostazioni dell'attività. Tutti gli aggiornamenti software che soddisfano i criteri nelle regole verranno scaricati negli archivi dei punti di distribuzione e verranno installati per correggere le vulnerabilità del software.

Se è stata creata l'attività *Correggi vulnerabilità*, vengono corrette solo le vulnerabilità del software nel software Microsoft.

Informazioni sulla ricerca e la correzione delle vulnerabilità del software

Kaspersky Security Center Cloud Console rileva e corregge le vulnerabilità del software nei dispositivi gestiti che eseguono i sistemi operativi delle famiglie Microsoft Windows. Le vulnerabilità vengono rilevate nel sistema operativo e nel software di terze parti, incluso il software Microsoft.

Individuazione delle vulnerabilità del software

Per individuare le vulnerabilità del software, Kaspersky Security Center Cloud Console utilizza le caratteristiche del database delle vulnerabilità note e del database di Windows Update. Questo database di vulnerabilità note viene creato e gestito dagli specialisti di Kaspersky. Contiene informazioni sulle vulnerabilità, come la descrizione della vulnerabilità, la data di rilevamento della vulnerabilità, il livello di criticità della vulnerabilità. Per informazioni dettagliate sulle vulnerabilità del software, visitare il sito Web di Kaspersky.

Kaspersky Security Center Cloud Console utilizza l'attività *Trova vulnerabilità e aggiornamenti richiesti* per rilevare le vulnerabilità del software.

Correzione delle vulnerabilità del software

Per correggere le vulnerabilità del software, Kaspersky Security Center Cloud Console utilizza gli aggiornamenti software rilasciati dai relativi fornitori. È possibile visualizzare l'elenco delle vulnerabilità del software in qualsiasi momento. I metadati degli aggiornamenti software vengono scaricati automaticamente nell'archivio di Administration Server e negli archivi dei punti di distribuzione a seguito dell'esecuzione dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*. È possibile creare questa attività tramite l'Avvio rapido guidato di Kaspersky Security Center Cloud Console o manualmente.

Gli aggiornamenti software per correggere le vulnerabilità possono essere rappresentati come patch o pacchetti o di distribuzione completi. Gli aggiornamenti software che correggono le vulnerabilità del software vengono denominati *correzioni*. In Kaspersky Security Center Cloud Console le vulnerabilità vengono corrette utilizzando le *correzioni consigliate*. Le correzioni consigliate sono gli aggiornamenti software consigliati per l'installazione dagli specialisti di Kaspersky.

A seconda della modalità di Kaspersky Security Center Cloud Console e della licenza corrente, è possibile utilizzare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità* per correggere le vulnerabilità del software.

L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* corregge automaticamente più vulnerabilità installando le correzioni consigliate. Per questa attività è possibile configurare manualmente determinate regole per correggere più vulnerabilità.

Tramite l'attività *Correggi vulnerabilità* è possibile correggere le vulnerabilità installando le correzioni consigliate per il software Microsoft.

Per motivi di sicurezza, tutti gli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management vengono automaticamente analizzati alla ricerca di malware dalle tecnologie Kaspersky. Queste tecnologie vengono utilizzate per il controllo automatico dei file e includono la scansione virus, l'analisi statica, l'analisi dinamica, l'analisi del comportamento nell'ambiente sandbox e il machine learning.

Gli esperti Kaspersky non eseguono l'analisi manuale degli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management. Inoltre, gli esperti di Kaspersky non ricercano vulnerabilità (note o sconosciute) o funzionalità non documentate in tali aggiornamenti, né eseguono altri tipi di analisi degli aggiornamenti diversi da quelli specificati nel paragrafo precedente.

Le attività di installazione degli aggiornamenti software prevedono una serie di limitazioni. Queste limitazioni dipendono dalla licenza con cui si utilizza Kaspersky Security Center Cloud Console e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Per correggere alcune vulnerabilità del software, è necessario accettare il Contratto di licenza con l'utente finale (EULA) per l'installazione del software, se è richiesta l'accettazione del Contratto di licenza con l'utente finale. Se non si accetta il Contratto di licenza con l'utente finale, la vulnerabilità del software non può essere corretta.

Le informazioni su ciascuna vulnerabilità corretta vengono archiviate nell'Administration Server per 90 giorni. Trascorso questo tempo, vengono automaticamente eliminate.

Correzione delle vulnerabilità del software

Dopo aver ottenuto l'elenco delle vulnerabilità del software, è possibile correggere le vulnerabilità del software nei dispositivi gestiti che eseguono Windows. È possibile correggere le vulnerabilità del software nel sistema operativo e nel software di terze parti, incluso il software Microsoft, creando ed eseguendo l'attività *Correggi vulnerabilità* o l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.

Le attività di installazione degli aggiornamenti software prevedono una serie di limitazioni. Queste limitazioni dipendono dalla licenza con cui si utilizza Kaspersky Security Center Cloud Console e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Facoltativamente, è possibile creare un'attività per correggere le vulnerabilità del software nei modi seguenti:

- Aprendo l'elenco delle vulnerabilità e specificando quali vulnerabilità correggere.

  Verrà creata una nuova attività per correggere le vulnerabilità del software. Facoltativamente è possibile aggiungere le vulnerabilità selezionate a un'attività esistente.

- Eseguendo la Correzione guidata vulnerabilità.

  La disponibilità di questa funzionalità dipende dalla modalità di Kaspersky Security Center Cloud Console e dalla licenza corrente.

  La procedura guidata semplifica la creazione e la configurazione di un'attività di correzione delle vulnerabilità e consente di eliminare la creazione di attività ridondanti che contengono gli stessi aggiornamenti da installare.

Correzione delle vulnerabilità del software tramite l'elenco delle vulnerabilità

Per correggere le vulnerabilità del software:

1. Aprire uno degli elenchi di vulnerabilità:

   - Per aprire l'elenco generale delle vulnerabilità nel menu principale, passare a **Operazioni** → **Gestione patch** → **Vulnerabilità del software**.

   - Per aprire l'elenco delle vulnerabilità per un dispositivo gestito nel menu principale, passare a **Risorse (dispositivi)** → **Dispositivi gestiti** → **<nome dispositivo>** → **Avanzate** → **Vulnerabilità del software**.

   - Per aprire l'elenco delle vulnerabilità per un'applicazione specifica nel menu principale, passare a **Operazioni** → **Applicazioni di terze parti** → **Registro delle applicazioni** → **<nome applicazione>** → **Vulnerabilità**.

   Verrà visualizzata una pagina con un elenco delle vulnerabilità nel software di terze parti.

2. Selezionare una o più vulnerabilità nell'elenco, quindi fare clic sul pulsante **Correggi vulnerabilità**.

   Se un aggiornamento software consigliato per correggere una delle vulnerabilità selezionate è assente, viene visualizzato un messaggio informativo.

   Per correggere alcune vulnerabilità del software, è necessario accettare il Contratto di licenza con l'utente finale (EULA) per l'installazione del software, se è richiesta l'accettazione del Contratto di licenza con l'utente finale. Se non si accetta il Contratto di licenza con l'utente finale, la vulnerabilità del software non viene corretta.

3. Selezionare una delle seguenti opzioni:

- **Nuova attività**

  Verrà avviata la Creazione guidata nuova attività. A seconda della modalità di Kaspersky Security Center Cloud Console e della licenza corrente, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità* è preselezionata. Seguire i passaggi della procedura guidata per completare la creazione dell'attività.

- **Correggi vulnerabilità (aggiungi regola all'attività specificata)**

  Selezionare un'attività a cui aggiungere le vulnerabilità selezionate. A seconda della modalità di Kaspersky Security Center Cloud Console e della licenza corrente, selezionare un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o un'attività *Correggi vulnerabilità*. Se si seleziona un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, una nuova regola per correggere le vulnerabilità selezionate verrà automaticamente aggiunta all'attività selezionata. Se si seleziona un'attività *Correggi vulnerabilità*, le vulnerabilità selezionate verranno aggiunte alle proprietà dell'attività.

  Verrà visualizzata la finestra delle proprietà dell'attività. Fare clic sul pulsante **Salva** per applicare le modifiche.

Se si è scelto di creare un'attività, l'attività viene creata e visualizzata nell'elenco delle attività in **Risorse (dispositivi)** → **Attività**. Se si è scelto di aggiungere le vulnerabilità a un'attività esistente, le vulnerabilità vengono salvate nelle proprietà dell'attività.

Per correggere le vulnerabilità del software di terze parti, avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità*. Se è stata creata l'attività *Correggi vulnerabilità*, è necessario specificare manualmente gli aggiornamenti software per correggere le vulnerabilità del software elencate nelle impostazioni dell'attività.

Correzione delle vulnerabilità del software tramite la Correzione guidata vulnerabilità

La disponibilità della Correzione guidata vulnerabilità dipende dalla licenza utilizzata e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

Per correggere le vulnerabilità del software utilizzando la Correzione guidata vulnerabilità:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Vulnerabilità del software**.

   Verrà visualizzata una pagina con un elenco delle vulnerabilità nel software di terze parti installato nei dispositivi gestiti.

2. Selezionare la casella di controllo accanto alla vulnerabilità da correggere.

3. Fare clic sul pulsante **Esegui Correzione guidata vulnerabilità**.

   Verrà avviata la Correzione guidata vulnerabilità. La pagina **Selezionare l'attività per la correzione della vulnerabilità** visualizza l'elenco di tutte le attività esistenti dei seguenti tipi:

   - *Installa aggiornamenti richiesti e correggi vulnerabilità*
   - *Installa aggiornamenti di Windows Update*
   - *Correggi vulnerabilità*

   Non è possibile modificare gli ultimi due tipi di attività per installare nuovi aggiornamenti. Per installare nuovi aggiornamenti, è possibile utilizzare solo l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.

4. Se si desidera che la procedura guidata visualizzi solo le attività per la correzione della vulnerabilità selezionata, abilitare l'opzione **Mostra solo le attività che consentono di correggere la vulnerabilità**.

5. Scegliere l'operazione da eseguire:

   - Per avviare un'attività, selezionare la casella di controllo accanto al nome dell'attività, quindi fare clic sul pulsante **Avvia**.

   - Per aggiungere una nuova regola a un'attività esistente:

     a. Selezionare la casella di controllo accanto al nome dell'attività, quindi fare clic sul pulsante **Aggiungi regola**.

     b. Nella pagina visualizzata configurare la nuova regola:

     - **Regola per la correzione delle vulnerabilità di questo livello di criticità**

       Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

       Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore alla criticità dell'aggiornamento selezionato (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

       Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

       Per impostazione predefinita, questa opzione è disabilitata.

     - **Regola per la correzione delle vulnerabilità tramite gli aggiornamenti dello stesso tipo dell'aggiornamento definito come consigliato per la vulnerabilità selezionata** (disponibile solo per le vulnerabilità del software Microsoft)

     - **Regola per la correzione delle vulnerabilità nelle applicazioni in base al fornitore selezionato** (disponibile solo per vulnerabilità del software di terze parti)

     - **Regola per la correzione di una vulnerabilità in tutte le versioni dell'applicazione selezionata** (disponibile solo per vulnerabilità software di terze parti)

     - **Regola per la correzione della vulnerabilità selezionata**

     - **Approva aggiornamenti in grado di correggere la vulnerabilità**

       L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

       Per impostazione predefinita, questa opzione è disabilitata.

     c. Fare clic sul pulsante **Aggiungi**.

   - Per creare un'attività:

     a. Fare clic sul pulsante **Nuova attività**.

b. Nella pagina visualizzata configurare la nuova regola:

- **Regola per la correzione delle vulnerabilità di questo livello di criticità**

  Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

  Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore alla criticità dell'aggiornamento selezionato (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

  Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Regola per la correzione delle vulnerabilità tramite gli aggiornamenti del tipo** (disponibile solo per le vulnerabilità del software Microsoft)
- **Regola per la correzione delle vulnerabilità nelle applicazioni in base al fornitore selezionato** (disponibile solo per vulnerabilità del software di terze parti)
- **Regola per la correzione di una vulnerabilità in tutte le versioni dell'applicazione selezionata** (disponibile solo per vulnerabilità software di terze parti)
- **Regola per la correzione della vulnerabilità selezionata**
- **Approva aggiornamenti in grado di correggere la vulnerabilità**

  L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

  Per impostazione predefinita, questa opzione è disabilitata.

c. Fare clic sul pulsante **Aggiungi**.

Se è stato scelto di avviare un'attività, è possibile chiudere la procedura guidata. L'attività verrà completata in background. Non sono necessarie ulteriori operazioni.

Se si è scelto di aggiungere una regola a un'attività esistente, verrà visualizzata la finestra delle proprietà dell'attività. La nuova regola è già stata aggiunta alle proprietà dell'attività. È possibile visualizzare o modificare la regola o altre impostazioni dell'attività. Fare clic sul pulsante **Salva** per applicare le modifiche.

Se è stato scelto di creare un'attività, continuare a creare l'attività nella Creazione guidata nuova attività. La nuova regola aggiunta nella Correzione guidata vulnerabilità viene visualizzata nella Creazione guidata nuova attività. Al termine della Creazione guidata nuova attività, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* verrà aggiunta all'elenco delle attività.

Creazione dell'attività Correggi vulnerabilità

L'attività *Correggi vulnerabilità* consente di correggere le vulnerabilità del software Microsoft nei dispositivi gestiti che eseguono Windows.

La disponibilità di questa funzionalità dipende dalla modalità di Kaspersky Security Center Cloud Console e dalla licenza corrente. È consigliabile utilizzare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* anziché l'attività *Correggi vulnerabilità*. L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* consente di installare automaticamente più aggiornamenti e correggere più vulnerabilità, in base alle regole definite.

Le attività di installazione degli aggiornamenti software prevedono una serie di limitazioni. Queste limitazioni dipendono dalla licenza con cui si utilizza Kaspersky Security Center Cloud Console e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Per creare l'attività Correggi vulnerabilità:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Per l'applicazione Kaspersky Security Center Cloud Console, selezionare il tipo di attività **Correggi vulnerabilità**.
4. Specificare il nome dell'attività che si intende creare.

   Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare i dispositivi a cui assegnare l'attività.
6. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzato l'elenco delle vulnerabilità.
7. Selezionare le vulnerabilità che si desidera correggere, quindi fare clic su **OK**.
8. Specificare le impostazioni per il riavvio del sistema operativo:

   - **Non riavviare il dispositivo**

     I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

   - **Riavvia il dispositivo**

     I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

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

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ripeti la richiesta ogni (min.)**

  Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

  Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

- **Riavvia dopo (min.)**

  Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

  Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

  L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

  Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

  Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

  Per impostazione predefinita, questa opzione è disabilitata.

9. Specificare le impostazioni per l'account:

- **Account predefinito**

  L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

  Per impostazione predefinita, questa opzione è selezionata.

- **Specifica account**

  Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

- **Account**

  Account tramite il quale viene eseguita l'attività.

- **Password**

  Password dell'account con cui verrà eseguita l'attività.

10. Se nella pagina **Completa creazione attività** si abilita l'opzione **Apri i dettagli dell'attività al termine della creazione**, è possibile modificare le impostazioni predefinite dell'attività. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

11. Fare clic sul pulsante **Fine**.

    L'attività verrà creata e visualizzata nell'elenco delle attività.

12. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

13. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

14. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità

La disponibilità dell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* dipende dalla modalità di Kaspersky Security Center Cloud Console e dalla licenza corrente.

L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per aggiornare e correggere le vulnerabilità nel software di terze parti, incluso il software Microsoft, installato nei dispositivi gestiti. Questa attività consente di installare più aggiornamenti e correggere più vulnerabilità in base a determinate regole.

Per installare aggiornamenti o correggere vulnerabilità utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile effettuare una delle seguenti operazioni:

- Eseguire l'Installazione guidata aggiornamenti o la Correzione guidata vulnerabilità.
- Creare un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.
- Aggiungere una regola per l'installazione dell'aggiornamento a un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* esistente.

Le attività di installazione degli aggiornamenti software prevedono una serie di limitazioni. Queste limitazioni dipendono dalla licenza con cui si utilizza Kaspersky Security Center Cloud Console e dalla modalità di esecuzione di Kaspersky Security Center Cloud Console.

Per creare un'attività Installa aggiornamenti richiesti e correggi vulnerabilità:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center Cloud Console, selezionare il tipo di attività **Installa aggiornamenti richiesti e correggi vulnerabilità**.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare i dispositivi a cui assegnare l'attività.
6. Specificare le regole per l'installazione dell'aggiornamento, quindi specificare le seguenti impostazioni:

   - **Avvia l'installazione al riavvio o all'arresto del dispositivo**

     Se questa opzione è abilitata, gli aggiornamenti vengono installati al riavvio o all'arresto del dispositivo. In caso contrario, gli aggiornamenti vengono installati in base a una pianificazione.

     Utilizzare questa opzione se l'installazione degli aggiornamenti può influire sulle prestazioni del dispositivo.

     Per impostazione predefinita, questa opzione è disabilitata.

   - **Installa i componenti generali del sistema richiesti**

     Se questa opzione è abilitata, prima di installare un aggiornamento l'applicazione installa automaticamente tutti i componenti di sistema generali (prerequisiti) richiesti per installare l'aggiornamento. Questi prerequisiti possono ad esempio essere aggiornamenti del sistema operativo.

     Se questa opzione è disabilitata, può essere necessario installare manualmente i prerequisiti.

     Per impostazione predefinita, questa opzione è disabilitata.

   - **Consenti l'installazione di nuove versioni dell'applicazione durante gli aggiornamenti**

     Se questa opzione è abilitata, gli aggiornamenti sono consentiti se implicano l'installazione di una nuova versione di un'applicazione software.

     Se questa opzione è disabilitata, l'upgrade del software non viene eseguito. È quindi possibile installare le nuove versioni del software manualmente o tramite un'altra attività. È ad esempio possibile utilizzare questa opzione se l'infrastruttura aziendale non è supportata da una nuova versione del software o se si desidera verificare un aggiornamento in un'infrastruttura di test.

     Per impostazione predefinita, questa opzione è abilitata.

     L'upgrade dell'applicazione può causare un malfunzionamento delle applicazioni dipendenti installate nei dispositivi client.

   - **Scarica gli aggiornamenti nel dispositivo senza installarli**

Se questa opzione è abilitata, l'applicazione scarica gli aggiornamenti nel dispositivo client ma non li installa automaticamente. È quindi possibile installare manualmente gli aggiornamenti scaricati.

Gli aggiornamenti Microsoft vengono scaricati nell'archiviazione di sistema di Windows. Gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) vengono scaricati nella cartella specificata nel campo **Scarica aggiornamenti in**.

Se questa opzione è disabilitata, gli aggiornamenti vengono installati automaticamente nel dispositivo.

Per impostazione predefinita, questa opzione è disabilitata.

- **Cartella per il download degli aggiornamenti**

  Questa cartella viene utilizzata per scaricare gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft).

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive le tracce anche se il tracciamento è disabilitato per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center Cloud Console. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center Cloud Console. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

7. Specificare le impostazioni per il riavvio del sistema operativo:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

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

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ripeti la richiesta ogni (min.)**

  Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

  Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

- **Riavvia dopo (min.)**

  Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

  Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Tempo di attesa prima della chiusura forzata delle applicazioni nelle sessioni bloccate (min.)**

  Viene forzata la chiusura delle applicazioni quando il dispositivo dell'utente viene bloccato (automaticamente dopo un intervallo di inattività specificato o manualmente).

  Se questa opzione è abilitata, viene forzata la chiusura delle applicazioni nel dispositivo bloccato alla scadenza dell'intervallo di tempo specificato nel campo di immissione.

  Se questa opzione è disabilitata, le applicazioni nel dispositivo bloccato non vengono chiuse.

  Per impostazione predefinita, questa opzione è disabilitata.

8. Se nella pagina **Completa creazione attività** si abilita l'opzione **Apri i dettagli dell'attività al termine della creazione**, è possibile modificare le impostazioni predefinite dell'attività. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

9. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.

10. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

11. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

12. Fare clic sul pulsante **Salva**.

    L'attività verrà creata e configurata.

Se i risultati dell'attività contengono l'avviso 0x80240033 "Errore di Windows Update Agent 80240033 ("Non è stato possibile scaricare le condizioni di licenza")", è possibile risolvere questo problema tramite il Registro di sistema di Windows.

Aggiunta delle regole per l'installazione dell'aggiornamento

La disponibilità di questa funzionalità dipende dalla modalità di Kaspersky Security Center Cloud Console e dalla licenza corrente.

Durante l'installazione di aggiornamenti software o la correzione di vulnerabilità del software tramite l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è necessario specificare le regole per l'installazione degli aggiornamenti. Queste regole determinano gli aggiornamenti da installare e le vulnerabilità da correggere.

Le esatte impostazioni dipendono dall'esigenza di aggiungere una regola per tutti gli aggiornamenti, per gli aggiornamenti di Windows Update o per gli aggiornamenti di applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft). Durante l'aggiunta di una regola per gli aggiornamenti di Windows Update o per gli aggiornamenti di applicazioni di terze parti, è possibile selezionare le specifiche applicazioni e versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Durante l'aggiunta di una regola per tutti gli aggiornamenti, è possibile selezionare gli specifici aggiornamenti da installare e le vulnerabilità che si desidera correggere tramite l'installazione degli aggiornamenti.

È possibile aggiungere una regola per l'installazione degli aggiornamenti nei modi seguenti:

- Aggiungendo una regola durante la creazione di una nuova attività Installa aggiornamenti richiesti e correggi vulnerabilità.
- Aggiungendo una regola nella scheda **Impostazioni applicazione** nella finestra delle proprietà di un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* esistente.
- Tramite l'Installazione guidata aggiornamenti o la Correzione guidata vulnerabilità.

Per aggiungere una nuova regola per tutti gli aggiornamenti:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per tutti gli aggiornamenti**.

3. Nella pagina **Criteri generali** utilizzare gli elenchi a discesa per specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

- **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
- **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
- **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

- **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

  Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

  Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

  Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

  Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Aggiornamenti** selezionare gli aggiornamenti da installare:

- **Installa tutti gli aggiornamenti appropriati**

  Installa tutti gli aggiornamenti software che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

- **Installa solo gli aggiornamenti nell'elenco**

  Installa solo gli aggiornamenti software che selezionati manualmente dall'elenco. Questo elenco contiene tutti gli aggiornamenti software disponibili.

  Ad esempio, è possibile selezionare aggiornamenti specifici nei seguenti casi: per verificarne l'installazione in un ambiente di test, per aggiornare solo le applicazioni critiche o per aggiornare solo specifiche applicazioni.

- **Installa automaticamente tutti gli aggiornamenti precedenti dell'applicazione necessari per l'installazione degli aggiornamenti selezionati**

Mantenere abilitata questa opzione se si desidera consentire l'installazione delle versioni intermedie delle applicazioni quando questa operazione è necessaria per l'installazione degli aggiornamenti selezionati.

Se questa opzione è disabilitata, vengono installate solo le versioni delle applicazioni selezionate. Disabilitare questa opzione se si desidera aggiornare le applicazioni in modo diretto, senza tentare di installare le versioni successive in modo incrementale. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

Si supponga di avere la versione 3 di un'applicazione installata in un dispositivo e di voler eseguire l'aggiornamento alla versione 5, ma la versione 5 di questa applicazione può essere installata solo sulla versione 4. Se questa opzione è abilitata, il software installa prima la versione 4 e quindi la versione 5. Se questa opzione è disabilitata, il software non riesce a eseguire l'aggiornamento l'applicazione.

Per impostazione predefinita, questa opzione è abilitata.

5. Nella pagina **Vulnerabilità** selezionare le vulnerabilità da correggere tramite l'installazione degli aggiornamenti selezionati:

   - **Correggi tutte le vulnerabilità che corrispondono ad altri criteri**

     Verranno corrette tutte le vulnerabilità che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

   - **Correggi solo le vulnerabilità nell'elenco**

     Verranno corrette solo le vulnerabilità selezionate manualmente dall'elenco. Questo elenco contiene tutte le vulnerabilità rilevate.

     Ad esempio, è possibile selezionare vulnerabilità specifiche nei seguenti casi: per verificarne la correzione in un ambiente di test, per correggere solo le vulnerabilità di applicazioni critiche o per correggere le vulnerabilità solo in specifiche applicazioni.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Per aggiungere una nuova regola per gli aggiornamenti di Windows Update:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per Windows Update**.

3. Nella finestra **Criteri generali** specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

- **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
- **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
- **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

- Correggi le vulnerabilità con un livello di criticità uguale o superiore a

  Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

  Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

  Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

  Per impostazione predefinita, questa opzione è disabilitata.

- Correggi le vulnerabilità con un livello di criticità MSRC uguale o superiore a

  Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

  Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Microsoft Security Response Center (MSRC) è uguale o superiore al valore selezionato nell'elenco (**Basso**, **Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

  Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

  Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Categorie di aggiornamenti** selezionare le categorie di aggiornamenti da installare. Queste categorie sono identiche a quelle del catalogo di Microsoft Update. Per impostazione predefinita, tutte le categorie sono selezionate.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Per aggiungere una nuova regola per gli aggiornamenti delle applicazioni di terze parti:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per gli aggiornamenti di terze parti**.

3. Nella finestra **Criteri generali** specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione Impostazioni della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Visualizzazione delle informazioni sulle vulnerabilità del software rilevate in tutti i dispositivi gestiti

Dopo aver eseguito la scansione del software nei dispositivi gestiti per individuare eventuali vulnerabilità, è possibile visualizzare l'elenco delle vulnerabilità del software rilevate in tutti i dispositivi gestiti.

Per visualizzare l'elenco delle vulnerabilità del software rilevate in tutti i dispositivi gestiti:

Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Vulnerabilità del software**.

La pagina visualizzerà l'elenco delle vulnerabilità del software rilevate nei dispositivi client.

È anche possibile generare e visualizzare il Rapporto sulle vulnerabilità.

È possibile specificare un filtro per visualizzare l'elenco delle vulnerabilità del software. Fare clic sull'icona **Filtro** ( ) nell'angolo superiore destro dell'elenco delle vulnerabilità del software per gestire il filtro. È anche possibile selezionare uno dei filtri preimpostati dall'elenco a discesa **Filtri preimpostati** sopra l'elenco delle vulnerabilità del software.

È possibile ottenere informazioni dettagliate su qualsiasi vulnerabilità nell'elenco.

Per ottenere informazioni su una vulnerabilità del software:

Nell'elenco delle vulnerabilità del software fare clic sul collegamento con il nome della vulnerabilità.

Verrà visualizzata la finestra delle proprietà della vulnerabilità del software.

Visualizzazione delle informazioni sulle vulnerabilità del software rilevate nel dispositivo gestito selezionato

È possibile visualizzare le informazioni sulle vulnerabilità del software rilevate nel dispositivo gestito selezionato che esegue Windows.

Per visualizzare un elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato:

1. Nel menu principale, accedere a **Risorse (dispositivi)** →**Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo per cui si desidera visualizzare le vulnerabilità del software rilevate.

   Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.

3. Nella finestra delle proprietà del dispositivo selezionato selezionare la scheda **Avanzate**.

4. Nel riquadro sinistro selezionare la sezione **Vulnerabilità del software**.

   Se si desidera visualizzare solo le vulnerabilità del software che è possibile correggere, selezionare l'opzione **Mostra solo le vulnerabilità che possono essere risolte.**

Verrà visualizzato l'elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato.

Per visualizzare le proprietà della vulnerabilità del software selezionata:

Fare clic sul collegamento con il nome della vulnerabilità del software nell'elenco delle vulnerabilità del software.

Verrà visualizzata la finestra delle proprietà della vulnerabilità del software selezionata.

Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti

È possibile visualizzare le statistiche per ogni vulnerabilità del software nei dispositivi gestiti. Le statistiche sono rappresentate sotto forma di diagramma. Il diagramma mostra il numero di dispositivi con i seguenti stati:

- *Ignorato in: <numero di dispositivi>*. Lo stato viene assegnato se, nelle proprietà della vulnerabilità, è stata impostata manualmente l'opzione per ignorare la vulnerabilità.
- *Corretto in: <numero di dispositivi>*. Lo stato viene assegnato se l'attività di correzione della vulnerabilità è stata completata.
- *Correzione pianificata in data: <numero di dispositivi>*. Lo stato viene assegnato se è stata creata l'attività per correggere la vulnerabilità ma l'attività non è ancora stata eseguita.
- *Patch applicata in: <numero di dispositivi>*. Lo stato viene assegnato se è stato selezionato manualmente un aggiornamento software per correggere la vulnerabilità ma questo software aggiornato non ha corretto la vulnerabilità.
- *È necessaria una correzione in: <numero di dispositivi>*. Lo stato viene assegnato se la vulnerabilità è stata corretta solo in una parte dei dispositivi gestiti e deve essere corretta nella parte restante dei dispositivi gestiti.

Per visualizzare le statistiche di una vulnerabilità nei dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni → Gestione patch → Vulnerabilità del software**.

   La pagina visualizza un elenco delle vulnerabilità nelle applicazioni rilevate nei dispositivi gestiti.

2. Selezionare la casella di controllo accanto alla vulnerabilità richiesta.
3. Fare clic sul pulsante **Statistiche di vulnerabilità nei dispositivi**

Verrà visualizzato un diagramma degli stati della vulnerabilità. Facendo clic su uno stato, viene aperto un elenco dei dispositivi in cui la vulnerabilità ha lo stato selezionato.

Esportazione dell'elenco delle vulnerabilità del software in un file

È possibile esportare l'elenco visualizzato delle vulnerabilità in file CSV o TXT. È ad esempio possibile utilizzare questi file per inviarli al responsabile della sicurezza delle informazioni o per archiviarli a fini statistici.

Per esportare in un file di testo l'elenco delle vulnerabilità del software rilevate in tutti i dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni → Gestione patch → Vulnerabilità del software**.

   La pagina visualizza un elenco delle vulnerabilità nelle applicazioni rilevate nei dispositivi gestiti.

2. Fare clic sul pulsante **Esporta in TXT** o **Esporta in CSV**, a seconda del formato preferito per l'esportazione.

Il file contenente l'elenco delle vulnerabilità del software verrà scaricato nel dispositivo in uso.

Per esportare in un file di testo l'elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato:

1. Aprire l'elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato.
2. Selezionare le vulnerabilità del software che si desidera esportare.

   Ignorare questo passaggio se si desidera esportare un elenco completo delle vulnerabilità del software rilevate nel dispositivo gestito.

Se si desidera esportare l'elenco completo delle vulnerabilità del software rilevate nel dispositivo gestito, verranno esportate solo le vulnerabilità visualizzate nella pagina corrente.

3. Fare clic sul pulsante **Esporta in TXT** o **Esporta in CSV**, a seconda del formato preferito per l'esportazione.

Il file contenente l'elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato verrà scaricato nel dispositivo in uso.

Ignorare le vulnerabilità del software

È possibile ignorare le vulnerabilità del software da correggere. I motivi per ignorare le vulnerabilità del software potrebbero essere, ad esempio, i seguenti:

- La vulnerabilità del software non viene considerata critica per l'organizzazione.
- Si ritiene che la correzione della vulnerabilità del software possa danneggiare i dati relativi al software per cui era necessaria la correzione della vulnerabilità.
- Si ha la certezza che la vulnerabilità del software non sia pericolosa per la rete dell'organizzazione in quanto si utilizzano altre misure per proteggere i dispositivi gestiti.

È possibile ignorare una vulnerabilità del software in tutti i dispositivi gestiti o solo nei dispositivi gestiti selezionati.

Per ignorare una vulnerabilità del software in tutti i dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Vulnerabilità del software**.

   La pagina visualizzerà l'elenco delle vulnerabilità del software rilevate nei dispositivi gestiti.

2. Nell'elenco delle vulnerabilità del software fare clic sul collegamento con il nome della vulnerabilità del software che si desidera ignorare.

   Verrà visualizzata la finestra delle proprietà delle vulnerabilità del software.

3. Nella scheda **Generale** abilitare l'opzione **Ignora vulnerabilità**.

4. Fare clic sul pulsante **Salva**.

   Verrà chiusa la finestra delle proprietà delle vulnerabilità del software.

La vulnerabilità del software viene ignorata in tutti i dispositivi gestiti.

Per ignorare una vulnerabilità del software nel dispositivo gestito selezionato:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo in cui si desidera ignorare una vulnerabilità del software.

   Verrà visualizzata la finestra delle proprietà del dispositivo.

3. Nella finestra delle proprietà del dispositivo selezionare la scheda **Avanzate**.

4. Nel riquadro sinistro selezionare la sezione **Vulnerabilità del software**.

Verrà visualizzato l'elenco delle vulnerabilità del software rilevate nel dispositivo.

5. Nell'elenco delle vulnerabilità del software selezionare la vulnerabilità che si desidera ignorare nel dispositivo selezionato.

   Verrà visualizzata la finestra delle proprietà delle vulnerabilità del software.

6. Nella finestra delle proprietà della vulnerabilità del software, nella scheda **Generale**, abilitare l'opzione **Ignora vulnerabilità**.

7. Fare clic sul pulsante **Salva**.

   Verrà chiusa la finestra delle proprietà delle vulnerabilità del software.

8. Chiudere la finestra delle proprietà del dispositivo.

La vulnerabilità del software viene ignorata nel dispositivo selezionato.

La vulnerabilità del software ignorata non verrà corretta dopo il completamento dell'attività *Correggi vulnerabilità* o dell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. È possibile escludere le vulnerabilità del software ignorate dall'elenco delle vulnerabilità mediante il filtro.

Impostazione del periodo di archiviazione massimo per le informazioni sulle vulnerabilità corrette

Per impostare il periodo di archiviazione massimo nel database per le informazioni sulle vulnerabilità già corrette nei dispositivi gestiti:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella pagina visualizzata, passare alla scheda **Archivio eventi**.

3. Specificare il periodo di archiviazione massimo per le informazioni sulle vulnerabilità corrette nel database.

   Per impostazione predefinita, il periodo di archiviazione è di 7 giorni nella modalità di prova e 60 giorni nella modalità commerciale. Il limite massimo è di 14 giorni nella modalità di prova e 365 giorni nella modalità commerciale.

4. Fare clic su **Salva**.

Il periodo di archiviazione massimo per le informazioni sulle vulnerabilità corrette si limita al numero di giorni specificato.

Gestione delle applicazioni in esecuzione nei dispositivi client

Questa sezione descrive le funzionalità di Kaspersky Security Center Cloud Console relative alla gestione delle applicazioni eseguite nei dispositivi client.

Scenario: Gestione applicazioni

È possibile gestire l'avvio delle applicazioni nei dispositivi client. È possibile consentire o bloccare l'esecuzione delle applicazioni nei dispositivi gestiti. Questa funzionalità è resa possibile dal componente Controllo Applicazioni. È possibile gestire le applicazioni installate nei dispositivi Windows o Linux.

Per i sistemi operativi basati su Linux, il componente Controllo Applicazioni è disponibile a partire da Kaspersky Endpoint Security 11.2 for Linux.

Prerequisiti

- Kaspersky Security Center Cloud Console viene distribuito nell'organizzazione.
- Il criterio di Kaspersky Endpoint Security for Windows o Kaspersky Endpoint Security for Linux è stato creato ed è attivo.

Passaggi

Lo scenario di utilizzo di Controllo Applicazioni prevede diversi passaggi:

1. **Creazione e visualizzazione dell'elenco delle applicazioni nei dispositivi client**

   Questo passaggio consente di scoprire quali applicazioni sono installate nei dispositivi gestiti. È possibile visualizzare l'elenco delle applicazioni e decidere quali applicazioni consentire e quali non consentire, in base ai criteri di sicurezza dell'organizzazione. Le restrizioni possono essere correlate ai criteri di sicurezza delle informazioni dell'organizzazione. È possibile ignorare questo passaggio se si sa esattamente quali applicazioni sono installate nei dispositivi gestiti.

   Istruzioni dettagliate: Recupero e visualizzazione di un elenco delle applicazioni installate nei dispositivi client

2. **Creazione e visualizzazione dell'elenco dei file eseguibili nei dispositivi client**

   Questo passaggio consente di scoprire quali file eseguibili sono presenti nei dispositivi gestiti. Visualizzare l'elenco dei file eseguibili e confrontarlo con l'elenco dei file eseguibili consentiti e non consentiti. Le restrizioni relative all'utilizzo dei file eseguibili possono essere correlate ai criteri di sicurezza delle informazioni dell'organizzazione. È possibile ignorare questo passaggio se si sa esattamente quali file eseguibili sono presenti nei dispositivi gestiti.

   Istruzioni dettagliate: Recupero e visualizzazione di un elenco dei file eseguibili installati nei dispositivi client

3. **Creazione delle categorie di applicazioni per le applicazioni utilizzate nell'organizzazione**

   Analizzare gli elenchi delle applicazioni e dei file eseguibili archiviati nei dispositivi gestiti. In base all'analisi, creare le categorie di applicazioni. È consigliabile creare una categoria "Applicazioni di lavoro" che includa il set standard di applicazioni utilizzate nell'organizzazione. Se differenti gruppi di sicurezza utilizzano diversi set di applicazioni nel proprio lavoro, è possibile creare una categoria di applicazioni distinta per ciascun gruppo di sicurezza.

   A seconda del set di criteri per la creazione di una categoria di applicazioni, è possibile creare due tipi di categorie di applicazioni.

   Istruzioni dettagliate: Creazione di una categoria di applicazioni con contenuto aggiunto manualmente, Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati

4. **Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows**

Configurare il componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows utilizzando le categorie di applicazioni create nel passaggio precedente.

Istruzioni dettagliate: Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

5. **Attivazione del componente Controllo Applicazioni in modalità di test**

   Per garantire che le regole di Controllo Applicazioni non blocchino le applicazioni richieste per il lavoro dell'utente, è consigliabile abilitare il test delle regole di Controllo Applicazioni e analizzarne il funzionamento dopo aver creato le nuove regole. Quando il test è abilitato, Kaspersky Endpoint Security for Windows non bloccherà le applicazioni il cui avvio non è consentito dalle regole di Controllo Applicazioni, ma invierà invece notifiche sul relativo avvio ad Administration Server.

   Durante il test delle regole di Controllo Applicazioni, è consigliabile eseguire le seguenti azioni:

   - Determinare il periodo di test. Il periodo di test può variare da alcuni giorni a due mesi.
   - Esaminare gli eventi risultanti dal test del funzionamento di Controllo Applicazioni.

   Istruzioni dettagliate: Configurazione del componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows. Seguire queste istruzioni e abilitare la modalità test nel processo di configurazione.

6. **Modifica delle impostazioni delle categorie di applicazioni del componente Controllo Applicazioni**

   Se necessario, apportare modifiche alle impostazioni di Controllo Applicazioni. In base ai risultati del test, è possibile aggiungere i file eseguibili correlati agli eventi del componente Controllo Applicazioni a una categoria di applicazioni con contenuto aggiunto manualmente.

   Istruzioni dettagliate: Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni

7. **Applicazione delle regole di Controllo Applicazioni in modalità operativa**

   Dopo aver testato le regole di Controllo Applicazioni e completato la configurazione delle categorie di applicazioni, è possibile applicare le regole di Controllo Applicazioni in modalità operativa.

   Istruzioni dettagliate: Configurazione del componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows. Seguire queste istruzioni e disabilitare la modalità test nel processo di configurazione.

8. **Verifica della configurazione di Controllo Applicazioni**

   Assicurarsi di quanto segue:

   - L'elenco delle categorie di applicazioni non è vuoto. Visualizzare l'elenco delle categorie di applicazioni e assicurarsi che contenga le categorie configurate.
   - Controllo Applicazioni è stato configurato utilizzando le categorie di applicazioni create. Visualizzare le impostazioni del criterio di Kaspersky Endpoint Security for Windows e assicurarsi di aver configurato Controllo Applicazioni in **Impostazioni applicazione** → **Controlli di Sicurezza** → **Controllo Applicazioni**.
   - Le regole di Controllo Applicazioni vengono applicate in modalità operativa. Controllare la modalità nel criterio di Kaspersky Endpoint Security for Windows e assicurarsi di aver disabilitato la **Modalità di test** in **Impostazioni applicazione** → **Controlli di Sicurezza** → **Controllo Applicazioni**.

Risultati

Al termine dello scenario, viene controllato l'avvio delle applicazioni nei dispositivi gestiti. Gli utenti possono avviare solo le applicazioni consentite nell'organizzazione, mentre non possono avviare quelle non consentite.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux

Informazioni su Controllo Applicazioni

Il componente Controllo Applicazioni monitora i tentativi degli utenti di avviare le applicazioni e regola l'avvio delle applicazioni tramite le regole di Controllo Applicazioni.

Il componente Controllo Applicazioni è disponibile per Kaspersky Endpoint Security for Windows e per Kaspersky Endpoint Security for Linux (versione 11.2 e successive). Tutte le istruzioni in questa sezione descrivono la configurazione di Controllo Applicazioni per Kaspersky Endpoint Security.

L'avvio delle applicazioni le cui impostazioni non corrispondono ad alcuna delle regole di Controllo Applicazioni è regolato dalla modalità operativa selezionata del componente:

- *Lista vietati*. La modalità viene utilizzata se si desidera consentire l'avvio di tutte le applicazioni tranne quelle specificate nelle regole di blocco. La modalità *Lista vietati* è selezionata per impostazione predefinita.
- *Lista consentiti*. La modalità viene utilizzata se si desidera bloccare l'avvio di tutte le applicazioni tranne quelle specificate nelle regole di permesso.

Le regole di Controllo Applicazioni sono implementate attraverso categorie di applicazioni. Le categorie di applicazioni vengono create definendo criteri specifici. In Kaspersky Security Center Cloud Console esistono due tipi di categorie di applicazioni:

- Categoria con contenuto aggiunto manualmente. Vengono definite le condizioni (ad esempio, metadati del file, codice hash del file, certificato del file, categoria KL o percorso del file) per includere i file eseguibili nella categoria.
- Categoria che include i file eseguibili dei dispositivi selezionati. Viene specificato un dispositivo che contiene i file eseguibili inclusi automaticamente nella categoria.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux

Recupero e visualizzazione di un elenco delle applicazioni installate nei dispositivi client

Kaspersky Security Center Cloud Console esegue l'inventario di tutto il software installato nei dispositivi client gestiti che eseguono Linux e Windows.

Network Agent compila un elenco delle applicazioni installate in un dispositivo, quindi trasmette questo elenco ad Administration Server. Sono necessari circa 10-15 minuti affinché Network Agent aggiorni l'elenco delle applicazioni.

Per i dispositivi client basati su Windows, Network Agent riceve la maggior parte delle informazioni sulle applicazioni installate dal Registro di sistema di Windows. Per i dispositivi client basati su Linux, gli strumenti di gestione di pacchetti forniscono informazioni sulle applicazioni installate a Network Agent.

Per visualizzare l'elenco delle applicazioni installate nei dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Registro delle applicazioni**.

   Nella pagina viene visualizzata una tabella con le applicazioni installate nei dispositivi gestiti. Selezionare l'applicazione per visualizzarne le proprietà, ad esempio il nome del fornitore, il numero di versione, l'elenco dei file eseguibili, l'elenco dei dispositivi in cui è installata l'applicazione, l'elenco degli aggiornamenti software disponibili e l'elenco delle vulnerabilità del software rilevate.

2. È possibile raggruppare e filtrare i dati della tabella con le applicazioni installate come segue:

   - Fare clic sull'icona delle impostazioni ( ) nell'angolo superiore destro della tabella.

     Nel menu **Impostazioni colonne** richiamato, selezionare le colonne da visualizzare nella tabella. Per visualizzare il tipo di sistema operativo dei dispositivi client in cui è installata l'applicazione, selezionare la colonna **Tipo di sistema operativo**.

   - Fare clic sull'icona del filtro ( ) nell'angolo superiore destro della tabella, quindi specificare e applicare il criterio di filtro nel menu richiamato.

     Viene visualizzata la tabella filtrata delle applicazioni installate.

Per visualizzare l'elenco delle applicazioni installate in un dispositivo gestito specifico:

Nel menu principale accedere a **Dispositivi → Dispositivi gestiti → <nome dispositivo> → Avanzate → Registro delle applicazioni**. In questo menu, è possibile esportare l'elenco delle applicazioni in un file CSV o TXT.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux

Recupero e visualizzazione di un elenco dei file eseguibili installati nei dispositivi client

È possibile ottenere un elenco dei file eseguibili installati nei dispositivi gestiti. Per eseguire un inventario dei file eseguibili, è necessario creare un'attività di inventario.

La funzione di inventario dei file eseguibili è disponibile per le seguenti applicazioni:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux (versione 11.2 e successive)

È possibile ridurre il carico sul database mentre si ottengono informazioni sulle applicazioni installate. A tale scopo, si consiglia di eseguire un'attività di inventario sui dispositivi di riferimento in cui è installato un set standard di software.

Per creare un'attività di inventario per i file eseguibili nei dispositivi client:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

   Verrà visualizzato l'elenco delle attività.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

3. Nella pagina **Nuova attività**, nell'elenco a discesa **Applicazione**, selezionare Kaspersky Endpoint Security for Windows o Kaspersky Endpoint Security for Linux, a seconda del tipo di sistema operativo dei dispositivi client.

4. Nell'elenco a discesa **Tipo di attività** selezionare **Inventario**.

5. Nella pagina **Completa creazione attività** fare clic sul pulsante **Fine**.

   Al termine della Creazione guidata nuova attività, l'attività **Inventario** viene creata e configurata. Se si desidera, è possibile modificare le impostazioni per l'attività creata. La nuova attività creata verrà visualizzata nell'elenco delle attività.

Per una descrizione dettagliata dell'attività di inventario, fare riferimento alle seguenti Guide:

- Guida di Kaspersky Endpoint Security for Windows
- Guida di Kaspersky Endpoint Security for Linux

Dopo l'esecuzione dell'attività **Inventario**, viene formato l'elenco dei file eseguibili installati nei dispositivi gestiti ed è possibile visualizzarlo.

Durante l'inventario, vengono rilevati i seguenti formati di file eseguibili: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Per visualizzare l'elenco dei file eseguibili archiviati nei dispositivi client,

Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **File eseguibili**.

La pagina visualizzerà l'elenco dei file eseguibili installati nei dispositivi client.

È inoltre possibile inviare il file eseguibile da un dispositivo gestito a Kaspersky, per verificare la presenza di potenziali minacce.

Per inviare il file eseguibile del dispositivo gestito a Kaspersky:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **File eseguibili**.

2. Fare clic sul collegamento del file eseguibile che si desidera inviare a Kaspersky.

3. Nella finestra visualizzata, accedere alla sezione **Dispositivi**, quindi selezionare la casella di controllo del dispositivo gestito da cui si desidera inviare il file eseguibile.

   Prima di inviare il file eseguibile, assicurarsi che il dispositivo gestito disponga di una connessione diretta ad Administration Server selezionando la casella di controllo **Non eseguire la disconnessione da Administration Server**. Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

4. Fare clic sul pulsante **Invia a Kaspersky**.

Il file eseguibile selezionato viene scaricato per un ulteriore invio a Kaspersky.

Creazione di una categoria di applicazioni con contenuto aggiunto manualmente

È possibile specificare un set di criteri come modello per i file eseguibili di cui consentire o bloccare l'avvio nell'organizzazione. In base ai file eseguibili corrispondenti ai criteri, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per creare una categoria di applicazioni con contenuto aggiunto manualmente:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Categorie di applicazioni**.

   Verrà visualizzata la pagina con un elenco di categorie di applicazioni.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova categoria. Seguire le istruzioni della procedura guidata.

3. Nella pagina **Selezionare il metodo di creazione della categoria** della procedura guidata selezionare l'opzione **Categoria con contenuto aggiunto manualmente. I dati dei file eseguibili vengono aggiunti alla categoria in modo manuale**.

4. Nella pagina **Condizioni** della procedura guidata fare clic sul pulsante **Aggiungi** per aggiungere un criterio di condizione per includere i file nella creazione della categoria.

5. Nella pagina **Criteri condizione** selezionare un tipo di regola per la creazione della categoria dall'elenco:

   - **Da categoria KL**

     Se questa opzione è selezionata, è possibile specificare una categoria di applicazioni Kaspersky come condizione per l'aggiunta di applicazioni alla categoria utente. Le applicazioni della categoria Kaspersky specificata verranno aggiunte alla categoria utente di applicazioni.

   - **Seleziona certificato dall'archivio**

     Se questa opzione è selezionata, è possibile specificare i certificati dell'archivio. I file eseguibili firmati in base ai certificati specificati verranno aggiunti alla categoria utente.

   - **Specificare il percorso dell'applicazione (maschere supportate)**

     Se questa opzione è selezionata, è possibile specificare il percorso di una cartella nel dispositivo client che contiene i file eseguibili da aggiungere alla categoria utente di applicazioni.

   - **Unità rimovibile**

     Se questa opzione è selezionata, è possibile specificare il tipo di supporto (qualsiasi unità o unità rimovibile) in cui viene eseguita l'applicazione. Le applicazioni che sono state eseguite nel tipo di unità selezionato verranno aggiunte alla categoria utente di applicazioni.

- **Hash, metadati o certificato**:
  - Selezionare dall'elenco dei file eseguibili

    Se questa opzione è selezionata, è possibile utilizzare l'elenco dei file eseguibili nel dispositivo client per selezionare e aggiungere applicazioni alla categoria.

  - Selezionare dal registro delle applicazioni

    Se questa opzione è selezionata, viene visualizzato il registro delle applicazioni. È possibile selezionare un'applicazione dal registro e specificare i seguenti metadati dei file:

    - Nome file.
    - Versione file. È possibile specificare un valore preciso per la versione o descrivere una condizione, ad esempio "maggiore di 5.0".
    - Nome applicazione.
    - Versione applicazione. È possibile specificare un valore preciso per la versione o descrivere una condizione, ad esempio "maggiore di 5.0".
    - Vendor.

  - Specificare manualmente

Se questa opzione è selezionata, è necessario specificare l'hash del file, i metadati o un certificato come condizione per l'aggiunta di applicazioni alla categoria utente.

Hash del file

A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center Cloud Console per i file di questa categoria. Le informazioni sui valori hash calcolati vengono archiviate nel database di Administration Server. L'archiviazione dei valori hash non aumenta in modo significativo le dimensioni del database.

SHA-256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive supportano il calcolo di SHA-256. Il calcolo della funzione hash MD5 è supportato da tutte le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center Cloud Console per i file della categoria:

- Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive, selezionare la casella di controllo **SHA-256**. Non è consigliabile aggiungere categorie create in base al criterio dell'hash SHA-256 di un file eseguibile per le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Questo può generare errori durante l'esecuzione dell'applicazione di protezione. In questo caso, è possibile utilizzare la funzione hash di criptaggio MD5 per i file della categoria.

- Se nella rete sono installate versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, selezionare **Hash MD5**. Non è possibile aggiungere una categoria che è stata creata in base al criterio del checksum MD5 di un file eseguibile per Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive. In questo caso, è possibile utilizzare la funzione hash di criptaggio SHA-256 per i file della categoria.

- Se diversi dispositivi della rete utilizzano versioni precedenti e successive di Kaspersky Endpoint Security 10, selezionare sia la casella di controllo **SHA-256** che la casella di controllo **Hash MD5**.

Metadati

Se questa opzione è selezionata, è possibile specificare i metadati del file, come il nome del file, la versione del file o il fornitore. I metadati verranno inviati ad Administration Server. I file eseguibili che contengono gli stessi metadati verranno aggiunti alla categoria di applicazioni.

Certificato

Se questa opzione è selezionata, è possibile specificare i certificati dell'archivio. I file eseguibili firmati in base ai certificati specificati verranno aggiunti alla categoria utente.

- Da file o pacchetto MSI/cartella archiviata

Se questa opzione è selezionata, è possibile specificare il file di un programma di installazione MSI come condizione per l'aggiunta di applicazioni alla categoria utente. I metadati del programma di installazione dell'applicazione verranno inviati ad Administration Server. Le applicazioni per cui i metadati del programma di installazione corrispondono a quelli del programma di installazione MSI specificato verranno aggiunte alla categoria utente di applicazioni.

Il criterio selezionato viene aggiunto all'elenco delle condizioni.

È possibile aggiungere tutti i criteri necessari per la creazione della categoria di applicazioni.

6. Nella pagina **Esclusioni** della procedura guidata fare clic sul pulsante **Aggiungi** per aggiungere un criterio di condizione esclusivo per escludere i file dalla categoria creata.

7. Nella pagina **Criteri condizione** selezionare un tipo di regola dall'elenco, nello stesso modo in cui è stato selezionato un tipo di regola per la creazione della categoria.

   Al termine della procedura guidata, viene creata la categoria di applicazioni. La regola è visualizzata nell'elenco delle categorie di applicazioni. È possibile utilizzare la categoria di applicazioni creata durante la configurazione di Controllo Applicazioni.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux

Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati

È possibile utilizzare i file eseguibili nei dispositivi selezionati come modello per i file eseguibili da consentire o bloccare. In base ai file eseguibili nei dispositivi selezionati, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per creare una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Categorie di applicazioni**.

   Verrà visualizzata la pagina con un elenco di categorie di applicazioni.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nella pagina **Selezionare il metodo di creazione della categoria** della procedura guidata specificare il nome della categoria e selezionare l'opzione **Categoria che include i file eseguibili dei dispositivi selezionati. Tali file eseguibili sono elaborati automaticamente e le relative metriche vengono aggiunte alla categoria**.

4. Fare clic su **Aggiungi**.

5. Nella finestra visualizzata selezionare uno o più dispositivi che contengono i file eseguibili da utilizzare per creare la categoria di applicazioni.

6. Specificare le seguenti impostazioni:

   - Algoritmo di calcolo del valore hash

A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center Cloud Console per i file di questa categoria. Le informazioni sui valori hash calcolati vengono archiviate nel database di Administration Server. L'archiviazione dei valori hash non aumenta in modo significativo le dimensioni del database.

SHA-256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive supportano il calcolo di SHA-256. Il calcolo della funzione hash MD5 è supportato da tutte le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center Cloud Console per i file della categoria:

- Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive, selezionare la casella di controllo **SHA-256**. Non è consigliabile aggiungere categorie create in base al criterio dell'hash SHA-256 di un file eseguibile per le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Questo può generare errori durante l'esecuzione dell'applicazione di protezione. In questo caso, è possibile utilizzare la funzione hash di criptaggio MD5 per i file della categoria.

- Se nella rete sono installate versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, selezionare **Hash MD5**. Non è possibile aggiungere una categoria che è stata creata in base al criterio del checksum MD5 di un file eseguibile per Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive. In questo caso, è possibile utilizzare la funzione hash di criptaggio SHA-256 per i file della categoria.

Se diversi dispositivi della rete utilizzano versioni precedenti e successive di Kaspersky Endpoint Security 10, selezionare sia la casella di controllo **SHA-256** che la casella di controllo **Hash MD5**.

La casella di controllo **Calcola SHA-256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)** è selezionata per impostazione predefinita.

La casella di controllo **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** è deselezionata per impostazione predefinita.

- Sincronizza i dati con l'archivio dell'Administration Server

Selezionare questa opzione se si desidera che Administration Server controlli periodicamente le modifiche nelle cartelle specificate.

Per impostazione predefinita, questa opzione è disabilitata.

Se si abilita questa opzione, specificare il periodo (in ore) per la verifica delle modifiche nelle cartelle specificate. Per impostazione predefinita, l'intervallo per la scansione è di 24 ore.

- Tipo di file

In questa sezione è possibile specificare il tipo di file utilizzato per creare la categoria di applicazioni.

Tutti i file. Durante la creazione della categoria vengono presi in considerazione tutti i file. Per impostazione predefinita, questa opzione è selezionata.

Solo i file esterni alle categorie di applicazioni. Durante la creazione della categoria vengono presi in considerazione solo i file esterni alle categorie di applicazioni.

- Cartelle

In questa sezione è possibile specificare quali cartelle nei dispositivi selezionati contengono i file utilizzati per creare la categoria di applicazioni.

Tutte le cartelle. Per la creazione della categoria vengono prese in considerazione tutte le cartelle. Per impostazione predefinita, questa opzione è selezionata.

Cartella specificata. Per la creazione della categoria viene presa in considerazione solo la cartella specificata. Se si seleziona questa opzione, è necessario specificare il percorso della cartella.

Al termine della procedura guidata, viene creata la categoria di applicazioni. La regola è visualizzata nell'elenco delle categorie di applicazioni. È possibile utilizzare la categoria di applicazioni creata durante la configurazione di Controllo Applicazioni.

Visualizzazione dell'elenco delle categorie di applicazioni

È possibile visualizzare l'elenco delle categorie di applicazioni configurate e le impostazioni di ciascuna categoria di applicazioni.

Per visualizzare l'elenco delle categorie di applicazioni:

Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Categorie di applicazioni**.

Verrà visualizzata la pagina con un elenco di categorie di applicazioni.

Per visualizzare le proprietà di una categoria di applicazioni:

Fare clic sul nome della categoria di applicazioni.

Verrà visualizzata la finestra delle proprietà della categoria di applicazioni. Le proprietà sono raggruppate in diverse schede.

Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

Dopo aver creato le categorie di Controllo Applicazioni, è possibile utilizzarle per configurare Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows.

Per configurare Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

1. Nel menu principale accedere a **Risorse (dispositivi) → Criteri e profili**.

   Verrà visualizzata una pagina con un elenco di criteri.

2. Fare clic sul criterio **Kaspersky Endpoint Security for Windows**.

   Verrà visualizzata la finestra delle impostazioni del criterio.

3. Passare a **Impostazioni applicazione → Security Controls → Application Control**.

Verrà visualizzata la finestra **Controllo Applicazioni** con le impostazioni di Controllo Applicazioni.

4. L'opzione **Controllo Applicazioni** è abilitata per impostazione predefinita. Spostare l'interruttore su **Controllo Applicazioni DISABILITATO** per disabilitare l'opzione.

5. Nelle impostazioni del blocco **Impostazioni di Controllo Applicazioni**, abilitare la modalità operativa per applicare le regole di Controllo applicazioni e consentire a Kaspersky Endpoint Security for Windows di bloccare l'avvio delle applicazioni.

   Se si desidera testare le regole di Controllo Applicazioni, nella sezione **Impostazioni di Controllo Applicazioni**, abilitare la modalità di test. In modalità di test, Kaspersky Endpoint Security for Windows non blocca l'avvio delle applicazioni, ma registra le informazioni sulle regole attivate nel rapporto. Fare clic sul collegamento **Visualizza rapporto** per visualizzare queste informazioni.

6. Abilitare l'opzione **Controlla il caricamento dei moduli DLL** se si desidera che Kaspersky Endpoint Security for Windows monitori il caricamento dei moduli DLL all'avvio delle applicazioni da parte degli utenti.

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

   Kaspersky Endpoint Security for Windows monitora solo i moduli DLL e i driver caricati dopo che è stata selezionata l'opzione **Controlla il caricamento dei moduli DLL**. Riavviare il computer dopo aver selezionato l'opzione **Controlla il caricamento dei moduli DLL** se si desidera che Kaspersky Endpoint Security for Windows monitori tutti i moduli DLL e i driver, inclusi quelli caricati prima dell'avvio di Kaspersky Endpoint Security for Windows.

7. (Facoltativo) Nella sezione **Modelli di messaggi** modificare il modello del messaggio visualizzato quando l'avvio di un'applicazione è bloccato e il modello del messaggio e-mail inviato.

8. Nelle impostazioni del gruppo **Modalità Controllo Applicazioni**, selezionare la modalità **Lista vietati** o **Lista consentiti**.

   Per impostazione predefinita, è selezionata la modalità **Lista vietati**.

9. Fare clic sul collegamento **Impostazioni elenchi di regole**.

   Verrà visualizzata la finestra **Liste vietati e Liste consentiti** per consentire di aggiungere una categoria di applicazioni. Per impostazione predefinita, è selezionata la scheda **Lista vietati** se è selezionata la modalità **Lista vietati** e la scheda **Lista consentiti** se è selezionata la modalità **Lista consentiti**.

10. Nella finestra **Liste vietati e liste consentiti** fare clic sul pulsante **Aggiungi**.

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

11. Fare clic sul collegamento **Scegliere una categoria**.

    Verrà visualizzata la finestra **Categoria di applicazioni**.

12. Aggiungere una o più categorie di applicazioni create in precedenza.

    È possibile modificare le impostazioni di una categoria creata facendo clic sul pulsante **Modifica**.

    È possibile creare una nuova categoria facendo clic sul pulsante **Aggiungi**.

    È possibile eliminare una categoria dall'elenco facendo clic sul pulsante **Elimina**.

13. Al termine della creazione dell'elenco delle categorie di applicazioni, fare clic sul pulsante **OK**.

    La finestra **Categoria di applicazioni** verrà chiusa.

14. Nella finestra **Regola di Controllo Applicazioni**, nella sezione **Soggetti e relativi diritti**, creare un elenco di utenti e gruppi di utenti a cui applicare la regola di Controllo Applicazioni.

15. Fare clic sul pulsante **OK** per salvare le impostazioni e chiudere la finestra **Regola di Controllo Applicazioni**.

16. Fare clic sul pulsante **OK** per salvare le impostazioni e chiudere la finestra **Liste vietati e liste consentiti**.
17. Fare clic sul pulsante **OK** per salvare le impostazioni e chiudere la finestra **Controllo Applicazioni**.
18. Chiudere la finestra con le impostazioni dei criteri di Kaspersky Endpoint Security for Windows.

    Controllo Applicazioni è configurato. Una volta propagato il criterio ai dispositivi client, viene gestito l'avvio dei file eseguibili.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux

Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni

Dopo aver configurato Controllo Applicazioni nei criteri di Kaspersky Endpoint Security for Windows, i seguenti eventi verranno visualizzati nell'elenco degli eventi:

- **Avvio dell'applicazione non consentito** (evento *Critico*). Questo evento viene visualizzato se è stato configurato Controllo Applicazioni per l'applicazione delle regole.
- **Avvio dell'applicazione non consentito in modalità test** (evento *Informazioni*). Questo evento viene visualizzato se è stato configurato Controllo Applicazioni per il test delle regole.
- **Messaggio all'amministratore sul divieto di avvio dell'applicazione** (evento di *avviso*). Questo evento viene visualizzato se è stato configurato Controllo Applicazioni per l'applicazione delle regole e un utente ha richiesto l'accesso a un'applicazione che è bloccata all'avvio.

È consigliabile creare selezioni eventi per visualizzare gli eventi relativi all'esecuzione di Controllo Applicazioni.

È possibile aggiungere i file eseguibili relativi agli eventi di Controllo Applicazioni a una categoria di applicazioni esistente o a una nuova categoria di applicazioni. È possibile aggiungere i file eseguibili solo a una categoria di applicazioni con contenuto aggiunto manualmente.

Per aggiungere file eseguibili relativi agli eventi di Controllo Applicazioni a una categoria di applicazioni:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.

   Verrà visualizzato l'elenco di selezioni eventi.

2. Selezionare la selezione eventi per visualizzare gli eventi relativi a Controllo Applicazioni e avviare questa selezione eventi.

   Se non è stata creata la selezione eventi correlata a Controllo Applicazioni, è possibile selezionare e avviare una selezione predefinita, ad esempio **Eventi recenti**.

   Verrà visualizzato l'elenco degli eventi.

3. Selezionare gli eventi di cui si desidera aggiungere i file eseguibili associati alla categoria di applicazioni, quindi fare clic sul pulsante **Assegna a categoria**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Nella pagina della procedura guidata, specificare le impostazioni appropriate:

- Nella sezione **Azione sul file eseguibile relativo all'evento** selezionare una delle seguenti opzioni:
  - Aggiungi a una nuova categoria di applicazioni

    Selezionare questa opzione se si desidera creare una nuova categoria di applicazioni basata sui file eseguibili correlati agli eventi.

    Per impostazione predefinita, questa opzione è selezionata.

    Se è stata selezionata questa opzione, specificare un nuovo nome di categoria.

  - Aggiungi a una categoria di applicazioni esistente

    Selezionare questa opzione se si desidera aggiungere i file eseguibili correlati agli eventi a una categoria di applicazioni esistente.

    Per impostazione predefinita, questa opzione non è selezionata.

    Se è stata selezionata questa opzione, selezionare la categoria di applicazioni con contenuto aggiunto manualmente a cui si desidera aggiungere file eseguibili.

- Nella sezione **Tipo di regola** selezionare una delle seguenti opzioni:
  - **Regole per l'aggiunta alle inclusioni**
  - **Regole per l'aggiunta alle esclusioni**
- Nella sezione **Parametro utilizzato come condizione** selezionare una delle seguenti opzioni:
  - Dettagli del certificato (o hash SHA-256 per i file senza certificato)

    I file possono essere firmati con un certificato. Più file possono essere firmati con lo stesso certificato. Ad esempio, lo stesso certificato può essere utilizzato per firmare differenti versioni della stessa applicazione o diverse applicazioni dello stesso fornitore. Quando si seleziona un certificato, possono essere inserite nella categoria diverse versioni di un'applicazione o diverse applicazioni dello stesso fornitore.

    Ogni file dispone di una specifica funzione hash SHA-256 univoca. Quando si seleziona una funzione hash SHA-256, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

    Selezionare questa opzione se si desidera aggiungere alle regole della categoria i dettagli del certificato di un file eseguibile (o la funzione hash SHA-256 per i file senza certificato).

    Per impostazione predefinita, questa opzione è selezionata.

  - Dettagli del certificato (i file senza certificato verranno ignorati)

    I file possono essere firmati con un certificato. Più file possono essere firmati con lo stesso certificato. Ad esempio, lo stesso certificato può essere utilizzato per firmare differenti versioni della stessa applicazione o diverse applicazioni dello stesso fornitore. Quando si seleziona un certificato, possono essere inserite nella categoria diverse versioni di un'applicazione o diverse applicazioni dello stesso fornitore.

    Selezionare questa opzione se si desidera aggiungere i dettagli del certificato di un file eseguibile alle regole della categoria. Se il file eseguibile non dispone di alcun certificato, verrà ignorato. Nessuna informazione sul file verrà aggiunta alla categoria.

- **Solo SHA-256 (i file senza hash verranno ignorati)**

  Ogni file dispone di una specifica funzione hash SHA-256 univoca. Quando si seleziona una funzione hash SHA-256, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

  Selezionare questa opzione se si desidera aggiungere solo i dettagli della funzione hash SHA-256 del file eseguibile.

- **Solo MD5 (modalità non più disponibile, solo per Kaspersky Endpoint Security 10 versione Service Pack 1)**

  Ogni file dispone di una specifica funzione hash MD5 univoca. Quando si seleziona una funzione hash MD5, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

  Selezionare questa opzione se si desidera aggiungere solo i dettagli della funzione hash MD5 del file eseguibile. Il calcolo della funzione hash MD5 è supportato da Kaspersky Endpoint Security 10 Service Pack 1 for Windows e da tutte le versioni precedenti.

5. Fare clic su **OK**.

   Al termine della procedura guidata, i file eseguibili relativi agli eventi di Controllo Applicazioni vengono aggiunti alla categoria di applicazioni esistente o a una nuova categoria di applicazioni. È possibile visualizzare le impostazioni della categoria di applicazioni che è stata modificata o creata.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux

Creazione di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky

Kaspersky Security Center Web Console consente di eseguire l'installazione remota delle applicazioni di terze parti utilizzando i pacchetti di installazione. Tali applicazioni di terze parti sono incluse in un database Kaspersky dedicato.

La creazione di pacchetti di installazione di applicazioni di terze parti dal database Kaspersky è disponibile solo con la licenza Vulnerability e patch management.

Per creare un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
2. Fare clic sul pulsante **Aggiungi**.
3. Nella pagina Creazione guidata nuovo pacchetto visualizzata selezionare l'opzione **Selezionare un'applicazione dal database di Kaspersky per creare un pacchetto di installazione**, quindi fare clic su **Avanti**.

4. Nell'elenco delle applicazioni visualizzato selezionare l'applicazione attinente, quindi fare clic su **Avanti**.

5. Selezionare la lingua di localizzazione attinente nell'elenco a discesa, quindi fare clic su **Avanti**.

   Questo passaggio viene visualizzato solo se l'applicazione offre più opzioni di lingua.

6. Se viene richiesto di accettare un Contratto di licenza per l'installazione, nella pagina **Contratto di licenza con l'utente finale** visualizzata fare clic sul collegamento per leggere il Contratto di licenza nel sito Web del produttore, quindi selezionare la casella di controllo **Confermo di aver letto, compreso e accettato i termini e le condizioni del presente Contratto di licenza con l'utente finale**.

7. Nella pagina **Nome del nuovo pacchetto di installazione** visualizzata, nel campo **Nome pacchetto**, immettere il nome del pacchetto di installazione, quindi fare clic su **Avanti**.

Attendere il caricamento del nuovo pacchetto di installazione creato in Administration Server. Quando la Creazione guidata nuovo pacchetto visualizza il messaggio per informare che il processo di creazione del pacchetto è andato a buon fine, fare clic su **Fine**.

Il nuovo pacchetto di installazione creato viene visualizzato nell'elenco dei pacchetti di installazione. È possibile selezionare questo pacchetto durante la creazione o la riconfigurazione dell'attività *Installa l'applicazione in remoto*.

Visualizzazione e modifica delle impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky

Se in precedenza sono stati creati pacchetti di installazione di applicazioni di terze parti elencate nel database Kaspersky, successivamente è possibile visualizzare e modificare le impostazioni di questi pacchetti.

La modifica delle impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky è disponibile solo con la licenza Vulnerability e patch management.

Per visualizzare e modificare le impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky:

1. Nel menu principale accedere a **Individuazione e distribuzione → Distribuzione e assegnazione → Pacchetti di installazione**.

2. Nell'elenco dei pacchetti di installazione visualizzato fare clic sul nome del pacchetto attinente.

3. Nella pagina delle proprietà visualizzata modificare le impostazioni, se necessario.

4. Fare clic sul pulsante **Salva**.

Le impostazioni modificate vengono salvate.

Impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky

Le impostazioni di un pacchetto di installazione di un'applicazione di terze parti sono raggruppate nelle seguenti schede:

Per impostazione predefinita viene visualizzata solo una parte delle impostazioni elencate di seguito, quindi è possibile aggiungere le colonne corrispondenti facendo clic sul pulsante **Filtro** e selezionando i nomi delle colonne attinenti dall'elenco.

- Scheda **Generale**:
  - Campo di immissione che contiene il nome del pacchetto di installazione che può essere modificato manualmente
  - Applicazione

    Il nome dell'applicazione di terze parti per cui viene creato il pacchetto di installazione.
  - Versione

    Il numero di versione dell'applicazione di terze parti per cui è stato creato il pacchetto di installazione.
  - Dimensione

    Le dimensioni del pacchetto di installazione di terze parti (in kilobyte).
  - Data creazione

    La data e l'ora in cui è stato creato il pacchetto di installazione di terze parti.
  - Percorso

    Percorso della cartella di rete in cui è archiviato il pacchetto di installazione di terze parti.
- Scheda **Procedura di installazione**:
  - Installa i componenti generali del sistema richiesti

    Se questa opzione è abilitata, prima di installare un aggiornamento l'applicazione installa automaticamente tutti i componenti di sistema generali (prerequisiti) richiesti per installare l'aggiornamento. Questi prerequisiti possono ad esempio essere aggiornamenti del sistema operativo.

    Se questa opzione è disabilitata, può essere necessario installare manualmente i prerequisiti.

    Per impostazione predefinita, questa opzione è disabilitata.
  - Tabella che mostra le proprietà dell'aggiornamento e che contiene le seguenti colonne:
    - Nome

      Nome dell'aggiornamento.
    - Descrizione

Descrizione dell'aggiornamento.

- **Origine**

  Origine dell'aggiornamento, ovvero se è stato rilasciato da Microsoft o da un altro sviluppatore di terze parti.

- **Tipo**

  Tipo di aggiornamento, ovvero se è destinato a un driver o a un'applicazione.

- **Categoria**

  Categoria WSUS (Windows Server Update Services) visualizzata per gli aggiornamenti Microsoft (Aggiornamenti critici, Aggiornamenti definizione, Driver, Feature Pack, Aggiornamenti della protezione, Service Pack, Strumenti, Aggiornamenti cumulativi, Aggiornamenti o Upgrade).

- **Livello di importanza in base a MSRC**

  Livello di importanza dell'aggiornamento definito da Microsoft Security Response Center (MSRC).

- **Livello di importanza**

  Livello di importanza dell'aggiornamento definito da Kaspersky.

- **Livello di importanza patch**

  Livello di importanza della patch, se è destinata a un'applicazione Kaspersky.

- **Articolo**

  Identificatore (ID) dell'articolo nella Knowledge Base che descrive l'aggiornamento.

- **Bollettino**

  ID del bollettino sulla sicurezza che descrive l'aggiornamento.

- **Non assegnato per installazione (nuova versione)**

  Indica se l'aggiornamento ha lo stato Non assegnato per l'installazione.

- **Da installare**

  Indica se l'aggiornamento ha lo stato Da installare.

- **Installazione in corso**

  Indica se l'aggiornamento ha lo stato Installazione in corso.

- **Installato**

  Indica se l'aggiornamento ha lo stato Installato.

- **Non riuscito**

  Indica se l'aggiornamento ha lo stato Non riuscito.

- **È necessario il riavvio**

  Indica se l'aggiornamento ha lo stato È necessario il riavvio.

- **Registrato**

  Indica la data e l'ora in cui è stato registrato l'aggiornamento.

- **Installato in modalità interattiva**

  Indica se l'aggiornamento richiede l'interazione con l'utente durante l'installazione.

- **Revocato**

  Indica la data e l'ora in cui l'aggiornamento è stato revocato.

- **Stato di approvazione dell'aggiornamento**

  Indica se l'aggiornamento è approvato per l'installazione.

- **Revisione**

  Indica il numero di revisione corrente dell'aggiornamento.

- **ID aggiornamento**

  Indica l'ID dell'aggiornamento.

- **Versione applicazione**

  Indica il numero di versione a cui deve essere aggiornata l'applicazione.

- **Sostituiti**

  Indica altri aggiornamenti che possono sostituire l'aggiornamento.

- **Sostituzione**

  Indica altri aggiornamenti che possono essere sostituiti dall'aggiornamento.

- **È necessario accettare i termini del Contratto di licenza**

Indica se l'aggiornamento richiede l'accettazione dei termini di un Contratto di licenza con l'utente finale (EULA).

- URL descrizione

  Indica il nome del fornitore dell'aggiornamento.

- Famiglia di applicazioni

  Indica il nome della famiglia di applicazioni a cui appartiene l'aggiornamento.

- Applicazione

  Indica il nome dell'applicazione a cui appartiene l'aggiornamento.

- Lingua localizzazione

  Indica la lingua della localizzazione dell'aggiornamento.

- Non assegnato per installazione (nuova versione)

  Indica se l'aggiornamento ha lo stato Non assegnato per l'installazione (nuova versione).

- Richiede l'installazione dei prerequisiti

  Indica se l'aggiornamento ha lo stato Richiede l'installazione dei prerequisiti.

- Modalità di download

  Indica la modalità di download dell'aggiornamento.

- È una patch

  Indica se l'aggiornamento è una patch.

- Non installato

  Indica se l'aggiornamento ha lo stato Non installato.

- Scheda **Impostazioni** che mostra le impostazioni del pacchetto di installazione, con i relativi nomi, descrizioni e valori, utilizzate come parametri della riga di comando durante l'installazione. Se il pacchetto non fornisce tali impostazioni, viene visualizzato il messaggio corrispondente. È possibile modificare i valori di queste impostazioni.

- Scheda **Cronologia revisioni** che mostra le revisioni del pacchetto di installazione e contiene le seguenti colonne:

  - Revisione

Visualizza il numero di revisione dei pacchetti di installazione.

- **Data/ora**

  Visualizza l'ora in cui è stata creata la revisione.

- **Utente**

  Visualizza il nome dell'account utente con cui è stata creata la revisione.

- **Azione**

  Elenca le azioni eseguite sul pacchetto di installazione all'interno della revisione.

- **Descrizione**

  Visualizza il testo descrittivo aggiunto per la revisione.

Tag applicazione

Questa sezione descrive i tag applicazione e fornisce istruzioni per crearli e modificarli, nonché per l'assegnazione di tag alle applicazioni di terzi.

Informazioni sui tag applicazione

Kaspersky Security Center Cloud Console consente di assegnare tag alle applicazioni di terze perti (applicazioni realizzate da fornitori di software diversi da Kaspersky). Un tag è l'etichetta di un'applicazione che può essere utilizzata per raggruppare o cercare le applicazioni. Un tag assegnato alle applicazioni può essere utilizzato come condizione nelle selezioni dispositivi.

È ad esempio possibile creare il tag `[Browser]` e assegnarlo a tutti i browser, quali Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Creazione di un tag applicazione

Per creare un tag applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Tag applicazione**.
2. Fare clic su **Aggiungi**.

   Verrà visualizzata una finestra per il nuovo tag.
3. Immettere il nome del tag.

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

Il nuovo tag verrà visualizzato nell'elenco dei tag applicazione.

Ridenominazione di un tag applicazione

Per rinominare un tag applicazione:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Tag applicazione**.
2. Selezionare la casella di controllo accanto al tag che si desidera rinominare, quindi fare clic su **Modifica**.

   Verrà visualizzata una finestra delle proprietà del tag.
3. Modificare il nome del tag.
4. Fare clic su **OK** per salvare le modifiche.

Il tag aggiornato verrà visualizzato nell'elenco dei tag applicazione.

Assegnazione di tag a un'applicazione

Per assegnare uno o più tag a un'applicazione:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Registro delle applicazioni**.
2. Fare clic sul nome dell'applicazione a cui si desidera assegnare i tag.
3. Fare clic sulla scheda **Tag**.

   La scheda mostra tutti i tag delle applicazioni presenti in Administration Server. Per i tag assegnati all'applicazione selezionata, la casella di controllo nella colonna **Tag assegnato** è selezionata.
4. Per i tag che si desidera assegnare, selezionare le caselle di controllo nella colonna **Tag assegnato**.
5. Fare clic su **Salva** per salvare le modifiche.

I tag verranno assegnati all'applicazione.

Rimozione dei tag assegnati a un'applicazione

Per rimuovere uno o più tag da un'applicazione:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Registro delle applicazioni**.
2. Fare clic sul nome dell'applicazione da cui si desidera rimuovere i tag.
3. Fare clic sulla scheda **Tag**.

La scheda mostra tutti i tag delle applicazioni presenti in Administration Server. Per i tag assegnati all'applicazione selezionata, la casella di controllo nella colonna **Tag assegnato** è selezionata.

4. Per i tag che si desidera rimuovere, deselezionare le caselle di controllo nella colonna **Tag assegnato**.
5. Fare clic su **Salva** per salvare le modifiche.

I tag verranno rimossi dall'applicazione.

I tag dell'applicazione rimossi non vengono eliminati. Se si desidera, è possibile eliminarli manualmente.

Eliminazione di un tag applicazione

Per eliminare un tag applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Tag applicazione**.
2. Selezionare dall'elenco il tag applicazione da eliminare.
3. Fare clic sul pulsante **Elimina**.
4. Nella finestra visualizzata fare clic su **OK**.

Il tag applicazione verrà eliminato. Il tag eliminato viene rimosso automaticamente da tutte le applicazioni a cui è stato assegnato.

Configurazione di Administration Server

Questa sezione descrive il processo di configurazione e le proprietà di Kaspersky Security Center Administration Server.

Creazione di una gerarchia di Administration Server: l'aggiunta un Administration Server secondario

È possibile fare in modo che un Administration Server in esecuzione in locale funga da Administration Server secondario, configurando così una gerarchia "primario/secondario" nella rete. Per l'Administration Server che si trova nell'infrastruttura Kaspersky, sia gli Administration Server primari che quelli secondari nella rete sono server secondari. È possibile aggiungere un Administration Server basato su Windows e un Administration Server basato su Linux.

Per aggiungere un Administration Server secondario disponibile per la connessione:

1. Assicurarsi che nel futuro Administration Server secondario sia installato Kaspersky Security Center Web Console.

2. Nel futuro Administration Server secondario scaricare il certificato di Administration Server e salvarlo in modo da poterlo aggiungere all'Administration Server primario durante uno dei passaggi dell'Aggiunta guidata Administration Server secondari.

3. Procedere come segue tramite Kaspersky Security Center Web Console nel futuro Administration Server secondario (in alternativa, è possibile chiedere all'amministratore del futuro Administration Server secondario di eseguire queste azioni):

   a. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome del futuro Administration Server secondario.

   b. Nella pagina delle proprietà visualizzata passare alla sezione **Gerarchia di Administration Server** della scheda **Generale**.

   c. Selezionare l'opzione **Questo Administration Server è secondario nella gerarchia**.

   d. Selezionare **Cloud Console** come tipo di Administration Server primario.

      I campi relativi alle impostazioni per stabilire la connessione tra Administration Server primario e secondario diventano disponibili.

   e. Nei campi **Indirizzo server HDS (dall'Administration Server primario in Cloud Console)** e **Porte del server HDS**, immettere l'indirizzo e la porta dell'Administration Server primario di Kaspersky Security Center Cloud Console.

      L'indirizzo del server HDS e la porta del server HDS sono disponibili nell'Administration Server di Kaspersky Security Center Cloud Console, nella sezione **Gerarchia di Administration Server** della scheda **Generale** della finestra delle proprietà. È possibile copiare e incollare questi dati nei campi della finestra dell'Administration Server secondario.

   f. Fare clic sul pulsante **Specifica certificato Administration Server primario**, quindi selezionare il certificato.

      È possibile scaricare questo certificato dall'Administration Server di Kaspersky Security Center Cloud Console, nella sezione **Gerarchia di Administration Server** della scheda **Generale** della finestra delle proprietà, facendo clic sul pulsante **Visualizza certificato di Administration Server**.

   g. Fare clic sul pulsante **Specifica certificati Hosted Discovery Service**, quindi selezionare il certificato.

È possibile scaricare questo certificato dall'Administration Server di Kaspersky Security Center Cloud Console, nella sezione **Gerarchia di Administration Server** della scheda **Generale** della finestra delle proprietà, facendo clic sul pulsante **Certificato autorità di certificazione radice HDS**.

h. Se si utilizza un server proxy per connettersi all'Administration Server di Kaspersky Security Center Cloud Console (cioè il server primario nella gerarchia creata), specificarlo e immettere le credenziali del server proxy.

i. Selezionare l'opzione **Connetti l'Administration Server primario all'Administration Server secondario nella rete perimetrale** se l'Administration Server secondario si trova in una rete perimetrale.

j. Fare clic su **Salva** per salvare le modifiche e chiudere la finestra.

4. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome del futuro Administration Server primario.

5. Nella pagina delle proprietà visualizzata fare clic sulla scheda **Administration Server**.

6. Selezionare la casella di controllo accanto al nome del gruppo di amministrazione a cui si desidera aggiungere l'Administration Server secondario.

7. Nella riga del menu fare clic su **Connetti Administration Server secondario**.

   Verrà avviata l'Aggiunta guidata Administration Server secondari.

8. Nella prima pagina della procedura guidata compilare i seguenti campi:

   - **Nome visualizzato dell'Administration Server secondario**

     Un nome con cui l'Administration Server secondario verrà visualizzato nella gerarchia. Se si desidera, è possibile immettere l'indirizzo IP come nome, oppure è possibile utilizzare un nome come "Server secondario per il gruppo 1".

   - **Indirizzo dell'Administration Server secondario (facoltativo)**

     Specificare l'indirizzo IP o il nome di dominio dell'Administration Server secondario.

9. Se si utilizza un server proxy per connettersi all'Administration Server di Kaspersky Security Center Cloud Console (cioè il futuro server primario), specificarlo e immettere le credenziali del server proxy.

10. Seguire le ulteriori istruzioni della procedura guidata.

Al termine della procedura guidata, verrà creata la gerarchia "primario/secondario". L'Administration Server primario inizia a ricevere la connessione dall'Administration Server secondario tramite la porta 13000. Le attività e i criteri dall'Administration Server primario vengono ricevuti e applicati. L'Administration Server secondario viene visualizzato nell'Administration Server primario, nel gruppo di amministrazione a cui è stato aggiunto.

Creazione dei gruppi di amministrazione

Inizialmente, la gerarchia dei gruppi di amministrazione contiene solo un gruppo di amministrazione denominato gruppo **Dispositivi gestiti**. È possibile aggiungere dispositivi e sottogruppi nel gruppo **Dispositivi gestiti**.

Per creare un gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nella gerarchia selezionare il gruppo di amministrazione che deve includere il nuovo gruppo di amministrazione.
3. Fare clic sul pulsante **Aggiungi**.
4. Nella finestra visualizzata immettere un nome per il gruppo, quindi fare clic su **Aggiungi**.

   Un nuovo gruppo di amministrazione con il nome specificato viene visualizzato nella gerarchia dei gruppi di amministrazione.

L'applicazione consente di creare una gerarchia di gruppi di amministrazione basata sulla struttura di Active Directory o sulla struttura della rete di dominio. È inoltre possibile creare una struttura di gruppi a partire da un file di testo.

Per creare una struttura di gruppi di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Fare clic sul pulsante **Importa**.

   Verrà avviata la Creazione guidata nuova struttura dei gruppi di amministrazione. Seguire le istruzioni della procedura guidata.

Configurazione del periodo di archiviazione degli eventi relativi ai dispositivi eliminati

In Kaspersky Security Center Cloud Console gli eventi vengono archiviati in un archivio eventi. Non è possibile configurare il numero di eventi da archiviare nell'archivio eventi.

Nella sezione **Archivio eventi** della finestra delle proprietà di Administration Server è possibile configurare il periodo di archiviazione massimo degli eventi relativi ai dispositivi eliminati. Il periodo di archiviazione massimo è 1000 giorni.

Per configurare il numero di giorni per l'archiviazione degli eventi relativi ai dispositivi eliminati:

1. Nella parte superiore dello schermo fare clic sull'icona Impostazioni ( ) accanto a Kaspersky Security Center Cloud Console Administration Server.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Generale** selezionare la sezione **Archivio eventi**.
3. Abilitare l'opzione **Archivia eventi dopo l'eliminazione dei dispositivi**.
4. Nella casella di modifica **Periodo di archiviazione massimo (giorni)** specificare il numero di giorni per l'archiviazione degli eventi relativi ai dispositivi eliminati.

Il numero di giorni per l'archiviazione degli eventi relativi ai dispositivi eliminati è limitato dal valore specificato.

È inoltre possibile modificare le impostazioni di qualsiasi attività per salvare gli eventi relativi all'avanzamento dell'attività oppure salvare solo i risultati dell'esecuzione dell'attività. In tal modo si riduce il numero di eventi nel database, si aumenta la velocità di esecuzione degli scenari associati all'analisi della tabella degli eventi nel database e si limita il rischio che gli eventi critici vengano sovrascritti da un ampio numero di eventi.

Messaggi email aggregati sugli eventi

Durante l'esecuzione, Kaspersky Security Center Cloud Console e le applicazioni Kaspersky gestite generano eventi. A ogni evento è attribuito un determinato tipo e un livello di criticità (*Critico, Errore funzionale, Avviso* o *informazioni*). A seconda delle condizioni in cui si è verificato un evento, Kaspersky Security Center Cloud Console può assegnare diversi livelli di criticità a eventi dello stesso tipo.

Kaspersky Security Center Cloud Console invia automaticamente, tramite e-mail, notifiche relative agli eventi. Kaspersky Security Center Cloud Console invia notifiche sugli eventi elencati nella finestra **Proprietà di Administration Server**, nella scheda **Configurazione eventi**. Le impostazioni di notifica comuni sono utilizzate per tutti i tipi di eventi.

Per limitare il numero di messaggi e-mail che devono essere inviati, Kaspersky Security Center Cloud Console, durante periodi specifici, aggrega gli eventi con lo stesso livello di criticità. I valori dei periodi sono gestiti dagli specialisti di Kaspersky. Di conseguenza, i destinatari ricevono messaggi e-mail aggregati secondo il modello seguente: "Si sono verificati <numero> eventi <Livello_criticità> (e di livello inferiore)".

Limitazioni sulla gestione degli Administration Server secondari in esecuzione in locale tramite Kaspersky Security Center Cloud Console

Dopo il passaggio a un Administration Server secondario in esecuzione in locale utilizzando l'opzione corrispondente in Kaspersky Security Center Cloud Console, l'applicazione impone limitazioni specifiche sulla gestione di questo Administration Server slave. Le seguenti impostazioni relative all'esecuzione di Kaspersky Security Center Cloud Console diventano non disponibili per l'utente:

- Nelle impostazioni dei criteri di Network Agent e dei criteri dell'Administration Server le schede **Configurazione eventi** e **Impostazioni applicazione** non sono disponibili; non è possibile creare nuovi criteri.
- Nelle impostazioni delle attività di Network Agent e delle attività dell'Administration Server le schede **Configurazione eventi** e **Impostazioni applicazione** non sono disponibili; non è possibile creare nuove attività.
- La gestione di Network Agent e Administration Server non è disponibile, così come la finestra delle proprietà dell'Administration Server secondario.
- L'avvio rapido guidato non è disponibile.
- Le impostazioni di archiviazione e notifica per gli eventi di Network Agent e Administration Server non possono essere modificate.
- La sezione **Versioni correnti delle applicazioni** non è disponibile.
- La sezione **Pacchetti di installazione** non è disponibile.

Visualizzazione dell'elenco degli Administration Server secondari

Per visualizzare l'elenco degli Administration Server secondari (inclusi quelli virtuali):

Nel menu principale, fare clic sul nome di Administration Server, accanto all'icona delle impostazioni ( ).

Viene visualizzato l'elenco a discesa degli Administration Server secondari (inclusi quelli virtuali).

È possibile passare a uno di questi Administration Server facendo clic sul relativo nome.

Eliminazione di una gerarchia di Administration Server

Se non si desidera più avere una gerarchia di Administration Server, è possibile disconnetterli da tale gerarchia.

Per eliminare una gerarchia di Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server primario.
2. Nella pagina visualizzata passare alla scheda **Administration Server**.
3. Nel gruppo di amministrazione da cui si desidera eliminare l'Administration Server secondario selezionare l'Administration Server secondario.
4. Nella riga del menu fare clic su **Elimina**.
5. Nella finestra di dialogo visualizzata fare clic su **OK** per confermare che si desidera eliminare l'Administration Server secondario.

I precedenti Administration Server primario e secondario sono ora indipendenti l'uno dall'altro. La gerarchia non è più presente.

Configurazione dell'interfaccia

È possibile configurare l'interfaccia di Kaspersky Security Center Cloud Console in modo da visualizzare e nascondere sezioni ed elementi dell'interfaccia, a seconda delle funzionalità in uso.

Per configurare l'interfaccia di Kaspersky Security Center Cloud Console in base al set di funzionalità utilizzate al momento:

1. Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Opzioni di interfaccia**.
2. Nella finestra **Opzioni di interfaccia** visualizzata abilitare o disabilitare le opzioni:
   - Mostra Criptaggio e protezione dei dati

     È possibile utilizzare questa opzione per nascondere o mostrare la sezione **Operazioni → Criptaggio e protezione dei dati** nell'interfaccia. Kaspersky Security Center Cloud Console salva il valore di questa opzione solo per il proprio account utente, mentre l'altro utente può impostare un valore diverso.

   - Mostra funzionalità MDR

È possibile utilizzare questa opzione per nascondere o mostrare la sezione **Monitoraggio e generazione dei rapporti** → **Incidenti** nell'interfaccia. Kaspersky Security Center Cloud Console salva il valore di questa opzione solo per il proprio account utente, mentre l'altro utente può impostare un valore diverso.

3. Impostare il numero di dispositivi che Kaspersky Security Center Cloud Console visualizza nei risultati di distribuzione dei criteri.
4. Fare clic su **Salva**.

Le impostazioni dell'interfaccia della console vengono configurate in base alle preferenze dell'utente.

Gestione di Administration Server virtuali

Questa sezione descrive le seguenti azioni per gestire Administration Server virtuali:

- Creare Administration Server virtuali
- Abilitare e disabilitare Administration Server virtuali
- Assegnare un amministratore per un Administration Server virtuale
- Modificare Administration Server per i dispositivi client
- Eliminare Administration Server virtuali

Creazione di un Administration Server virtuale

È possibile creare Administration Server virtuali e aggiungerli ai gruppi di amministrazione.

Per creare e aggiungere un Administration Server virtuale:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome dell'Administration Server richiesto.
2. Nella pagina visualizzata passare alla scheda **Administration Server**.
3. Selezionare il gruppo di amministrazione a cui si desidera aggiungere un Administration Server virtuale.
4. Nella riga del menu fare clic su **Nuovo Administration Server virtuale**.
5. Nella pagina visualizzata definire il **Nome Administration Server virtuale**.
6. Fare clic su **Salva**.

Il nuovo Administration Server virtuale verrà creato, aggiunto al gruppo di amministrazione e visualizzato nella scheda **Administration Server**.

Abilitazione e disabilitazione di un Administration Server virtuale

Quando si crea un nuovo Administration Server virtuale, questo viene abilitato per impostazione predefinita. È possibile disabilitarlo o abilitarlo nuovamente in qualsiasi momento. La disabilitazione o l'abilitazione di un Administration Server virtuale equivale alla disattivazione o all'attivazione di un Administration Server fisico.

Per abilitare o disabilitare un Administration Server virtuale:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.
2. Nella pagina visualizzata passare alla scheda **Administration Server**.
3. Selezionare l'Administration Server virtuale che si desidera abilitare o disabilitare.
4. Nella riga del menu fare clic sul pulsante **Abilita/disabilita l'Administration Server virtuale**.

Lo stato dell'Administration Server virtuale viene modificato in abilitato o disabilitato, a seconda del suo stato precedente. Viene visualizzato lo stato aggiornato accanto al nome dell'Administration Server.

Assegnazione di un amministratore per un Administration Server virtuale

Quando si utilizzano Administration Server virtuali nell'organizzazione, è consigliabile assegnare un amministratore dedicato per ciascun Administration Server virtuale. Questo potrebbe ad esempio essere utile quando si creano Administration Server virtuali per gestire uffici o reparti separati della propria organizzazione oppure se si è un provider MSP e si gestiscono i tenant tramite Administration Server virtuali.

Quando si crea un Administration Server virtuale, eredita l'elenco di utenti e tutti i diritti utente dell'Administration Server primario. Se un utente dispone dei diritti di accesso al server primario, ha anche i diritti di accesso al server virtuale. Dopo la creazione, si configurano i diritti di accesso ai server in modo indipendente. Se si desidera assegnare un amministratore solo per un Administration Server virtuale, accertarsi che l'amministratore non sia incluso nell'elenco **Diritti di accesso** nelle proprietà dell'Administration Server primario.

Si assegna un amministratore per un Administration Server virtuale concedendo all'amministratore i diritti di accesso all'Administration Server virtuale. È possibile concedere i diritti di accesso necessari in uno dei seguenti modi:

- Configurare manualmente i diritti di accesso per l'amministratore
- Assegnare uno o più ruoli utente per l'amministratore

Quando si assegna un amministratore, assicurarsi di concedere l'accesso a un unico Administration Server virtuale. Un amministratore con accesso a più Administration Server virtuali non può accedere a Kaspersky Security Center Cloud Console.

Un amministratore di un Administration Server virtuale accede a Kaspersky Security Center Cloud Console allo stesso modo con cui accede all'Administration Server primario. Kaspersky Security Center Cloud Console autentica l'amministratore e apre l'Administration Server virtuale per il quale l'amministratore dispone dei diritti di accesso. L'amministratore non può passare da un Administration Server all'altro.

Prerequisiti

Prima di iniziare, assicurarsi che vengano soddisfatte le seguenti condizioni:

- L'Administration Server virtuale è stato creato.
- Nell'Administration Server primario è stato creato un account per l'amministratore che si desidera assegnare per l'Administration Server virtuale.
- L'account dell'amministratore del server virtuale creato non è incluso negli elenchi **Diritti di accesso** nelle proprietà dei server, primari o secondari che siano.
- L'utente dispone del diritto **Modifica elenchi di controllo degli accessi agli oggetti** nell'area funzionale **Caratteristiche generali**: **Autorizzazioni utente**.

Configurazione manuale dei diritti di accesso

Per assegnare un amministratore per un Administration Server virtuale:

1. Nella menu principale, passare all'Administration Server virtuale desiderato:
   a. Fare clic sull'icona a forma di freccia di espansione (›) a destra del nome corrente dell'Administration Server.
   b. Selezionare l'Administration Server desiderato.
2. Nel menu principale, fare clic sull'icona delle impostazioni (⚙) accanto al nome di Administration Server.
   Verrà visualizzata la finestra delle proprietà di Administration Server.
3. Nella scheda **Diritti di accesso**, fare clic sul pulsante **Aggiungi**.
   Viene visualizzato un elenco unificato di utenti dell'Administration Server primario e dell'Administration Server virtuale corrente.
4. Nell'elenco di utenti selezionare l'account dell'amministratore che si desidera assegnare per l'Administration Server virtuale, quindi fare clic sul pulsante **OK**.
   L'applicazione aggiunge l'utente selezionato all'elenco utenti nella scheda **Diritti di accesso**.
5. Selezionare la casella di controllo accanto all'account aggiunto, quindi fare clic sul pulsante **Diritti di accesso**.
6. Configurare i diritti che l'amministratore avrà sull'Administration Server virtuale.
   Per fare in modo che l'autenticazione vada a buon fine, l'amministratore deve disporre almeno dei seguenti diritti:
   - Diritto **Lettura** nell'area funzionale **Caratteristiche generali** → **Funzionalità di base**
   - Diritto **Lettura** nell'area funzionale **Caratteristiche generali** → **Administration Server virtuali**

L'applicazione salva i diritti utente modificati nell'account amministratore.

Configurazione dei diritti di accesso assegnando ruoli utente

In alternativa, è possibile concedere i diritti di accesso a un amministratore dell'Administration Server virtuale tramite i ruoli utente. Questo potrebbe ad esempio essere utile se si desidera assegnare più amministratori nello stesso Administration Server virtuale. In tal caso, è possibile assegnare agli account degli amministratori gli stessi ruoli utente (uno o più di questi) anziché configurare gli stessi diritti utente per più amministratori.

Per assegnare un amministratore a un Administration Server virtuale assegnando ruoli utente:

1. Nell'Administration Server primario creare un nuovo ruolo utente, quindi specificare tutti i diritti di accesso necessari di cui un amministratore deve disporre nell'Administration Server virtuale. È possibile creare più ruoli, ad esempio, se si desidera separare l'accesso a diverse aree funzionali.

2. Nella menu principale, passare all'Administration Server virtuale desiderato:

   a. Fare clic sull'icona a forma di freccia di espansione (›) a destra del nome corrente dell'Administration Server.

   b. Selezionare l'Administration Server desiderato.

3. Assegnare il nuovo ruolo o diversi ruoli all'account amministratore.

L'applicazione assegna il nuovo ruolo all'account amministratore.

Configurazione dei diritti di accesso a livello di oggetto

Oltre ad assegnare diritti di accesso a livello di area funzionale, è possibile configurare l'accesso a oggetti specifici nell'Administration Server virtuale, ad esempio, a un gruppo di amministrazione specifico o a un'attività. A tale scopo, passare all'Administration Server virtuale, quindi configurare i diritti di accesso nelle proprietà dell'oggetto.

Eliminazione di un Administration Server virtuale

Quando si elimina un Administration Server virtuale, verranno eliminati anche tutti gli oggetti creati nell'Administration Server, inclusi criteri e attività. I dispositivi gestiti dei gruppi di amministrazione che erano gestiti dall'Administration Server virtuale verranno rimossi dai gruppi di amministrazione. Per far tornare i dispositivi sotto la gestione di Kaspersky Security Center Cloud Console, eseguire il polling di rete, quindi spostare i dispositivi rilevati dal gruppo Dispositivi non assegnati ai gruppi di amministrazione.

Per eliminare un Administration Server virtuale:

1. Nel menu principale, fare clic sull'icona delle impostazioni (⚙) accanto al nome di Administration Server.

2. Nella pagina visualizzata passare alla scheda **Administration Server**.

3. Selezionare l'Administration Server virtuale che si desidera eliminare.

4. Nella riga del menu fare clic sul pulsante **Elimina**.

L'Administration Server virtuale viene eliminato.

Monitoraggio e generazione di rapporti

Questa sezione illustra le funzionalità di monitoraggio e reportistica di Kaspersky Security Center Cloud Console. Queste funzionalità offrono una panoramica dell'infrastruttura, degli stati di protezione e delle statistiche.

Dopo la distribuzione di Kaspersky Security Center Cloud Console o durante l'esecuzione, è possibile configurare le funzionalità di monitoraggio e generazione dei rapporti in base alle esigenze.

Scenario: monitoraggio e generazione di rapporti

Questa sezione fornisce uno scenario per la configurazione della funzionalità di monitoraggio e generazione dei rapporti in Kaspersky Security Center Cloud Console.

Prerequisiti

Dopo aver distribuito Kaspersky Security Center Cloud Console nella rete di un'organizzazione, è possibile iniziare a monitorarlo e generare rapporti sul relativo funzionamento.

Passaggi

La configurazione del monitoraggio e della generazione dei rapporti nella rete di un'organizzazione prevede diversi passaggi:

1. **Configurazione del passaggio degli stati del dispositivo**

   Acquisire familiarità con le impostazioni per gli stati del dispositivo in base a condizioni specifiche. Modificando queste impostazioni, è possibile modificare il numero di eventi con livelli di importanza Critico o Avviso. Durante la configurazione del passaggio degli stati del dispositivo, verificare quanto segue:

   - Le nuove impostazioni non sono in conflitto con i criteri di sicurezza delle informazioni dell'organizzazione.
   - Si è in grado di reagire tempestivamente agli eventi di sicurezza importanti nella rete dell'organizzazione.

2. **Configurazione delle notifiche degli eventi nei dispositivi client**

   Istruzioni dettagliate: Configurare la notifica (tramite e-mail) di eventi nei dispositivi client

3. **Modifica della risposta della rete di sicurezza all'evento Epidemia di virus**

   È possibile modificare le specifiche soglie nelle proprietà di Administration Server. È inoltre possibile creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.

4. **Analisi dello stato di sicurezza della rete dell'organizzazione**

   Istruzioni dettagliate:

   - Esaminare il widget **Stato protezione**
   - Generare ed esaminare il **Rapporto sullo stato della protezione**
   - Generare ed esaminare il **Rapporto sugli errori**

5. **Individuazione dei dispositivi client che non sono protetti**

Istruzioni dettagliate:

- Esaminare il widget **Nuovi dispositivi**
- Generare ed esaminare il **Rapporto sulla distribuzione della protezione**

6. **Verifica della protezione dei dispositivi client**

   Istruzioni dettagliate:

   - Generare ed esaminare i rapporti delle categorie **Stato protezione** e **Statistiche delle minacce**
   - Avviare ed esaminare la selezione eventi **Critico**

7. **Analisi delle informazioni sulla licenza**

   Istruzioni dettagliate:

   - Aggiungere il widget **Utilizzo chiavi di licenza** al dashboard ed esaminarlo
   - Generare ed esaminare il **Rapporto sull'utilizzo delle chiavi di licenza**

Risultati

Al termine dello scenario, si dispone di informazioni sulla protezione della rete dell'organizzazione e quindi è possibile pianificare le azioni per il miglioramento della protezione.

Informazioni sui tipi di monitoraggio e generazione di rapporti

Le informazioni sugli eventi di sicurezza nella rete di un'organizzazione sono archiviate nel database di Administration Server. In base agli eventi, Kaspersky Security Center Cloud Console fornisce i seguenti tipi di monitoraggio e generazione di rapporti nella rete dell'organizzazione:

- Dashboard
- Rapporti
- Selezioni eventi

Dashboard

Il dashboard consente di monitorare le tendenze relative alla sicurezza nella rete dell'organizzazione fornendo una visualizzazione grafica delle informazioni.

Rapporti

La funzionalità Rapporti consente di ottenere informazioni numeriche dettagliate sulla sicurezza della rete dell'organizzazione, nonché di salvare le informazioni in un file, inviarlo tramite e-mail e stamparlo.

Selezioni eventi

Le selezioni eventi consentono di visualizzare i set denominati degli eventi selezionati dal database di Administration Server. Questi set di eventi sono raggruppati in base alle seguenti categorie:

- In base al livello di importanza: **Eventi critici**, **Errori funzionali**, **Avvisi** e **Eventi informativi**
- In base al tempo: **Eventi recenti**
- In base al tipo: **Richieste utente** e **Eventi di controllo**

È possibile creare e visualizzare le selezioni eventi definite dall'utente in base alle impostazioni disponibili per la configurazione nell'interfaccia di Kaspersky Security Center Cloud Console.

Dashboard e widget

Questa sezione contiene informazioni sul dashboard e sui widget forniti dal dashboard. La sezione include istruzioni su come gestire i widget e configurare le impostazioni dei widget.

Utilizzo del dashboard

Il dashboard consente di monitorare le tendenze relative alla sicurezza nella rete dell'organizzazione fornendo una visualizzazione grafica delle informazioni.

Il dashboard è disponibile in Kaspersky Security Center Cloud Console, nella sezione **Monitoraggio e generazione dei rapporti**, facendo clic su **Dashboard**.

Il dashboard fornisce widget che possono essere personalizzati. È possibile scegliere tra numerosi widget diversi, presentati come grafici a torta o grafici ad anello, tabelle, grafici, grafici a barre ed elenchi. Le informazioni visualizzate nei widget vengono aggiornate automaticamente, il periodo di aggiornamento è di uno o due minuti. L'intervallo tra gli aggiornamenti varia per i diversi widget. È possibile aggiornare manualmente i dati in un widget in qualsiasi momento tramite il menu delle impostazioni.

Per impostazione predefinita, i widget includono informazioni su tutti gli eventi archiviati nel database di Administration Server.

Kaspersky Security Center Cloud Console dispone di un set predefinito di widget per le seguenti categorie:

- **Stato protezione**
- **Distribuzione**
- **Aggiornamento**
- **Statistiche delle minacce**
- **Altro**

Alcuni widget contengono informazioni di testo con collegamenti. È possibile visualizzare informazioni dettagliate facendo clic su un collegamento.

Quando si configura il dashboard, è possibile aggiungere i widget desiderati, nascondere i widget non necessari, modificare le dimensioni o l'aspetto dei widget, spostare i widget e modificarne le impostazioni.

Aggiunta di widget al dashboard

Per aggiungere widget al dashboard:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sul pulsante **Aggiungi o ripristina widget Web**.
3. Nell'elenco dei widget disponibili selezionare i widget che si desidera aggiungere al dashboard.

   I widget sono raggruppati per categoria. Per visualizzare l'elenco dei widget inclusi in una categoria, fare clic sull'icona della freccia di espansione (>) accanto al nome della categoria.
4. Fare clic sul pulsante **Aggiungi**.

I widget selezionati verranno aggiunti alla fine del dashboard.

Ora è possibile modificare la rappresentazione e i parametri dei widget aggiunti.

Occultamento di un widget dal dashboard

Per nascondere un widget visualizzato dal dashboard:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera nascondere.
3. Selezionare **Nascondi widget Web**.
4. Nella finestra **Avviso** visualizzata fare clic su **OK**.

Il widget selezionato verrà nascosto. In seguito, è possibile aggiungere nuovamente il widget al dashboard.

Spostamento di un widget nel dashboard

Per spostare un widget nel dashboard:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera spostare.
3. Selezionare **Sposta**.
4. Fare clic sul punto in cui si desidera spostare il widget. È possibile selezionare solo un altro widget.

Le posizioni dei widget selezionati vengono scambiate.

Modifica delle dimensioni o dell'aspetto del widget

Per i widget che visualizzano un grafico, è possibile modificarne la rappresentazione: un grafico a barre o un grafico a linee. Per alcuni widget è possibile modificare le dimensioni: Compatto, Medio o Massimo.

Per modificare la rappresentazione del widget:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera modificare.
3. Eseguire una delle seguenti operazioni:
   - Per visualizzare il widget come grafico a barre, selezionare **Tipo di grafico: barre**.
   - Per visualizzare il widget come grafico a linee, selezionare **Tipo di grafico: linee**.
   - Per modificare l'area occupata dal widget, selezionare uno dei valori:
     - **Compatto**
     - **Compatto (solo barra)**
     - **Medio (grafico ad anello)**
     - **Medio (grafico a barre)**
     - **Massimo**

La rappresentazione del widget selezionato verrà modificata.

Modifica delle impostazioni del widget

Per modificare le impostazioni di un widget:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera modificare.
3. Selezionare **Mostra impostazioni**.
4. Nella finestra delle impostazioni del widget visualizzata modificare le impostazioni del widget come richiesto.
5. Fare clic su **Salva** per salvare le modifiche.

Le impostazioni del widget selezionato verranno modificate.

Il set di impostazioni dipende dallo specifico widget. Di seguito sono riportate alcune delle impostazioni comuni:

- **Ambito del widget Web** (il set di oggetti per cui il widget visualizza informazioni), ad esempio un gruppo di amministrazione o una selezione dispositivi.
- **Seleziona attività** (l'attività per cui il widget visualizza informazioni).
- **Intervallo** (l'intervallo di tempo per cui le informazioni vengono visualizzate nel widget): tra le due date specificate, dalla data specificata al giorno corrente o dal giorno corrente meno il numero di giorni specificato al giorno corrente.
- **Imposta su Critico se è specificato** e **Imposta su Avviso se è specificato** (le regole che determinano il colore di un indicatore a semaforo).

Dopo aver modificato le impostazioni del widget, è possibile aggiornare manualmente i dati nel widget.

Per aggiornare i dati su un widget:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera spostare.
3. Selezionare **Aggiorna**.

I dati nel widget vengono aggiornati.

Informazioni sulla modalità Solo dashboard

È possibile configurare la modalità Solo dashboard per i dipendenti che non gestiscono la rete ma che desiderano visualizzare le statistiche di protezione della rete in Kaspersky Security Center Cloud Console (ad esempio un Top Manager). Con questa modalità abilitata, l'utente visualizza solo un dashboard con un set predefinito di widget. L'utente può quindi monitorare le statistiche specificate nei widget, ad esempio lo stato di protezione di tutti i dispositivi gestiti, il numero di minacce rilevate di recente o l'elenco delle minacce più frequenti nella rete.

Quando un utente usa la modalità Solo dashboard, vengono applicate le seguenti restrizioni:

- Il menu principale non viene mostrato all'utente, che non potrà quindi modificare le impostazioni di protezione della rete.
- L'utente non può eseguire alcuna azione con i widget, ad esempio aggiungerli o nasconderli. È pertanto necessario inserire tutti i widget necessari per l'utente nel dashboard e configurarli, ad esempio impostando la regola di conteggio degli oggetti o specificando l'intervallo di tempo.

Non è possibile assegnare a se stessi la modalità Solo dashboard. Se si desidera utilizzare questa modalità, contattare un amministratore di sistema, un MSP (Managed Service Provider) o un utente con il diritto **Modifica elenchi di controllo degli accessi agli oggetti** nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

Configurazione della modalità Solo dashboard

Prima di iniziare a configurare la modalità Solo dashboard, assicurarsi che vengano soddisfatti i seguenti prerequisiti:

- L'utente dispone del diritto **Modifica elenchi di controllo degli accessi agli oggetti** nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**. Se non si dispone di questo diritto, la scheda per la configurazione della modalità non sarà presente.
- L'utente ha il diritto **Lettura** nell'area funzionale **Caratteristiche generali: Funzionalità di base**.

Se nella rete è organizzata una gerarchia di Administration Server, per configurare la modalità Solo dashboard passare al Server in cui è disponibile l'account utente nella sezione **Utenti** tab of the **Utenti e ruoli** → **Utenti e gruppi**. Può trattarsi di un server primario o di un server secondario fisico. Non è possibile regolare la modalità in un server virtuale.

Per configurare la modalità Solo dashboard:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account utente per il quale si desidera modificare il dashboard con i widget.
3. Nella finestra delle impostazioni dell'account visualizzata selezionare la scheda **Dashboard**.

   Nella scheda aperta viene visualizzato lo stesso dashboard dell'utente.
4. Se l'opzione **Visualizza la console in modalità Solo dashboard** è abilitata, spostare l'interruttore per disabilitarla.

   Quando questa opzione è abilitata, non è nemmeno possibile modificare il dashboard. Dopo aver disabilitato l'opzione, è possibile gestire i widget.
5. Configurare l'aspetto del dashboard. Il set di widget preparato nella scheda **Dashboard** è disponibile per l'utente con l'account personalizzabile. L'utente non può modificare in alcun modo le impostazioni o le dimensioni dei widget, né aggiungere o rimuovere widget dal dashboard. È pertanto opportuno modificarli per l'utente, in modo che possa visualizzare le statistiche sulla protezione della rete. A tale scopo, nella scheda **Dashboard** è possibile eseguire con i widget le stesse azioni della sezione **Monitoraggio e generazione dei rapporti** → **Dashboard**:
   - Aggiungere nuovi widget al dashboard.
   - Nascondere i widget di cui l'utente non ha bisogno.
   - Spostare i widget in un ordine specifico.
   - Modificare le dimensioni o l'aspetto dei widget.
   - Modificare le impostazioni dei widget.
6. Spostare l'interruttore per abilitare l'opzione **Visualizza la console in modalità Solo dashboard**.

   Successivamente, sarà disponibile solo il dashboard per l'utente. Quest'ultimo può monitorare le statistiche ma non può modificare le impostazioni di protezione della rete e l'aspetto del dashboard. Poiché viene visualizzato lo stesso dashboard che appare all'utente, non è possibile modificarlo.

   Se si mantiene l'opzione disabilitata, viene visualizzato il menu principale per l'utente, in modo che possa eseguire varie azioni in Kaspersky Security Center Cloud Console, inclusa la modifica delle impostazioni di protezione e dei widget.
7. Fare clic sul pulsante **Salva** al termine della configurazione della modalità Solo dashboard. Solo successivamente l'utente visualizzerà il dashboard preconfigurato.
8. Se l'utente desidera visualizzare le statistiche delle applicazioni Kaspersky supportate e ha bisogno dei diritti di accesso per farlo, configurare i diritti per l'utente. Successivamente, l'utente può visualizzare i dati delle

applicazioni Kaspersky nei widget di queste applicazioni.

Adesso l'utente può accedere a Kaspersky Security Center Cloud Console con l'account personalizzato e monitorare le statistiche di protezione della rete in modalità Solo dashboard.

Rapporti

Questa sezione descrive come utilizzare i rapporti, gestire i modelli di rapporti personalizzati, utilizzare i modelli di rapporti per generarne di nuovi e creare attività di distribuzione dei rapporti.

Utilizzo dei rapporti

La funzionalità Rapporti consente di ottenere informazioni numeriche dettagliate sulla sicurezza della rete dell'organizzazione, nonché di salvare le informazioni in un file, inviarlo tramite e-mail e stamparlo.

I rapporti sono disponibili in Kaspersky Security Center Cloud Console, nella sezione **Monitoraggio e generazione dei rapporti**, facendo clic su **Rapporti**.

Per impostazione predefinita, i rapporti includono informazioni relative agli ultimi 30 giorni.

Kaspersky Security Center Cloud Console dispone di un set predefinito di rapporti per le seguenti categorie:

- **Stato protezione**
- **Distribuzione**
- **Aggiornamento**
- **Statistiche delle minacce**
- **Altro**

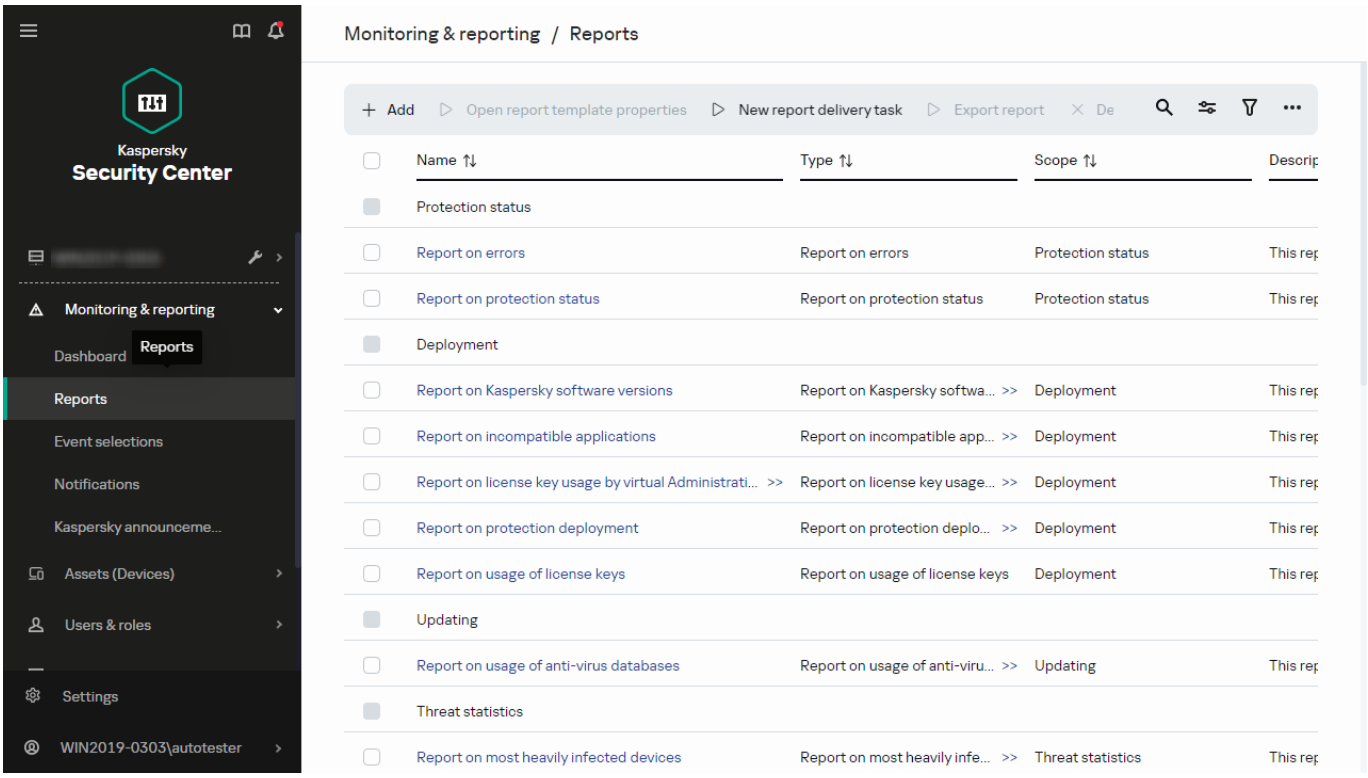
È possibile creare modelli di rapporto personalizzati, modificare i modelli di rapporto ed eliminarli.

È possibile creare rapporti basati su modelli esistenti, esportare i rapporti in file e creare attività per l'invio dei rapporti.

Creazione di un modello di rapporto

Per creare un modello di rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.

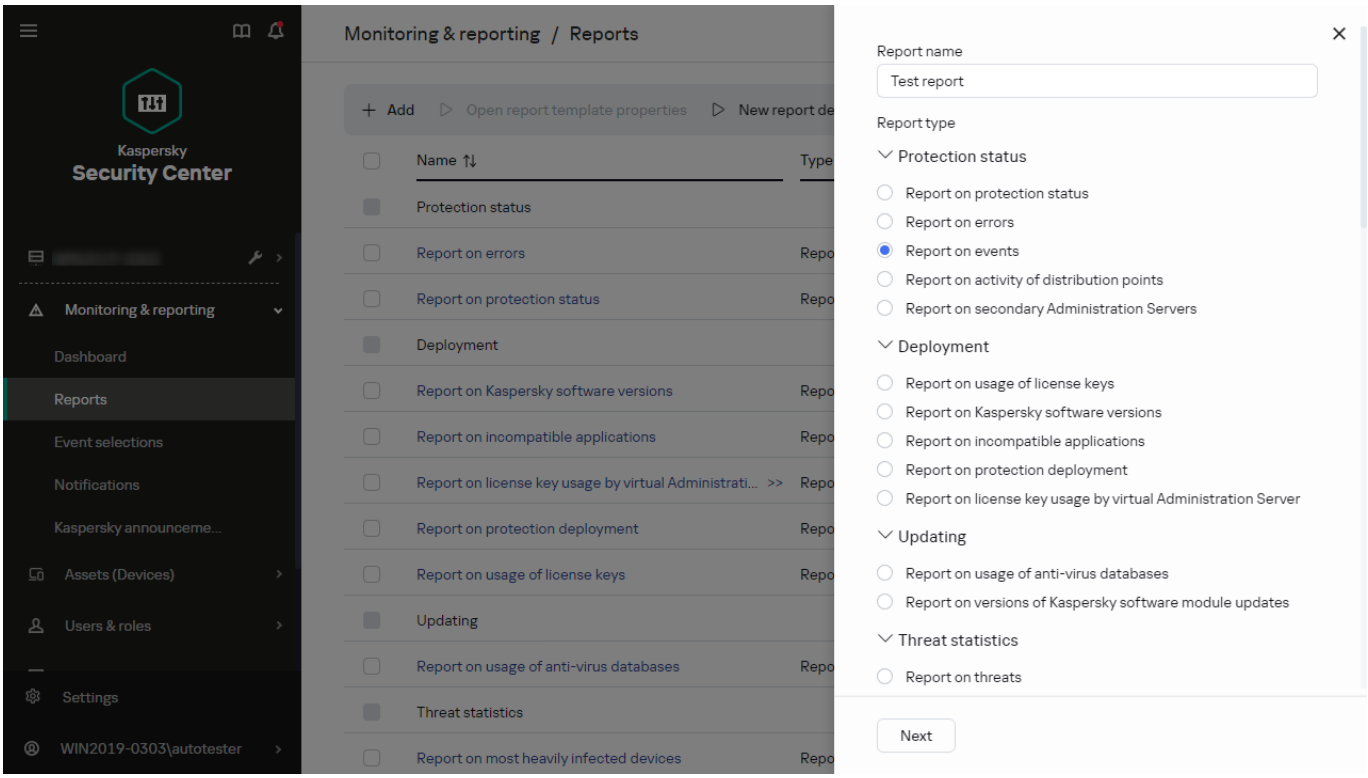


L'elenco dei modelli di rapporti nella sottosezione Rapporti

2. Fare clic su **Aggiungi**.

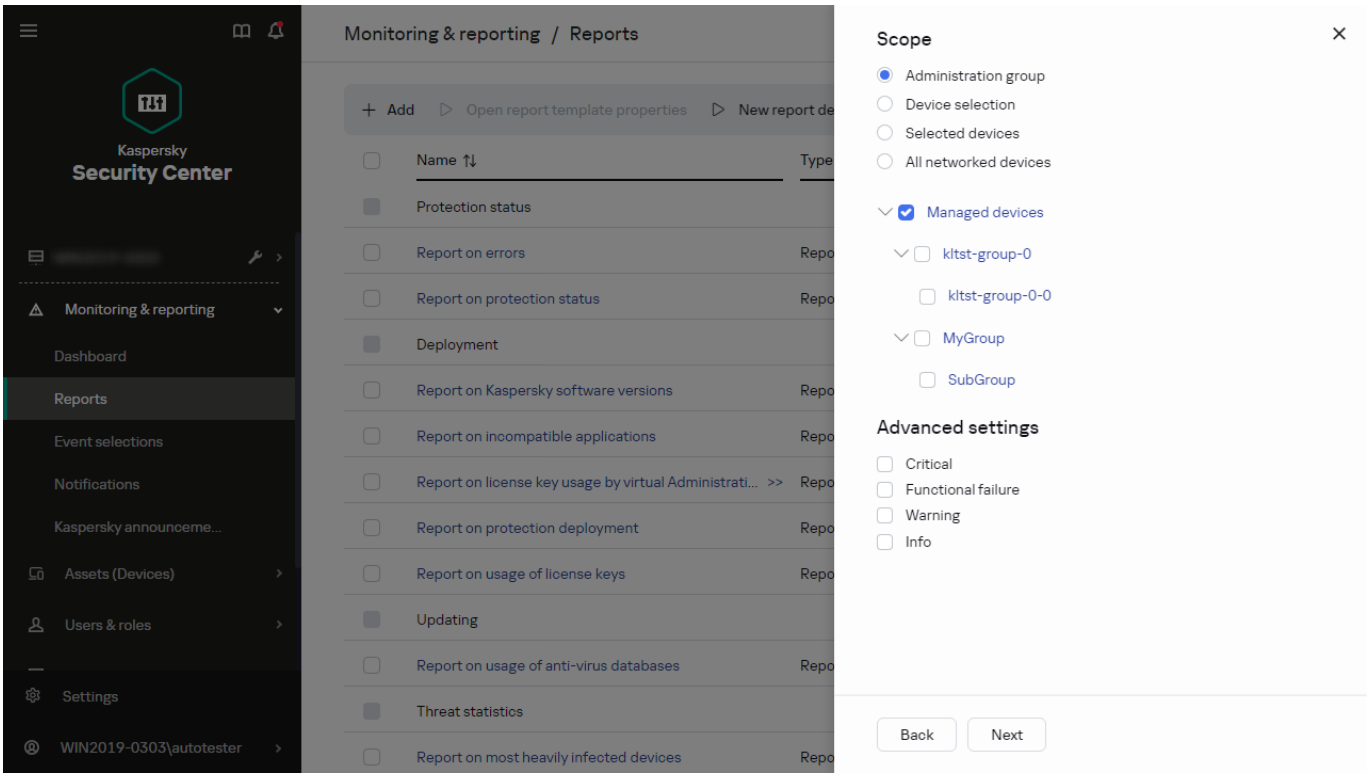
   Verrà avviata la Creazione guidata nuovo modello di rapporto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nella prima pagina della procedura guidata, immettere il nome del rapporto e selezionare il tipo di rapporto.



Creazione guidata nuovo modello di rapporto. Indicazione del nome e del tipo del modello di rapporto

4. Nella pagina **Ambito** della procedura guidata selezionare il set di dispositivi client (gruppo di amministrazione, selezione dispositivi, dispositivi selezionati o tutti i dispositivi nella rete) per cui visualizzare i dati nei rapporti basati su questo modello di rapporto.

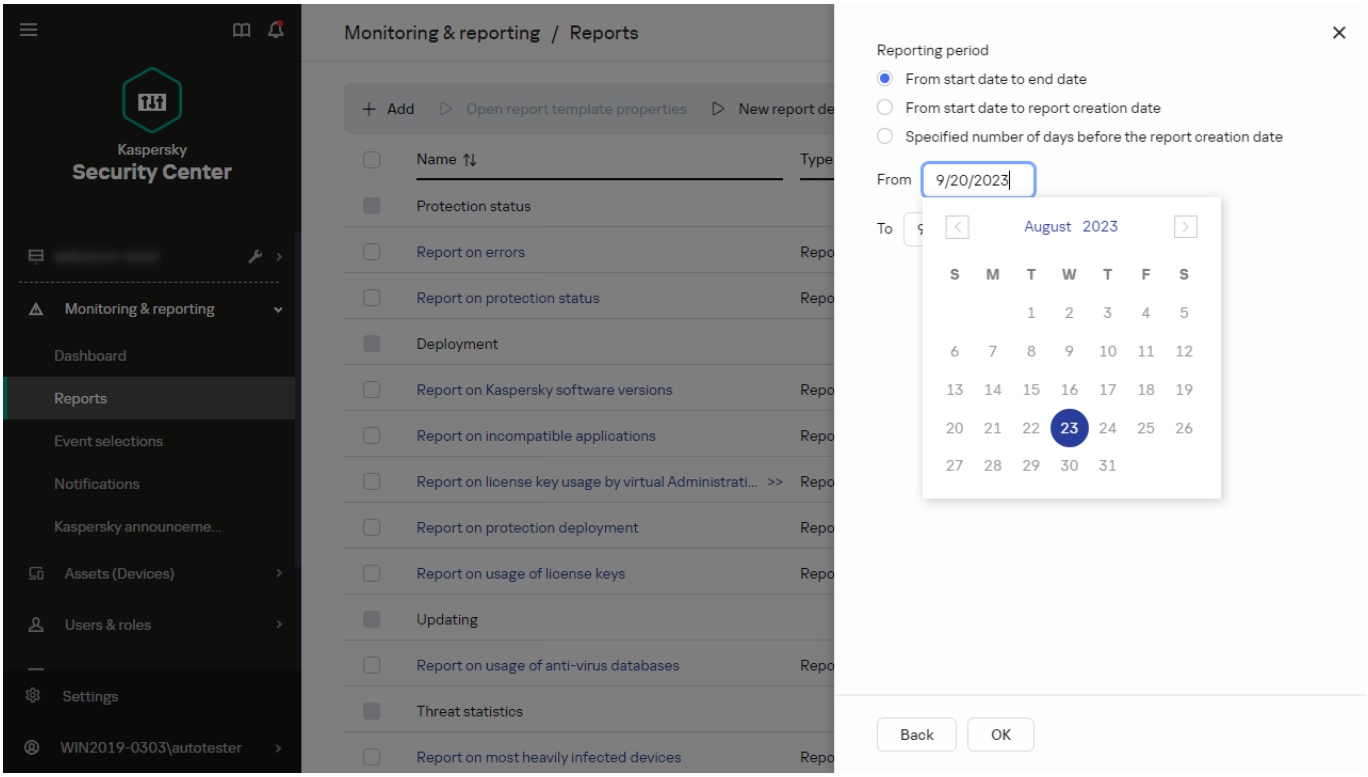


Creazione guidata nuovo modello di rapporto. Indicazione dell'ambito del modello di rapporto

5. Nella pagina **Periodo di generazione del rapporto** della procedura guidata specificare il periodo del rapporto. I valori disponibili sono i seguenti:

   - Tra le due date specificate
   - Dalla data specificata alla data di creazione del rapporto
   - Dalla data di creazione del rapporto meno il numero specificato di giorni alla data di creazione del rapporto

   Questa pagina potrebbe non essere visualizzata per alcuni rapporti.



Creazione guidata nuovo modello di rapporto. Indicazione del periodo di riferimento

6. Fare clic su **OK** per chiudere la procedura guidata.

7. Eseguire una delle seguenti operazioni:

   - Fare clic sul pulsante **Salva ed esegui** per salvare il nuovo modello di rapporto ed eseguire un rapporto basato su di esso.

     Il modello di rapporto verrà salvato. Il rapporto verrà generato.

   - Fare clic sul pulsante **Salva** per salvare il nuovo modello di rapporto.

     Il modello di rapporto verrà salvato.

È possibile utilizzare il nuovo modello per la creazione e la visualizzazione dei rapporti.

Visualizzazione e modifica delle proprietà dei modelli di rapporto

È possibile visualizzare e modificare le proprietà di base di un modello di rapporto, ad esempio il nome del modello di rapporto o i campi visualizzati nel rapporto.

Per visualizzare e modificare le proprietà di un modello di rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.

2. Selezionare la casella di controllo accanto al modello di rapporto per cui si desidera visualizzare e modificare le proprietà.

   In alternativa, è possibile generare il rapporto e quindi fare clic sul pulsante **Modifica**.

3. Fare clic sul pulsante **Apri proprietà del modello di rapporto**.

   Verrà visualizzata la finestra **Modifica del rapporto <Nome rapporto>** con la scheda **Generale** selezionata.

4. Modificare le proprietà del modello di rapporto:

   - Scheda **Generale**:

     - Nome del modello di rapporto

     - Numero massimo di voci da visualizzare

Se questa opzione è abilitata, il numero di voci visualizzate nella tabella con i dati dettagliati del rapporto non supera il valore specificato. Si noti che questa opzione non influisce sul numero massimo di eventi che è possibile includere nel rapporto quando si esporta il rapporto in un file.

Le voci nei rapporti vengono prima ordinate in base alle regole specificate nella sezione **Campi** → **Campi dettagli** delle proprietà del modello di rapporto, quindi vengono mantenute solo le prime voci risultanti. Il titolo della tabella con i dati dettagliati del rapporto mostra il numero di voci visualizzate e il numero totale di voci disponibili, corrispondenti alle altre impostazioni del modello di rapporto.

Se questa opzione è disabilitata, la tabella con i dati dettagliati del rapporto conterrà tutte le voci disponibili. Non è consigliabile disabilitare questa opzione. La limitazione del numero di voci visualizzate nel rapporto consente di ridurre il carico sul sistema di gestione database (DBMS) e il tempo necessario per la creazione e l'esportazione del rapporto. Alcuni rapporti contengono un numero eccessivo di voci. In questi casi, potrebbe essere difficile leggerle e analizzarle tutte. Inoltre, nel dispositivo potrebbe verificarsi l'esaurimento della memoria durante la generazione di un rapporto e, in questo caso, non sarà possibile visualizzare il rapporto.

Per impostazione predefinita, questa opzione è abilitata. Il valore predefinito è 1000.

Tenere presente che l'interfaccia di Kaspersky Security Center Cloud Console può visualizzare al massimo 2500 voci. Se è necessario visualizzare un numero maggiore di eventi, utilizzare la funzionalità di esportazione dei rapporti.

- **Gruppo**

  Fare clic sul pulsante **Impostazioni** per modificare il set di dispositivi client per cui viene creato il rapporto. Per alcuni tipi di rapporti, il pulsante potrebbe non essere disponibile. Le impostazioni effettive dipendono dalle impostazioni specificate durante la creazione del modello di rapporto.

- **Intervallo**

  Fare clic sul pulsante **Impostazioni** per modificare il periodo del rapporto. Per alcuni tipi di rapporti, il pulsante potrebbe non essere disponibile. I valori disponibili sono i seguenti:

  - Tra le due date specificate
  - Dalla data specificata alla data di creazione del rapporto
  - Dalla data di creazione del rapporto meno il numero specificato di giorni alla data di creazione del rapporto

- Includi i dati degli Administration Server secondari e virtuali

  Se questa opzione è abilitata, il rapporto include le informazioni ottenute dagli Administration Server secondari e virtuali subordinati all'Administration Server per cui viene creato il modello di rapporto.

  Disabilitare questa opzione per visualizzare solo i dati relativi all'Administration Server corrente.

  Per impostazione predefinita, questa opzione è abilitata.

- Fino al livello di nidificazione

  Il rapporto include i dati degli Administration Server secondari e virtuali posizionati al di sotto dell'Administration Server corrente a un livello di nidificazione minore o uguale al valore specificato.

  Il valore predefinito è 1. È consigliabile modificare questo valore se è necessario recuperare informazioni da Administration Server secondari posizionati a livelli inferiori della struttura.

- Intervallo di attesa dati (min.)

Prima della generazione del rapporto, l'Administration Server per cui viene creato il modello di rapporto attende i dati dagli Administration Server secondari per il numero di minuti specificato. Se non viene ricevuto alcun dato da un Administration Server secondario al termine di questo periodo, il rapporto viene eseguito comunque. Anziché i dati effettivi, il rapporto mostra i dati recuperati dalla cache (se è abilitata l'opzione **Salva nella cache i dati degli Administration Server secondari**) oppure **N/D** (non disponibile) in caso contrario.

Il valore predefinito è 5 (minuti).

- Salva nella cache i dati degli Administration Server secondari

  Gli Administration Server secondari trasferiscono regolarmente i dati all'Administration Server per cui viene creato il modello di rapporto. I dati trasferiti vengono quindi archiviati nella cache.

  Se l'Administration Server corrente non riesce a ricevere i dati da un Administration Server secondario durante la generazione del rapporto, il rapporto mostra i dati recuperati dalla cache. Verrà anche visualizzata la data in cui i dati sono stati trasferiti nella cache.

  Se questa opzione è abilitata, è possibile visualizzare le informazioni dagli Administration Server secondari, anche se non è possibile recuperare i dati aggiornati. I dati visualizzati potrebbero tuttavia essere obsoleti.

  Per impostazione predefinita, questa opzione è disabilitata.

- Frequenza di aggiornamento cache (ore)

  A intervalli regolari gli Administration Server secondari trasferiscono i dati all'Administration Server per cui viene creato il modello di rapporto. È possibile specificare questo periodo in ore. Se si specificano 0 ore, i dati vengono trasferiti solo al momento della generazione del rapporto.

  Il valore predefinito è 0.

- Trasferisci informazioni dettagliate dagli Administration Server secondari

  Nel rapporto generato, la tabella con i dati dettagliati del rapporto include i dati ottenuti dagli Administration Server secondari dell'Administration Server per cui viene creato il modello di rapporto.

  L'abilitazione di questa opzione rallenta la generazione dei rapporti e aumenta il traffico tra gli Administration Server. È tuttavia possibile visualizzare tutti i dati in un solo rapporto.

  Anziché attivare questa opzione, può essere preferibile analizzare i dati dettagliati del rapporto per identificare un Administration Server secondario che presenta problemi e quindi generare lo stesso rapporto solo per tale Administration Server.

  Per impostazione predefinita, questa opzione è disabilitata.

- Scheda **Campi**

  Selezionare i campi che verranno visualizzati nel rapporto e utilizzare i pulsanti **Sposta su** e **Sposta giù** per modificare l'ordine dei campi. Utilizzare il pulsante **Aggiungi** o **Modifica** per specificare se le informazioni nel rapporto devono essere ordinate e filtrate in base a ciascuno dei campi.

  Nella sezione **Filtri di Campi dettagli** è inoltre possibile fare clic sul pulsante **Converti filtri** per iniziare a utilizzare il formato di filtro esteso. Questo formato consente di combinare le condizioni di filtro specificate in vari campi utilizzando l'operatore logico OR. Dopo aver fatto clic sul pulsante, il pannello **Converti filtri** si aprirà a destra. Fare clic sul pulsante **Converti filtri** per confermare la conversione. Adesso è possibile definire un filtro convertito con condizioni dalla sezione **Campi dettagli** che vengono applicate utilizzando l'operatore logico OR.

La conversione di un rapporto nel formato che supporta condizioni di filtro complesse renderà il rapporto incompatibile con le versioni precedenti di Kaspersky Security Center (11 e precedenti). Inoltre, il rapporto convertito non conterrà alcun dato degli Administration Server secondari che eseguono le versioni incompatibili.

5. Fare clic su **Salva** per salvare le modifiche.
6. Chiudere la finestra **Modifica del rapporto <nome rapporto>**.

Il modello di rapporto aggiornato verrà visualizzato nell'elenco dei modelli di rapporto.

Esportazione di un rapporto in un file

È possibile salvare uno o più rapporti in formato XML, HTML o PDF. Kaspersky Security Center Cloud Console consente di esportare contemporaneamente fino a 10 rapporti in file del formato specificato.

Per esportare un rapporto in un file:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Scegliere i rapporti da esportare.

   Se si scelgono più di 10 rapporti, il pulsante **Esporta rapporto** verrà disabilitato.
3. Fare clic sul pulsante **Esporta rapporto**.
4. Nella finestra visualizzata, specificare i seguenti parametri di esportazione:

   - **Nome file**.

     Se si seleziona un rapporto da esportare, specificare il nome del file del rapporto.

     Se si seleziona più di un rapporto, i nomi dei file dei rapporti coincideranno con il nome dei modelli di rapporto selezionati.

   - **Numero massimo di voci**.

     Specificare il numero massimo di voci incluse nel file del rapporto. Il valore predefinito è 10.000.

   - **Formato file**.

     Selezionare il formato del file del rapporto: XML, HTML o PDF. Se si esportano più rapporti, tutti i rapporti selezionati vengono salvati nel formato specificato come file separati.
5. Fare clic sul pulsante **Esporta rapporto**.

Il rapporto viene salvato in un file nel formato specificato.

Generazione e visualizzazione di un rapporto

Per creare e visualizzare un rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Fare clic sul nome del modello di rapporto che si desidera utilizzare per creare un rapporto.

Verrà generato e visualizzato un rapporto che utilizza il modello selezionato.

I dati del rapporto vengono visualizzati solo in inglese; altre localizzazioni non sono disponibili.

Il rapporto include i seguenti dati:

- Nella scheda **Riepilogo**:
  - Nome e tipo di rapporto, breve descrizione e periodo di generazione del rapporto, oltre che informazioni sul gruppo di dispositivi per cui è stato generato il rapporto.
  - Grafico con i dati più significativi del rapporto.
  - Tabella consolidata con indicatori del rapporto calcolati.
- Nella scheda **Dettagli** viene visualizzata una tabella con dati dettagliati sul rapporto.

Creazione di un'attività di invio dei rapporti

È possibile creare un'attività per l'invio dei rapporti selezionati.

Per creare un'attività di invio dei rapporti:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. [Facoltativo] Selezionare le caselle di controllo accanto ai modelli di rapporto per cui si desidera creare un'attività di invio dei rapporti.
3. Fare clic sul pulsante **Nuova attività di invio rapporti**.
4. Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
5. Nella prima pagina della procedura guidata immettere il nome dell'attività. Il nome predefinito è **Invia rapporti (<N>)**, dove <N> è il numero progressivo dell'attività.
6. Nella pagina delle impostazioni dell'attività della procedura guidata specificare le seguenti impostazioni:
   a. Modelli di rapporti che devono essere inviati dall'attività. Se sono stati selezionati nel passaggio 2, ignorare questo passaggio.
   b. Formato del rapporto: HTML, XLS o PDF.
   c. Se i rapporti devono essere inviati tramite e-mail, insieme alle impostazioni di notifica tramite e-mail.
7. Se si desidera modificare altre impostazioni dell'attività dopo averla creata, nella pagina **Completa creazione attività** della procedura guidata abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione**.

8. Fare clic sul pulsante **Crea** per creare l'attività e chiudere la procedura guidata.

   Verrà creata l'attività di invio dei rapporti. Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata la finestra delle impostazioni dell'attività.

Eliminazione di modelli di rapporto

Per eliminare uno o più modelli di rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Selezionare le caselle di controllo accanto ai modelli di rapporto che si desidera eliminare.
3. Fare clic sul pulsante **Elimina**.
4. Nella finestra visualizzata fare clic su **OK** per confermare la selezione.

I modelli di rapporto selezionati verranno eliminati. Se questi modelli di rapporto sono stati inclusi nelle attività di invio dei rapporti, verranno rimossi anche dalle attività.

Eventi e selezioni di eventi

Questa sezione fornisce informazioni sugli eventi e sulle selezioni di eventi, sui tipi di eventi che si verificano nei componenti di Kaspersky Security Center Cloud Console e sulla gestione del blocco degli eventi frequenti.

Informazioni sugli eventi in Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Le informazioni sugli eventi vengono salvate nel database di Administration Server. È possibile esportare queste informazioni in sistemi SIEM esterni. L'esportazione delle informazioni sugli eventi nei sistemi SIEM esterni consente agli amministratori dei sistemi SIEM di rispondere tempestivamente agli eventi del sistema di protezione che si verificano nei dispositivi o nei gruppi di dispositivi gestiti.

Eventi in base al tipo

In Kaspersky Security Center Cloud Console sono disponibili i seguenti tipi di eventi:

- Eventi generici. Questi eventi si verificano in tutte le applicazioni Kaspersky gestite. Un esempio di evento generico è l'Epidemia di virus. Gli eventi generici hanno sintassi e semantica rigorosamente definite. Gli eventi generici vengono ad esempio utilizzati nei rapporti e nei dashboard.
- Eventi specifici delle applicazioni gestiti da Kaspersky. Ogni applicazione Kaspersky gestita dispone di uno specifico set di eventi.

Eventi in base alla sorgente

È possibile visualizzare l'elenco completo degli eventi che possono essere generati da un'applicazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare l'elenco degli eventi nelle proprietà dell'Administration Server.

Gli eventi possono essere generati dalle seguenti applicazioni:

- Componenti di Kaspersky Security Center Cloud Console:
  - Administration Server
  - Network Agent
- Applicazioni Kaspersky gestite

  Per i dettagli sugli eventi generati dalle applicazioni gestite da Kaspersky, consultare la documentazione dell'applicazione corrispondente.

Eventi in base al livello di importanza

Ogni evento dispone di uno specifico livello di importanza. In base alle condizioni in cui si verifica, a un evento possono essere assegnati diversi livelli di importanza. Esistono quattro livelli di importanza degli eventi:

- Un *evento critico* è un evento che indica la presenza di un problema critico che può determinare una perdita dei dati, un malfunzionamento o un errore critico.
- Un *errore funzionale* è un evento che indica la presenza di un problema grave, un errore o un malfunzionamento che si è verificato durante l'esecuzione dell'applicazione o di una procedura.
- Un *avviso* è un evento che non è necessariamente grave, ma indica comunque un potenziale problema futuro. La maggior parte degli eventi viene designata come avviso se l'applicazione può essere ripristinata senza perdite di dati o funzionalità importanti dopo che si sono verificati tali eventi.
- Un *evento informativo* è un evento che si verifica allo scopo di segnalare il completamento di un'operazione, il corretto funzionamento dell'applicazione o il completamento di una procedura.

Ogni evento ha un periodo di archiviazione definito, durante il quale può essere visualizzato o modificato in Kaspersky Security Center Cloud Console. Alcuni eventi non vengono salvati nel database di Administration Server per impostazione predefinita, poiché il relativo periodo di archiviazione definito è pari a zero. Solo gli eventi che verranno memorizzati nel database di Administration Server per almeno un giorno possono essere esportati in sistemi esterni.

Eventi dei componenti di Kaspersky Security Center Cloud Console

Ogni componente Kaspersky Security Center Cloud Console dispone di uno specifico set di tipi di eventi. Questa sezione elenca i tipi di eventi che si verificano nell'Administration Server di Kaspersky Security Center Cloud Console e in Network Agent. I tipi di eventi che si verificano nelle applicazioni Kaspersky non sono elencati in questa sezione.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Struttura dei dati della descrizione del tipo di evento

Per ogni tipo di evento, sono indicati il relativo nome visualizzato, l'identificatore (ID), il codice alfabetico, la descrizione e il periodo di archiviazione predefinito.

- **Nome visualizzato del tipo di evento**. Questo testo è visualizzato in Kaspersky Security Center Cloud Console durante la configurazione degli eventi e quando gli eventi si verificano.
- **ID del tipo di evento**. Questo codice numerico viene utilizzato durante l'elaborazione degli eventi tramite strumenti di terzi per l'analisi degli eventi.
- **Tipo di evento** (codice alfabetico). Questo codice viene utilizzato quando si esplorano e si elaborano gli eventi con le visualizzazione pubbliche disponibili nel database di Kaspersky Security Center Cloud Console.
- **Descrizione**. Questo testo contiene le situazioni in cui si verifica un evento e come procedere in questo caso.
- **Periodo di archiviazione predefinito**. Rappresenta il numero di giorni per cui l'evento viene memorizzato nel database di Administration Server ed è visualizzato nell'elenco degli eventi in Administration Server. Al termine di questo periodo, l'evento viene eliminato. Se il valore per il periodo di archiviazione degli eventi è 0, gli eventi vengono rilevati ma non sono visualizzati nell'elenco degli eventi in Administration Server.

Eventi di Administration Server

Questa sezione contiene informazioni sugli eventi relativi ad Administration Server.

Eventi critici di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Cloud Console Administration Server con il livello di importanza **Critico**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi critici di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo archiviazi predefin
È stato superato il limite di licenze	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Una volta al giorno Kaspersky Security Center Cloud Console verifica se è stata superata una limitazione di licenza.	180 giorni

			Gli eventi di questo tipo si verificano quando Administration Server rileva il superamento di alcune limitazioni di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client e se il numero delle unità di licensing attualmente utilizzate coperte da una singola licenza supera il 110% del numero totale di unità coperte dalla licenza. Anche quando si verifica questo evento, i dispositivi client sono protetti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare i dispositivi non in uso. • Fornire una licenza per più dispositivi (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). Kaspersky Security Center Cloud Console determina le regole per generare gli eventi quando viene superata una limitazione di licenza.	
Epidemia di virus	26 (per Protezione minacce file)	GNRL_EV_VIRUS_OUTBREAK	Gli eventi di questo tipo si verificano quando il numero di oggetti dannosi rilevati in più dispositivi gestiti	180 giorni

			supera il limite in un periodo di tempo limitato. È possibile rispondere all'evento nei seguenti modi: • Configurare la soglia nelle proprietà di Administration Server. • Creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.	
Epidemia di virus	27 (per Protezione minacce di posta)	GNRL_EV_VIRUS_OUTBREAK	Gli eventi di questo tipo si verificano quando il numero di oggetti dannosi rilevati in più dispositivi gestiti supera il limite in un periodo di tempo limitato. È possibile rispondere all'evento nei seguenti modi: • Configurare la soglia nelle proprietà di Administration Server. • Creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.	180 giorni
Epidemia di virus	28 (per firewall)	GNRL_EV_VIRUS_OUTBREAK	Gli eventi di questo tipo si verificano quando il numero di oggetti dannosi rilevati in più dispositivi gestiti supera il limite in un periodo di tempo limitato.	180 giorni

			È possibile rispondere all'evento nei seguenti modi: • Configurare la soglia nelle proprietà di Administration Server. • Creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.	
Il dispositivo è diventato non gestito	4111	KLSRV_HOST_OUT_CONTROL	Eventi di questo tipo si verificano se un dispositivo gestito è visibile nella rete ma non si connette ad Administration Server da un periodo di tempo specifico. Determinare il motivo che impedisce il corretto funzionamento di Network Agent nel dispositivo. Le cause possibili includono i problemi di rete e la rimozione di Network Agent dal dispositivo.	180 giorni
Lo stato del dispositivo è Critico	4113	KLSRV_HOST_STATUS_CRITICAL	Eventi di questo tipo si verificano quando a un dispositivo gestito viene assegnato lo stato *Critico*. È possibile configurare le condizioni in cui lo stato del dispositivo diventa *Critico*.	180 giorni
Modalità con funzionalità limitate	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Eventi di questo tipo si verificano quando Kaspersky Security Center Cloud Console viene avviato con funzionalità di base, senza le funzionalità Vulnerability e patch management e	180 giorni

			Mobile Device Management. Di seguito sono riportati i motivi dell'evento e le risposte appropriate: • Il periodo licenza è scaduto. Fornire una licenza per utilizzare la modalità con funzionalità complete di Kaspersky Security Center Cloud Console (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). • Administration Server gestisce più dispositivi rispetto a quanto previsto dalla limitazione licenza. Spostare i dispositivi dai gruppi di amministrazione di un Administration Server a quelli di un altro Administration Server (se la limitazione licenza dell'altro Administration Server lo consente).	
La licenza sta per scadere	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Eventi di questo tipo si verificano quando si avvicina la data di scadenza della licenza commerciale.	180 giorni

			Una volta al giorno Kaspersky Security Center verifica se si è in prossimità della data di scadenza della licenza. Gli eventi di questo tipo vengono pubblicati 30 giorni, 15 giorni, 5 giorni e 1 giorno prima della data di scadenza della licenza. Questo numero di giorni non può essere modificato. Se Administration Server è disattivato nel giorno specificato prima della data di scadenza della licenza, l'evento non verrà pubblicato fino al giorno successivo. Alla scadenza della licenza commerciale, Kaspersky Security Center Cloud Console fornisce solo le funzionalità di base. È possibile rispondere all'evento nei seguenti modi: • Verificare di aver aggiunto una chiave di licenza aggiuntiva ad Administration Server. • Se si utilizza un abbonamento, assicurarsi di rinnovarlo. L'abbonamento illimitato viene rinnovato automaticamente se il pagamento al provider di servizi è stato effettuato anticipatamente entro il termine.	
Il certificato è	4132	KLSRV_CERTIFICATE_EXPIRED	Le informazioni	180 giorni

scaduto			verranno aggiunte a breve.	
Gli aggiornamenti per i moduli software Kaspersky sono stati revocati	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Eventi di questo tipo si verificano se gli aggiornamenti immediati sono stati revocati (per questi aggiornamenti viene visualizzato lo stato *Revocato*) dagli esperti di Kaspersky perché, ad esempio, devono essere aggiornati a una versione più recente. L'evento riguarda le patch di Kaspersky Security Center Cloud Console e non riguarda i moduli delle applicazioni gestite di Kaspersky. L'evento indica come motivo che gli aggiornamenti immediati non sono installati.	180 giorni
Controllo: esportazione in SIEM non riuscita	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Eventi di questo tipo si verificano quando l'esportazione degli eventi nel sistema SIEM non è riuscita a causa di un errore di connessione con il sistema SIEM.	180 giorni

Eventi di errore funzionale di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Cloud Console Administration Server con il livello di importanza **Errore funzionale**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di errore funzionale di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Limite di installazioni superato per	4126	KLSRV_INVLICPROD_EXCEDED	Administration Server genera periodicamente eventi di questo tipo (ogni ora). Eventi di	180 giorni

uno dei gruppi di applicazioni concesse in licenza			questo tipo si verificano se in Kaspersky Security Center Cloud Console si gestiscono chiavi di licenza di applicazioni di terze parti e se il numero di installazioni ha superato il limite impostato dalla chiave di licenza dell'applicazione di terze parti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare l'applicazione di terzi dai dispositivi in cui non è in uso l'applicazione. • Utilizzare una licenza di terzi per altri dispositivi. È possibile gestire le chiavi di licenza di applicazioni di terzi utilizzando le funzionalità dei gruppi di applicazioni concesse in licenza. Un gruppo di applicazioni concesse in licenza include le applicazioni di terzi che soddisfano i criteri impostati dall'utente.	

Eventi di avviso di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Cloud Console Administration Server con il livello di importanza **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
È stato superato il limite di licenze	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una volta al giorno Kaspersky Security Center Cloud Console verifica se è stata superata una limitazione di licenza.	90 giorni

				Gli eventi di questo tipo si verificano quando Administration Server rileva il superamento di alcune limitazioni di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client e se il numero delle unità di licensing attualmente utilizzate coperte da una singola licenza costituisce dal 100% al 110% del numero totale di unità coperte dalla licenza. Anche quando si verifica questo evento, i dispositivi client sono protetti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare i dispositivi non in uso. • Fornire una licenza per più dispositivi (aggiungere un codice di attivazione valido o un file chiave ad Administration Server).

			Kaspersky Security Center Cloud Console determina le regole per generare gli eventi quando viene superata una limitazione di licenza.	
Il dispositivo è rimasto inattivo nella rete per molto tempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Le informazioni verranno aggiunte a breve.	90 giorni
Conflitto dei nomi di dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Le informazioni verranno aggiunte a breve.	90 giorni
Lo stato del dispositivo è Avviso	4114	KLSRV_HOST_STATUS_WARNING	Eventi di questo tipo si verificano quando a un dispositivo gestito viene assegnato lo stato *Avviso*. È possibile configurare le condizioni in cui lo stato del dispositivo diventa *Avviso*.	90 giorni
Il limite di installazioni sta per essere raggiunto per uno dei gruppi di applicazioni concesse in licenza	4127	KLSRV_INVLICPROD_FILLED	Le informazioni verranno aggiunte a breve.	90 giorni
Il certificato è stato richiesto	4133	KLSRV_CERTIFICATE_REQUESTED	Le informazioni verranno aggiunte a breve.	90 giorni
Il certificato è stato rimosso	4134	KLSRV_CERTIFICATE_REMOVED	Le informazioni verranno aggiunte a breve.	90 giorni
Il certificato APNs è scaduto	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Le informazioni verranno aggiunte a breve.	90 giorni
Il certificato APNs sta per scadere	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Le informazioni verranno aggiunte a breve.	90 giorni
Impossibile	4138	KLSRV_GCM_DEVICE_ERROR	Le informazioni	90 giorni

inviare il messaggio FCM al dispositivo mobile			verranno aggiunte a breve.	
Errore HTTP durante l'invio del messaggio FCM al server FCM	4139	KLSRV_GCM_HTTP_ERROR	Le informazioni verranno aggiunte a breve.	90 giorni
Impossibile inviare il messaggio FCM al server FCM	4140	KLSRV_GCM_GENERAL_ERROR	Le informazioni verranno aggiunte a breve.	90 giorni
La connessione all'Administration Server secondario è stata interrotta	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Le informazioni verranno aggiunte a breve.	90 giorni
La connessione all'Administration Server primario è stata interrotta	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Le informazioni verranno aggiunte a breve.	90 giorni
Proxy KSN avviato. Impossibile verificare la disponibilità di KSN	7719	KSNPROXY_STARTED_CON_CHK_FAILED	Le informazioni verranno aggiunte a breve.	90 giorni
Sono stati registrati nuovi aggiornamenti per i moduli software Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Le informazioni verranno aggiunte a breve.	90 giorni
Poiché è stato superato il limite relativo al numero di eventi nel database, è stata avviata l'eliminazione degli eventi	4145	KLSRV_EVP_DB_TRUNCATING	Eventi di questo tipo si verificano quando viene avviata l'eliminazione degli eventi precedenti dal database di Administration Server dopo il raggiungimento della capacità massima del database di Administration Server. È possibile rispondere all'evento nei seguenti modi:	90 giorni

			• Cambiare il numero massimo di eventi archiviati nel database di Administration Server. • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server.	
Poiché è stato superato il limite relativo al numero di eventi nel database, gli eventi sono stati eliminati	4146	KLSRV_EVP_DB_TRUNCATED	Eventi di questo tipo si verificano dopo l'eliminazione degli eventi precedenti dal database di Administration Server in seguito al raggiungimento della capacità massima del database di Administration Server. È possibile rispondere all'evento nei seguenti modi: • Cambiare il numero massimo consentito di eventi archiviati nel database di Administration Server. • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server.	90 giorni
La licenza sta per scadere	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Le informazioni verranno aggiunte a breve.	90 giorni

Controllo: test della connessione al server SIEM non riuscito	5120	KLAUD_EV_SIEM_TEST_FAILED	Eventi di questo tipo si verificano quando un test di connessione automatico al server SIEM non riesce.	90 giorni

Eventi informativi di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Cloud Console Administration Server con il livello di importanza **Informazioni**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi informativi di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Utilizzo della chiave di licenza superiore al 90%	4097	KLSRV_EV_LICENSE_CHECK_90	30 giorni
Nuovo dispositivo rilevato	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 giorni
Il dispositivo è stato spostato automaticamente in base a una regola	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 giorni
Il dispositivo è stato rimosso dal gruppo poiché inattivo nella rete per molto tempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 giorni
Sta per essere superato il limite di installazioni (è stato utilizzato più del 95%) per uno dei gruppi di applicazioni concesse in licenza	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 giorni
Sono disponibili alcuni file da inviare a Kaspersky per l'analisi	4131	KLSRV_APS_FILE_APPEARED	30 giorni
L'ID istanza FCM è stato modificato in questo dispositivo mobile	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 giorni
Aggiornamenti copiati nella cartella specificata	4122	KLSRV_UPD_REPL_OK	30 giorni
La connessione all'Administration Server secondario è stata stabilita	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 giorni
La connessione all'Administration Server primario è stata stabilita	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 giorni
I database sono stati aggiornati	4144	KLSRV_UPD_BASES_UPDATED	30 giorni

(In Kaspersky Security Center Cloud Console questo tipo di evento è disponibile solo per un Administration Server secondario.)			
Proxy KSN avviato. La verifica della disponibilità di KSN è stata completata	7718	KSNPROXY_STARTED_CON_CHK_OK	30 giorni
Proxy KSN arrestato	7720	KSNPROXY_STOPPED	30 giorni
Controllo: la connessione ad Administration Server è stata stabilita	4147	KLAUD_EV_SERVERCONNECT	30 giorni
Controllo: l'oggetto è stato modificato	4148	KLAUD_EV_OBJECTMODIFY	30 giorni
Controllo: lo stato dell'oggetto è stato modificato	4150	KLAUD_EV_TASK_STATE_CHANGED	30 giorni
Controllo: le impostazioni del gruppo sono state modificate	4149	KLAUD_EV_ADMGROUP_CHANGED	30 giorni
Controllo: le chiavi di criptaggio sono state importate o esportate da Administration Server	5100	KLAUD_EV_DPEKEYSEXPORT	30 giorni
Controllo (test della connessione al server SIEM riuscito)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 giorni

Eventi di Network Agent

Questa sezione contiene informazioni sugli eventi relativi a Network Agent.

Eventi di errore funzionale di Network Agent

La tabella seguente elenca gli eventi di Kaspersky Security Center Network Agent con il livello di criticità **Errore funzionale**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di errore funzionale di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Errore durante l'installazione dell'aggiornamento	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Gli eventi di questo tipo si verificano se l'installazione automatica di aggiornamenti e patch per i	30 giorni

			componenti Kaspersky Security Center Cloud Console non è andata a buon fine. L'evento non riguarda gli aggiornamenti delle applicazioni gestite Kaspersky. Leggere la descrizione dell'evento. Un problema di Windows in Administration Server potrebbe essere la causa dell'evento. Se nella descrizione vengono menzionati problemi relativi alla configurazione di Windows, risolvere il problema.	
Impossibile installare l'aggiornamento software di terze parti	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Gli eventi di questo tipo si verificano se sono in uso le funzionalità Vulnerability e patch management e Mobile Device Management e se l'aggiornamento del software di terze parti non è andato a buon fine. Verificare che il collegamento al software di terze parti sia valido. Leggere la descrizione dell'evento.	30 giorni
Impossibile installare gli aggiornamenti di Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Gli eventi di questo tipo si verificano se gli aggiornamenti di	30 giorni

			Windows non sono andati a buon fine. Configurare gli aggiornamenti di Windows in un criterio di Network Agent. Leggere la descrizione dell'evento. Cercare l'errore nella Microsoft Knowledge Base. Contattare il supporto tecnico Microsoft se non si riesce a risolvere autonomamente il problema.	

Eventi di avviso di Network Agent

La tabella seguente elenca gli eventi di Kaspersky Security Center Network Agent con il livello di gravità **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
È stato restituito un avviso durante l'installazione dell'aggiornamento dei moduli software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 giorni
Installazione dell'aggiornamento software di terze parti completata con un avviso	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 giorni
Installazione dell'aggiornamento software di terze parti rimandata	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 giorni
Si è verificato un problema di sicurezza	549	GNRL_EV_APP_INCIDENT_OCCURED	30 giorni
Proxy KSN avviato. Impossibile verificare la disponibilità di KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 giorni

Eventi informativi di Network Agent

La tabella seguente elenca gli eventi di Kaspersky Security Center Network Agent con il livello di gravità **Informazioni**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi informativi di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Installazione dell'aggiornamento per i moduli software completata	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 giorni
Installazione dell'aggiornamento per i moduli software avviata	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 giorni
Applicazione installata	7703	KLNAG_EV_INV_APP_INSTALLED	30 giorni
Applicazione rimossa	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 giorni
Applicazione monitorata installata	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 giorni
Applicazione monitorata rimossa	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 giorni
Applicazione di terze parti installata	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 giorni
Nuovo dispositivo aggiunto	7708	KLNAG_EV_DEVICE_ARRIVAL	30 giorni
Dispositivo rimosso	7709	KLNAG_EV_DEVICE_REMOVE	30 giorni
Dispositivo rilevato	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 giorni
Dispositivo autorizzato	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 giorni
Condivisione desktop Windows: file letto	7712	KLUSRLOG_EV_FILE_READ	30 giorni
Condivisione desktop Windows: file modificato	7713	KLUSRLOG_EV_FILE_MODIFIED	30 giorni
Condivisione desktop Windows: applicazione avviata	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 giorni
Condivisione desktop Windows: avviata	7715	KLUSRLOG_EV_WDS_BEGIN	30 giorni
Condivisione desktop Windows: arrestata	7716	KLUSRLOG_EV_WDS_END	30 giorni

Installazione dell'aggiornamento software di terze parti completata	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 giorni
Installazione dell'aggiornamento software di terze parti avviata	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 giorni
Proxy KSN avviato. La verifica della disponibilità di KSN è stata completata	7719	KSNPROXY_STARTED_CON_CHK_OK	30 giorni
Proxy KSN arrestato	7720	KSNPROXY_STOPPED	30 giorni

Utilizzo di selezioni eventi

Le selezioni eventi consentono di visualizzare i set denominati degli eventi selezionati dal database di Administration Server. Questi set di eventi sono raggruppati in base alle seguenti categorie:

- In base al livello di importanza: **Eventi critici**, **Errori funzionali**, **Avvisi** e **Eventi informativi**
- In base al tempo: **Eventi recenti**
- In base al tipo: **Richieste utente** e **Eventi di controllo**

È possibile creare e visualizzare le selezioni eventi definite dall'utente in base alle impostazioni disponibili per la configurazione nell'interfaccia di Kaspersky Security Center Cloud Console.

Le selezioni eventi sono disponibili in Kaspersky Security Center Cloud Console, nella sezione **Monitoraggio e generazione dei rapporti**, facendo clic su **Selezioni eventi**.

Per impostazione predefinita, le selezioni eventi includono informazioni relative agli ultimi sette giorni.

Kaspersky Security Center Cloud Console dispone di un set predefinito di selezioni eventi (preimpostate):

- Eventi con diversi livelli di importanza:
  - **Eventi critici**
  - **Errori funzionali**
  - **Avvisi**
  - **Messaggi informativi**
- **Richieste utente** (eventi delle applicazioni gestite)
- **Eventi recenti** (nell'ultima settimana)
- Eventi di controllo

In Kaspersky Security Center Cloud Console vengono visualizzati gli eventi di controllo relativi alle operazioni di servizio nell'area di lavoro. Questi eventi sono condizionati dalle azioni degli specialisti di Kaspersky. Questi eventi includono ad esempio: modifica delle porte di Administration Server; backup dei database di Administration Server; creazione, modifica ed eliminazione degli account utente.

È inoltre possibile creare e configurare ulteriori selezioni definite dall'utente. Nelle selezioni definite dall'utente è possibile filtrare gli eventi in base alle proprietà dei dispositivi da cui hanno avuto origine (nomi dei dispositivi, intervalli IP e gruppi di amministrazione), per tipi di eventi e livelli di criticità, per nome dell'applicazione e del componente e per intervallo di tempo. È anche possibile includere i risultati delle attività nell'ambito della ricerca. È inoltre disponibile un semplice campo di ricerca, in cui è possibile digitare una o più parole. Vengono visualizzati tutti gli eventi che contengono una delle parole digitate in qualsiasi punto dei relativi attributi (come nome dell'evento, descrizione o nome del componente).

Sia per le selezioni predefinite che per quelle definite dall'utente, è possibile limitare il numero di eventi visualizzati o il numero di record da cercare. Entrambe le opzioni influiscono sul tempo richiesto da Kaspersky Security Center Cloud Console per visualizzare gli eventi. Più grande è il database, più tempo può richiedere il processo.

È possibile procedere come segue:

- Modificare le proprietà delle selezioni eventi
- Generare selezioni eventi
- Visualizzare i dettagli delle selezioni eventi
- Eliminare le selezioni eventi
- Eliminare gli eventi dal database di Administration Server

Creazione di una selezione eventi

Per creare una selezione eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Selezioni eventi**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Nuova selezione eventi** visualizzata specificare le impostazioni della nuova selezione eventi. Eseguire tale operazione in una o più sezioni della finestra.
4. Fare clic su **Salva** per salvare le modifiche.

   Verrà visualizzata la finestra di conferma.
5. Per visualizzare i risultati della selezione eventi, mantenere selezionata la casella di controllo **Vai al risultato della selezione**.
6. Fare clic su **Salva** per confermare la creazione della selezione eventi.

Se è stata mantenuta selezionata la casella di controllo **Vai al risultato della selezione**, verranno visualizzati i risultati della selezione eventi. In caso contrario, la nuova selezione eventi verrà visualizzata nell'elenco delle selezioni eventi.

Modifica di una selezione eventi

Per modificare una selezione eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Selezioni eventi**.
2. Selezionare la casella di controllo accanto alla selezione eventi che si desidera modificare.
3. Fare clic sul pulsante **Proprietà**.

   Verrà visualizzata una finestra delle impostazioni della selezione eventi.
4. Modificare le proprietà della selezione eventi.

   > Per le selezioni di eventi predefinite, è possibile modificare solo le proprietà nelle seguenti schede: **Generale** (tranne il nome della selezione), **Data/ora** e **Diritti di accesso**.

   Per le selezioni definite dall'utente, è possibile modificare tutte le proprietà.
5. Fare clic su **Salva** per salvare le modifiche.

La selezione eventi modificata verrà visualizzata nell'elenco.

Visualizzazione di un elenco di una selezione eventi

Per visualizzare una selezione eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Selezioni eventi**.
2. Selezionare la casella di controllo accanto alla selezione eventi che si desidera avviare.
3. Eseguire una delle seguenti operazioni:
   - Se si desidera configurare l'ordinamento dei risultati della selezione eventi, effettuare le seguenti operazioni:
     a. Fare clic sul pulsante **Riconfigura ordinamento e avvia**.
     b. Nella finestra **Riconfigurare l'ordinamento per la selezione eventi** visualizzata specificare le impostazioni di ordinamento.
     c. Fare clic sul nome della selezione.
   - In caso contrario, se si desidera visualizzare l'elenco degli eventi in base all'ordinamento in Administration Server, fare clic sul nome della selezione.

Verranno visualizzati i risultati della selezione eventi.

Esportazione di una selezione di eventi

Kaspersky Security Center Cloud Console consente di salvare una selezione di eventi e le relative impostazioni in un file KLO. È possibile utilizzare questo file KLO per importare la selezione di eventi salvata sia per Kaspersky Security Center Windows che per Kaspersky Security Center Linux.

Si noti che è possibile esportare solo le selezioni di eventi definite dall'utente. Le selezioni di eventi dal set predefinito di Kaspersky Security Center Cloud Console (selezioni predefinite) non possono essere salvate in un file.

Per esportare una selezione di eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.
2. Selezionare la casella di controllo accanto alla selezione eventi che si desidera esportare.

   Non è possibile esportare più selezioni di eventi contemporaneamente. Se si selezionano più selezioni, il pulsante **Esporta** verrà disabilitato.
3. Fare clic sul pulsante **Esporta**.
4. Nella finestra **Salva con nome** aperta, specificare il nome e il percorso del file della selezione di eventi, quindi fare clic sul pulsante **Salva**.

   La finestra **Salva con nome** viene visualizzata solo se si utilizza Google Chrome, Microsoft Edge oppure Opera. Se si utilizza un altro browser, il file della selezione di eventi viene salvato automaticamente nella cartella **Download**.

Importazione di una selezione di eventi

Kaspersky Security Center Cloud Console consente di importare una selezione di eventi da un file KLO. Il file KLO contiene la selezione di eventi esportata e le sue impostazioni.

Per importare una selezione di eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.
2. Fare clic sul pulsante **Importa**, quindi scegliere una selezione di eventi che si desidera importare.
3. Nella finestra visualizzata, specificare il percorso del file KLO, quindi fare clic sul pulsante **Apri**. Si noti che è possibile selezionare solo una selezione di eventi.

   Viene avviata l'elaborazione della selezione di eventi.

Viene visualizzata la notifica con i risultati dell'importazione. Se la selezione di eventi viene importata correttamente, è possibile fare clic sul collegamento **Visualizza dettagli importazione** per visualizzare le proprietà della selezione di eventi.

Dopo un'importazione riuscita, la selezione di eventi viene visualizzata nell'elenco delle selezioni. Vengono importate anche le impostazioni della selezione di eventi.

Se la selezione di eventi appena importata ha un nome identico a quello di una selezione di eventi esistente, il nome della selezione importata viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Visualizzazione dei dettagli di un evento

Per visualizzare i dettagli di un evento:

1. Avviare una selezione eventi.
2. Fare clic sull'ora dell'evento desiderato.

   Verrà visualizzata la finestra **Proprietà evento**.
3. Nella finestra visualizzata è possibile eseguire le seguenti operazioni:
   - Visualizzare le informazioni sull'evento selezionato
   - Passare all'evento successivo e all'evento precedente nei risultati della selezione eventi
   - Passare al dispositivo in cui si è verificato l'evento
   - Passare al gruppo di amministrazione che include il dispositivo in cui si è verificato l'evento
   - Per un evento correlato a un'attività, passare alle proprietà dell'attività

Esportazione degli eventi in un file

Per esportare gli eventi in un file:

1. Avviare una selezione eventi.
2. Selezionare la casella di controllo accanto all'evento desiderato.
3. Fare clic sul pulsante **Esporta in un file**.

L'evento selezionato verrà esportato in un file.

Visualizzazione della cronologia di un oggetto da un evento

Da un evento di creazione o di modifica di un oggetto che supporta la gestione delle revisioni, è possibile passare alla cronologia delle revisioni dell'oggetto.

Per visualizzare la cronologia di un oggetto da un evento:

1. Avviare una selezione eventi.

2. Selezionare la casella di controllo accanto all'evento desiderato.

3. Fare clic sul pulsante **Cronologia revisioni**.

Verrà aperta la cronologia delle revisioni dell'oggetto.

Registrazione delle informazioni sugli eventi per le attività e i criteri

Questa sezione offre suggerimenti per ridurre al minimo il numero di eventi per attività e criteri archiviati nel database di Kaspersky Security Center Cloud Console. Per impostazione predefinita, ogni 1000 dispositivi hanno 100.000 eventi. Se questo limite viene superato, i nuovi eventi sovrascrivono i precedenti. Di conseguenza, gli eventi critici possono scomparire. Inoltre, potrebbe verificarsi l'evento di avviso di Administration Server denominato **Poiché è stato superato il limite relativo al numero di eventi nel database, gli eventi sono stati eliminati**. In questi casi, è consigliabile seguire le istruzioni contenute in questa sezione.

Di conseguenza, si aumenterà la velocità di esecuzione degli scenari associati all'analisi degli eventi. Questi suggerimenti consentono inoltre di ridurre il rischio che gli eventi critici vengano sovrascritti da un numero elevato di eventi.

Per impostazione predefinita, le proprietà di ogni attività e criterio consentono l'archiviazione di tutti gli eventi relativi all'esecuzione delle attività e all'applicazione dei criteri. Tuttavia, se un'attività viene eseguita di frequente (ad esempio più di una volta a settimana), il numero di eventi può rivelarsi troppo ampio e gli eventi possono riempire eccessivamente il database. In questo caso è consigliabile selezionare una delle due opzioni nelle impostazioni dell'attività:

- **Salva eventi correlati all'avanzamento dell'attività**. In questo caso Kaspersky Security Center Cloud Console archivia solo le informazioni sull'avvio, sull'avanzamento e sul completamento delle attività (completata, con un avviso o con un errore) da ciascun dispositivo in cui viene eseguita l'attività.

- **Salva solo i risultati dell'esecuzione dell'attività**. In questo caso Kaspersky Security Center Cloud Console archivia solo le informazioni sul completamento delle attività (completata, con un avviso o con un errore) da ciascun dispositivo in cui viene eseguita l'attività.

Se è stato definito un criterio per un ampio numero di dispositivi (ad esempio più di 10.000), il numero di eventi può anche rivelarsi troppo ampio e gli eventi possono riempire eccessivamente il database. In questo caso è consigliabile selezionare solo gli eventi più critici nelle impostazioni del criterio e abilitare la relativa registrazione. È consigliabile disabilitare la registrazione di tutti gli altri eventi.

È anche possibile ridurre il periodo di archiviazione per gli eventi associati a un'attività o a un criterio. Il periodo predefinito è di 7 giorni per gli eventi correlati alle attività e di 30 giorni per gli eventi correlati ai criteri. Quando si modifica il periodo di archiviazione di un evento è opportuno prendere in considerazione le procedure operative in atto nell'organizzazione e la quantità di tempo che l'amministratore di sistema può dedicare all'analisi di ciascun evento.

È consigliabile modificare le impostazioni di archiviazione degli eventi se gli eventi relativi alle modifiche negli stati intermedi delle attività di gruppo e gli eventi relativi all'applicazione dei criteri rappresentano un'ampia porzione di tutti gli eventi nel database di Kaspersky Security Center Cloud Console.

Eliminazione di eventi

Per eliminare uno o più eventi:

1. Avviare una selezione eventi.

2. Selezionare le caselle di controllo accanto agli eventi desiderati.

3. Fare clic sul pulsante **Elimina**.

Gli eventi selezionati verranno eliminati e non potranno essere ripristinati.

Eliminazione di selezioni eventi

È possibile eliminare solo le selezioni eventi definite dall'utente. Le selezioni eventi predefinite non possono essere eliminate.

Per eliminare una o più selezioni eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Selezioni eventi**.

2. Selezionare le caselle di controllo accanto alle selezioni eventi che si desidera eliminare.

3. Fare clic su **Elimina**.

4. Nella finestra visualizzata fare clic su **OK**.

La selezione eventi verrà eliminata.

Notifiche e stati del dispositivo

Questa sezione contiene informazioni su come visualizzare le notifiche, configurare il recapito delle notifiche, utilizzare gli stati dei dispositivi e abilitare la modifica degli stati dei dispositivi.

Informazioni sulle notifiche

Kaspersky Security Center Cloud Console offre la possibilità di monitorare la rete dell'organizzazione inviando notifiche su qualsiasi evento che si ritiene importante. Per ogni evento è possibile configurare le notifiche via e-mail.

Quando si ricevono notifiche tramite e-mail, è possibile decidere la risposta a un evento. Questa risposta deve essere la più appropriata per la rete dell'organizzazione.

Configurazione del passaggio degli stati del dispositivo

È possibile modificare le condizioni per assegnare lo stato *Critico* o *Avviso* a un dispositivo.

Per abilitare la modifica dello stato del dispositivo in Critico:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.
4. Nel riquadro sinistro selezionare **Critico**.
5. Nel riquadro destro, nella sezione **Imposta su Critico se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Critico*.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio padre.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.
7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.
8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.
9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Critico*.

Per abilitare la modifica dello stato del dispositivo in Avviso:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.
4. Nel riquadro sinistro selezionare **Avviso**.
5. Nel riquadro destro, nella sezione **Imposta su Avviso se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Avviso*.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio padre.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.
7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.
8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.
9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Avviso*.

Configurazione dell'invio delle notifiche

È possibile configurare notifiche e-mail per gli eventi che si verificano in Kaspersky Security Center Cloud Console.

Per configurare l'invio delle notifiche per gli eventi che si verificano in Kaspersky Security Center Cloud Console:

1. Nel menu principale, fare clic sull'icona delle impostazioni (⚙) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server, con la scheda **Generale** selezionata.

2. Fare clic sulla sezione **Notifica** e nel riquadro destro definire le impostazioni di notifica e-mail:

   Destinatari (indirizzi e-mail)

   Gli indirizzi e-mail a cui Kaspersky Security Center Cloud Console invierà le notifiche. È possibile specificare più indirizzi in questo campo, separandoli con punto e virgola.

   È possibile specificare al massimo 24 indirizzi e-mail.

3. Fare clic sul pulsante **Invia messaggio di test** per verificare se le notifiche sono state configurate correttamente: l'applicazione invia una notifica di prova all'indirizzo e-mail specificato.

4. Fare clic sul pulsante **OK** per chiudere la finestra delle proprietà di Administration Server.

Le impostazioni di invio delle notifiche salvate vengono applicate a tutti gli eventi che si verificano in Kaspersky Security Center Cloud Console.

È possibile sostituire le impostazioni di invio delle notifiche per determinati eventi nella sezione **Configurazione eventi** delle impostazioni di Administration Server, delle impostazioni di un criterio o delle impostazioni di un'applicazione.

Annunci Kaspersky

Questa sezione descrive come utilizzare, configurare e disabilitare gli annunci di Kaspersky.

Informazioni sugli annunci di Kaspersky

La sezione Annunci Kaspersky (**Monitoraggio e generazione dei rapporti → Annunci Kaspersky**) consente di rimanere informati fornendo informazioni relative a Kaspersky Security Center Cloud Console e alle applicazioni gestite installate nei dispositivi gestiti. Kaspersky Security Center Cloud Console aggiorna periodicamente le informazioni nella sezione rimuovendo gli annunci obsoleti e aggiungendo nuove informazioni.

Kaspersky Security Center Cloud Console mostra solo gli annunci di Kaspersky relativi all'Administration Server attualmente connesso e alle applicazioni Kaspersky installate nei dispositivi gestiti di questo Administration Server. Gli annunci vengono visualizzati singolarmente per qualsiasi tipo di Administration Server: primario, secondario o virtuale.

Se più amministratori utilizzano Kaspersky Security Center Cloud Console e impostano lingue dell'interfaccia diverse, Kaspersky Security Center Cloud Console visualizza gli annunci Kaspersky in tutte le lingue utilizzate dagli amministratori. Quando si cambia la lingua dell'interfaccia, gli annunci Kaspersky nella lingua selezionata vengono aggiunti automaticamente alla sezione quando si effettua nuovamente l'accesso dopo la disconnessione dalla console.

Gli annunci includono informazioni dei seguenti tipi:

- Annunci relativi alla sicurezza

  Gli annunci relativi alla sicurezza hanno lo scopo di mantenere aggiornate e completamente funzionanti le applicazioni Kaspersky installate nella rete. Gli annunci possono includere informazioni sugli aggiornamenti critici per le applicazioni Kaspersky, correzioni per le vulnerabilità rilevate e modalità di risoluzione di altri problemi nelle applicazioni Kaspersky. Gli annunci relativi alla sicurezza sono abilitati per impostazione predefinita. Se non si desidera ricevere gli annunci, è possibile disabilitare questa funzionalità.

  > Non è possibile disabilitare gli annunci relativi alla sicurezza nella modalità di prova di Kaspersky Security Center Cloud Console.

  Per mostrare le informazioni corrispondenti alla configurazione della protezione di rete, Kaspersky Security Center Cloud Console invia i dati ai server cloud Kaspersky e riceve solo gli annunci relativi alle applicazioni Kaspersky installate nella rete. Il set di dati che può essere inviato ai server è descritto nel Contratto di Kaspersky Security Center Cloud Console accettato durante la creazione di un'area di lavoro aziendale.

- Annunci di marketing

  Gli annunci di marketing includono informazioni su offerte speciali per le applicazioni Kaspersky, pubblicità e notizie provenienti da Kaspersky. Gli annunci di marketing sono disabilitati per impostazione predefinita. Questo tipo di annunci viene ricevuto solo se è stato abilitato Kaspersky Security Network (KSN). È possibile disabilitare gli annunci di marketing disabilitando KSN.

  Al fine di mostrare solo le informazioni attinenti che potrebbero essere utili per la protezione dei dispositivi di rete e nelle attività quotidiane, Kaspersky Security Center Cloud Console invia i dati ai server cloud Kaspersky e riceve gli annunci appropriati. Il set di dati che può essere inviato ai server è descritto nella sezione Dati elaborati dell' Informativa KSN.

Le nuove informazioni sono suddivise nelle seguenti categorie, in base al livello di importanza:

1. Informazioni critiche
2. Novità importanti
3. Avviso
4. Informazioni

Quando vengono visualizzate nuove informazioni nella sezione Annunci Kaspersky, Kaspersky Security Center Cloud Console visualizza un'etichetta di notifica che corrisponde al livello di importanza degli annunci. È possibile fare clic sull'etichetta per visualizzare l'annuncio nella sezione Annunci Kaspersky.

Disabilitazione degli annunci di Kaspersky

La sezione Annunci Kaspersky (**Monitoraggio e generazione dei rapporti → Annunci Kaspersky**) consente di rimanere informati fornendo informazioni relative alla versione in uso di Kaspersky Security Center Cloud Console e alle applicazioni gestite installate nei dispositivi gestiti. Se non si desidera ricevere gli annunci di Kaspersky, è possibile disabilitare questa funzionalità.

Gli annunci Kaspersky includono due tipi di informazioni: annunci relativi alla sicurezza e annunci di marketing. È possibile disabilitare separatamente gli annunci di ciascun tipo.

Non è possibile disabilitare gli annunci relativi alla sicurezza nella modalità di prova di Kaspersky Security Center Cloud Console.

Per disabilitare gli annunci relativi alla sicurezza:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome di Administration Server.
   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Generale** selezionare la sezione **Annunci Kaspersky**.
3. Spostare l'interruttore sulla posizione **Annunci relativi alla sicurezza Disabilitati**.
4. Fare clic sul pulsante **Salva**.
   Gli annunci di Kaspersky vengono disabilitati.

Gli annunci di marketing sono disabilitati per impostazione predefinita. Gli annunci di marketing vengono ricevuti solo se è stato abilitato Kaspersky Security Network (KSN). È possibile disabilitare questo tipo di annunci disabilitando KSN.

Per disabilitare gli annunci di marketing:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome di Administration Server.
   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Generale** selezionare la sezione **Impostazioni KSN**.
3. Disabilitare l'opzione **Accetto di utilizzare Kaspersky Security Network**.
4. Fare clic sul pulsante **Salva**.
   Gli annunci di marketing vengono disabilitati.

Ricezione dell'avviso di scadenza della licenza

Per aggiungere una chiave di licenza di Kaspersky Endpoint Security for Business Select nell'Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome di Administration Server.
   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Generale** selezionare la sezione **Chiavi di licenza**.
3. Fare clic su **Seleziona**.
4. Nella finestra visualizzata selezionare la licenza e fare clic su **OK**.

In alternativa, se non viene visualizzata alcuna licenza, è possibile fare clic su **Aggiungi nuova chiave di licenza** e utilizzare il proprio codice di attivazione.

La licenza viene aggiunta all'archivio dell'Administration Server. Di conseguenza l'Administration Server genera un evento critico *La licenza sta per scadere* un giorno prima della scadenza del periodo licenza e un evento critico *Modalità con funzionalità limitate* dopo la scadenza del periodo licenza. È possibile configurare l'invio delle notifiche.

Se si aggiunge una chiave di licenza di Kaspersky Endpoint Security for Business Select all'archivio dell'Administration Server, la licenza viene considerata utilizzata su un dispositivo.

Cloud Discovery

Kaspersky Security Center Cloud Console consente di monitorare l'utilizzo dei servizi cloud nei dispositivi gestiti che eseguono Windows e di bloccare l'accesso ai servizi cloud considerati indesiderati. Cloud Discovery monitora i tentativi da parte degli utenti di ottenere l'accesso a questi servizi tramite i browser e le applicazioni desktop. Inoltre, tiene traccia dei tentativi da parte degli utenti di ottenere l'accesso ai servizi cloud tramite connessioni non criptate (ad esempio utilizzando il protocollo HTTP). Questa funzionalità consente di rilevare e bloccare l'utilizzo dei servizi cloud tramite shadow IT.

La funzionalità Cloud Discovery è disponibile solo se è stata acquistata una delle licenze Kaspersky NEXT. Per ulteriori dettagli, consultare Licenze e numero minimo di dispositivi per ogni licenza.

È possibile abilitare la funzionalità Cloud Discovery e selezionare i profili di protezione per i quali si desidera abilitare la funzionalità. È anche possibile abilitare o disabilitare la funzionalità separatamente in ciascun criterio o profilo di protezione. È possibile bloccare l'accesso ai servizi cloud a cui si desidera che gli utenti non accedano.

Per poter bloccare l'accesso ai servizi cloud indesiderati, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Si utilizza Kaspersky Endpoint Security 11.2 for Windows o versioni successive. Le versioni precedenti dell'applicazione di protezione consentono solo di monitorare l'utilizzo dei servizi cloud.
- È stata acquistata una delle licenze Kaspersky NEXT che offrono la possibilità di bloccare l'accesso ai servizi cloud indesiderati.

Il widget Cloud Discovery e i rapporti Cloud Discovery consentono di visualizzare le informazioni sui tentativi riusciti e bloccati di ottenere l'accesso ai servizi cloud. Il widget mostra inoltre il livello di rischio di ciascun servizio cloud. Kaspersky Security Center Cloud Console ottiene le informazioni sull'utilizzo dei servizi cloud da tutti i dispositivi gestiti protetti solo dai criteri o dai profili di protezione con la funzionalità abilitata.

Abilitazione di Cloud Discovery utilizzando il widget

La funzionalità Cloud Discovery consente di ottenere informazioni sull'utilizzo dei servizi cloud da tutti i dispositivi gestiti protetti solo dai criteri di protezione con la funzionalità abilitata. È possibile abilitare o disabilitare Cloud Discovery solo per il criterio di Kaspersky Endpoint Security for Windows.

Esistono due modi per abilitare la funzionalità Cloud Discovery:

- Utilizzando il widget Cloud Discovery:
- Nelle proprietà del criterio di Kaspersky Endpoint Security for Windows.

  Per informazioni dettagliate su come abilitare la funzionalità Cloud Discovery nelle proprietà del criterio di Kaspersky Endpoint Security for Windows, fare riferimento alla sezione Cloud Discovery della Guida di Kaspersky Endpoint Security for Windows.

Si noti che è possibile disabilitare la funzionalità Cloud Discovery solo nei parametri del criterio di Kaspersky Endpoint Security for Windows.

Per poter abilitare Cloud Discovery, è necessario disporre del diritto di **Scrittura** nell'area funzionale **Funzionalità generali: Funzionalità di base**.

Per abilitare la funzionalità Cloud Discovery utilizzando il widget Cloud Discovery:

1. Passare a Kaspersky Security Center Cloud Console.
2. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
3. Nel widget **Cloud Discovery**, fare clic sul pulsante **Abilita**.
4. Nella finestra **Abilita Cloud Discovery** visualizzata, selezionare i criteri di sicurezza per cui si desidera abilitare la funzionalità, quindi fare clic sul pulsante **Abilita**.

   Le seguenti impostazioni dei criteri verranno abilitate automaticamente: **Inocula script nel traffico Web per interagire con le pagine Web**, **Monitoraggio sessione Web** e **Scansione connessioni criptate**.

La funzionalità Cloud Discovery è abilitata e il widget viene aggiunto al dashboard.

Aggiunta del widget Cloud Discovery al dashboard

È possibile aggiungere il widget **Cloud Discovery** al dashboard per monitorare l'utilizzo dei servizi cloud nei dispositivi gestiti.

Per poter aggiungere il widget Cloud Discovery al dashboard, è necessario disporre del diritto di **Scrittura** nell'area **Funzionalità generali: Funzionalità di base**.

Per aggiungere il widget Cloud Discovery al dashboard:

1. Passare a Kaspersky Security Center Cloud Console.
2. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
3. Fare clic sul pulsante **Aggiungi o ripristina widget Web**.
4. Nell'elenco dei widget disponibili, fare clic sull'icona della freccia di espansione (>) accanto alla categoria **Altro**.
5. Selezionare il widget **Cloud Discovery**, quindi fare clic sul pulsante **Aggiungi**.

   Se la funzionalità Cloud Discovery è disabilitata, seguire le istruzioni nella sezione Abilitazione di Cloud Discovery utilizzando il widget.

Il widget selezionato verrà aggiunto alla fine del dashboard.

Visualizzazione delle informazioni sull'utilizzo dei servizi cloud

È possibile visualizzare il widget **Cloud Discovery** che mostra informazioni sui tentativi di accesso ai servizi cloud. Il widget mostra inoltre il livello di rischio di ciascun servizio cloud. Kaspersky Security Center Cloud Console ottiene le informazioni sull'utilizzo dei servizi cloud da tutti i dispositivi gestiti protetti solo dai criteri di protezione con la funzionalità abilitata.

Prima di visualizzare, assicurarsi che:

- il widget Cloud Discovery sia aggiunto al dashboard.
- la funzionalità Cloud Discovery sia abilitata.
- di disponga del diritto **Lettura** nell'area funzionale **Caratteristiche generali: Funzionalità di base**.

Per visualizzare il widget Cloud Discovery:

1. Passare a Kaspersky Security Center Cloud Console.
2. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.

   Il widget **Cloud Discovery** viene visualizzato nel dashboard.
3. Nella parte sinistra del widget Informazioni su **Cloud Discovery** selezionare una categoria di servizi cloud.

   La tabella nella parte destra del widget mostra fino a cinque servizi, della categoria selezionata, a cui gli utenti tentano più spesso di accedere. Vengono calcolati sia i tentativi andati a buon fine che quelli bloccati.
4. Nella parte destra del widget selezionare un servizio specifico.

   La tabella seguente mostra fino a dieci dispositivi che tentano più spesso di ottenere l'accesso al servizio.

Il widget visualizza le informazioni richieste.

Dal widget visualizzato è possibile effettuare le seguenti operazioni:

- Passare alla sezione **Monitoraggio e generazione dei rapporti** → **Rapporti** per visualizzare i rapporti di Cloud Discovery.
- Bloccare o consentire l'accesso al servizio cloud selezionato.

La funzionalità Cloud Discovery è disponibile solo se è stata acquistata una delle licenze Kaspersky NEXT. Per ulteriori dettagli, consultare Licenze e numero minimo di dispositivi per ogni licenza.

Livello di rischio di un servizio cloud

Per ogni servizio cloud, Cloud Discovery fornisce un livello di rischio. Il livello di rischio consente di determinare i servizi che non soddisfano i requisiti di protezione dell'organizzazione. Ad esempio, è possibile tenere conto del livello di rischio quando si decide se bloccare l'accesso a un determinato servizio.

Il livello di rischio è un indice stimato e non fornisce indicazioni sulla qualità di un servizio cloud o sul produttore del servizio. Il livello di rischio è semplicemente una raccomandazione degli esperti di Kaspersky.

I livelli di rischio dei servizi cloud vengono visualizzati nel widget Cloud Discovery e nell'elenco di tutti i servizi cloud monitorati.

Blocco dell'accesso ai servizi cloud indesiderati

È possibile bloccare l'accesso ai servizi cloud a cui si desidera che gli utenti non accedano. È inoltre possibile consentire l'accesso ai servizi cloud precedentemente bloccati.

Tra le altre considerazioni, è consigliabile tenere conto del livello di rischio quando si decide se bloccare l'accesso a un determinato servizio.

È possibile bloccare o consentire l'accesso ai servizi cloud per un criterio o un profilo di sicurezza.

Esistono due modi per bloccare l'accesso ai servizi cloud indesiderati:

- Utilizzando il widget Cloud Discovery:

  In questo caso, è possibile bloccare uno per uno l'accesso ai servizi.

- Nelle proprietà del criterio di Kaspersky Endpoint Security for Windows.

  In questo caso, è possibile bloccare l'accesso ai servizi uno per uno o bloccare l'intera categoria contemporaneamente.

  Per informazioni dettagliate su come abilitare la funzionalità Cloud Discovery nelle proprietà del criterio di Kaspersky Endpoint Security for Windows, fare riferimento alla sezione Cloud Discovery della Guida di Kaspersky Endpoint Security for Windows.

Per bloccare o consentire l'accesso a un servizio cloud utilizzando il widget:

1. Aprire il widget Cloud Discovery e selezionare il servizio cloud richiesto.
2. Nel riquadro **Primi 10 dispositivi che utilizzano il servizio**, individuare il criterio o il profilo di sicurezza per cui si desidera bloccare o consentire il servizio.
3. Nella colonna **Stato dell'accesso nel criterio o nei profili** della riga desiderata eseguire una delle seguenti operazioni:
   - Per bloccare il servizio, selezionare **Bloccato** nell'elenco a discesa.
   - Per consentire il servizio, selezionare **Consentito** nell'elenco a discesa.
4. Fare clic sul pulsante **Salva**.

L'accesso al servizio selezionato è bloccato o consentito per il criterio o il profilo di protezione.

Diagnostica remota dei dispositivi client

È possibile utilizzare la diagnostica remota per l'esecuzione remota delle seguenti operazioni nei dispositivi client basati su Windows e basati su Linux:

- Abilitazione e disabilitazione del tracciamento, modifica del livello di traccia e download del file di traccia
- Download di informazioni sul sistema e impostazioni dell'applicazione
- Download dei registri eventi
- Generazione di un file di dump per un'applicazione
- Avvio della diagnostica e download dei rapporti
- Avvio, arresto e riavvio delle applicazioni

È possibile utilizzare i registri eventi e i rapporti di diagnostica scaricati da un dispositivo client per eseguire autonomamente la risoluzione dei problemi. Inoltre, se si contatta il Servizio di assistenza tecnica Kaspersky, uno specialista del Servizio di assistenza tecnica potrebbe richiedere di scaricare file di traccia, file di dump, registri eventi e rapporti di diagnostica da un dispositivo client per ulteriori analisi da parte di Kaspersky.

Apertura della finestra di diagnostica remota

Per eseguire la diagnostica remota in dispositivi client basati su Windows e basati su Linux, è prima necessario aprire la finestra di diagnostica remota.

Per aprire la finestra di diagnostica remota:

1. Per selezionare il dispositivo per cui si desidera aprire la finestra di diagnostica remota, eseguire una delle seguenti operazioni:
   - Se il dispositivo appartiene a un gruppo di amministrazione, nel menu principale passare a **Risorse (dispositivi)** → **Gruppi** → **<group name>** → **Dispositivi gestiti**.
   - Se il dispositivo appartiene al gruppo Dispositivi non assegnati, nel menu principale passare a **Individuazione e distribuzione** → **Dispositivi non assegnati**.
2. Fare clic sul nome del dispositivo desiderato.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Avanzate**.
4. Nella finestra visualizzata fare clic su **Diagnostica remota**.

   Viene aperta la finestra **Diagnostica remota** di un dispositivo client. Se la connessione tra Administration Server e il dispositivo client non viene stabilita, viene visualizzato il messaggio di errore.

In alternativa, se è necessario ottenere tutte le informazioni diagnostiche su un dispositivo client basato su Linux, è possibile eseguire lo script collect.sh in questo dispositivo.

Abilitazione e disabilitazione del tracciamento per le applicazioni

È possibile abilitare e disabilitare il tracciamento per le applicazioni, incluso il tracciamento Xperf.

Abilitazione e disabilitazione del tracciamento

Per abilitare o disabilitare il tracciamento in un dispositivo remoto:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni selezionare l'applicazione per cui si desidera disabilitare il tracciamento.

   Si apre l'elenco delle opzioni di diagnostica remota.
4. Se si desidera abilitare il tracciamento:

   a. Nella sezione **Traccia**, fare clic su **Abilita traccia**.

   b. Nella finestra **Modifica livello di traccia** visualizzata è consigliabile mantenere i valori predefiniti delle impostazioni. Se necessario, uno specialista del Servizio di assistenza tecnica fornirà il supporto richiesto per il processo di configurazione. Sono disponibili le seguenti impostazioni:

   - **Livello di traccia**

     Il livello di traccia definisce la quantità di dettagli contenuti nel file di traccia.

   - **Traccia basata sulla rotazione**

     L'applicazione sovrascrive le informazioni di tracciamento per evitare un aumento eccessivo delle dimensioni del file di traccia. Specificare il numero massimo di file da utilizzare per archiviare le informazioni di tracciamento e la dimensione massima di ciascun file. Se viene eseguita la scrittura del numero massimo di file di traccia della dimensione massima, il file di traccia meno recente viene eliminato in modo da consentire la creazione di un nuovo file di traccia.

     Questa impostazione è disponibile solo per Kaspersky Endpoint Security.

   c. Fare clic su **Salva**.

   Il tracciamento è abilitato per l'applicazione selezionata. In alcuni casi, è necessario riavviare un'applicazione di protezione e la relativa attività per abilitare il tracciamento.

   Nei dispositivi client basati su Linux, il tracciamento per il componente Updater of Kaspersky Security Agent è regolata dalle impostazioni di Network Agent. Pertanto, le opzioni **Abilita traccia** e **Modifica livello di traccia** sono disabilitate per questo componente nei dispositivi client in cui viene eseguito Linux.
5. Se si desidera disabilitare il tracciamento per l'applicazione selezionata, fare clic su **Disabilita traccia**.

   Il tracciamento è disabilitato per l'applicazione selezionata.

Abilitazione del tracciamento Xperf

Per Kaspersky Endpoint Security, uno specialista del Servizio di assistenza tecnica può richiedere di abilitare il tracciamento Xperf per ottenere informazioni sulle prestazioni del sistema.

Per abilitare e configurare il tracciamento Xperf o disabilitarlo:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni selezionare Kaspersky Endpoint Security for Windows.

   Viene visualizzato l'elenco delle opzioni di diagnostica remota per Kaspersky Endpoint Security for Windows.
4. Nella sezione **Traccia Xperf**, fare clic su **Abilita traccia Xperf**.

   Se il tracciamento Xperf è già abilitato, viene invece visualizzato il pulsante **Disabilita traccia Xperf**. Fare clic su questo pulsante se si desidera disabilitare il tracciamento Xperf per Kaspersky Endpoint Security for Windows.
5. Nella finestra **Modifica livello di traccia Xperf** visualizzata, a seconda di quanto richiesto dallo specialista del Servizio di assistenza tecnica, eseguire una delle seguenti azioni:

   a. Selezionare uno dei seguenti livelli di traccia:

   - **Livello superficiale**

     Un file di traccia di questo tipo contiene la quantità minima di informazioni sul sistema.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Livello approfondito**

     Un file di traccia di questo tipo contiene informazioni più dettagliate rispetto ai file di traccia di tipo *Superficiale* e può essere richiesto dagli specialisti del Servizio di assistenza tecnica quando un file di traccia di tipo *Superficiale* non è sufficiente per la valutazione delle prestazioni. Un file di traccia *Approfondito* contiene informazioni tecniche sul sistema, incluse informazioni su hardware, sistema operativo, elenco di processi e applicazioni avviati e arrestati, eventi utilizzati per la valutazione delle prestazioni ed eventi raccolti da Strumento Valutazione sistema Windows.

   b. Selezionare uno dei seguenti tipi di tracciamento Xperf:

   - **Tipologia di base**

     Le informazioni di tracciamento vengono ricevute durante l'esecuzione dell'applicazione Kaspersky Endpoint Security.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Tipologia al riavvio**

     Le informazioni di tracciamento vengono ricevute all'avvio del sistema operativo nel dispositivo gestito. Questo tipo di tracciamento è utile quando il problema che influisce sulle prestazioni del sistema si verifica dopo l'accensione del dispositivo e prima dell'avvio di Kaspersky Endpoint Security.

Potrebbe anche essere necessario abilitare l'opzione **Dimensioni del file con rotazione (MB)** per impedire un aumento eccessivo delle dimensioni del file di traccia. Specificare quindi la dimensione massima del file di traccia. Quando il file raggiunge la dimensione massima, le informazioni di tracciamento meno recenti vengono sovrascritte da quelle nuove.

c. Definire le dimensioni del file di rotazione.

d. Fare clic su **Salva**.

Il tracciamento Xperf è abilitato e configurato.

6. Se si desidera disabilitare il tracciamento Xperf per Kaspersky Endpoint Security for Windows, fare clic su **Disabilita traccia Xperf** nella sezione **Traccia Xperf**.

   Il tracciamento Xperf è disabilitato.

Download dei file di traccia di un'applicazione

È possibile scaricare i file di traccia da un dispositivo client solo se viene soddisfatta una delle seguenti condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo, è in uso un server push oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Per scaricare un file di traccia di un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.

3. Nell'elenco delle applicazioni, selezionare l'applicazione per la quale si desidera scaricare un file di traccia.

4. Nella sezione **Traccia** fare clic sul pulsante **File di traccia**.

   Viene aperta la finestra **Log di traccia del dispositivo**, dove viene visualizzato un elenco dei file di traccia.

5. Nell'elenco dei file di traccia, selezionare il file che si desidera scaricare.

6. Eseguire una delle seguenti operazioni:

   - Scaricare il file selezionato facendo clic su **Scarica**. È possibile selezionare uno o più file da scaricare.

   - Scaricare una parte del file selezionato:

     a. Fare clic su **Scarica una parte**.

     Non è possibile scaricare parti di più file contemporaneamente. Se si seleziona più di un file di traccia, il pulsante **Scarica una parte** sarà disabilitato.

     b. Nella finestra visualizzata specificare il nome e la parte del file da scaricare, in base alle esigenze.

     Per i dispositivi basati su Linux, la modifica del nome di parte del file non è disponibile.

c. Fare clic su **Scarica.**

Il file selezionato, o la relativa parte, viene scaricato nella posizione specificata.

Eliminazione dei file di traccia

È possibile eliminare i file di traccia non più necessari.

Per eliminare un file di traccia:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra di diagnostica remota visualizzata, selezionare la scheda **Log eventi**.
3. Nella sezione **File di traccia**, fare clic su **Log di Windows Update** o **Log di installazione remota**, in base ai file di traccia che si desidera eliminare.

   Viene aperta la finestra **Log di traccia del dispositivo**, dove viene visualizzato un elenco dei file di traccia.
4. Nell'elenco dei file di traccia, selezionare uno o più file da eliminare.
5. Fare clic sul pulsante **Rimuovi**.

I file di traccia selezionati vengono eliminati.

Download delle impostazioni delle applicazioni

È possibile scaricare le impostazioni dell'applicazione da un dispositivo client solo se viene soddisfatta una delle seguenti condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo, è in uso un server push oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Per scaricare le impostazioni dell'applicazione da un dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.
3. Nella sezione **Impostazioni applicazione**. fare clic sul pulsante **Scarica** per scaricare le informazioni sulle impostazioni delle applicazioni installate nel dispositivo client.

L'archivio ZIP con le informazioni viene scaricato nella posizione specificata.

Download delle informazioni di sistema da un dispositivo client

È possibile scaricare le informazioni di sistema nel dispositivo da un dispositivo client solo se viene soddisfatta una delle seguenti condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo, è in uso un server push oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Per scaricare le informazioni di sistema da un dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Informazioni di sistema**.
3. Fare clic sul pulsante **Scarica** per scaricare le informazioni di sistema sul dispositivo client.

Il file con le informazioni viene scaricato nella posizione specificata.

Download dei registri eventi

È possibile scaricare i registri eventi nel dispositivo da un dispositivo client solo se viene soddisfatta una delle seguenti condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo, è in uso un server push oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Per scaricare un registro eventi da un dispositivo remoto:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, nella scheda **Log eventi**, fare clic su **Tutti i log del dispositivo**.
3. Nella finestra **Tutti i log del dispositivo**, selezionare uno o più log pertinenti.
4. Eseguire una delle seguenti operazioni:
   - Scaricare il log selezionato facendo clic su **Scarica l'intero file**.
   - Scaricare una parte del log selezionato:
     a. Fare clic su **Scarica una parte**.
     Non è possibile scaricare parti di più registri contemporaneamente. Se si seleziona più di un registro eventi, il pulsante **Scarica una parte** sarà disabilitato.
     b. Nella finestra visualizzata specificare il nome e la parte del registro da scaricare, in base alle esigenze.
     c. Fare clic su **Scarica**.

Il registro eventi selezionato, o la relativa parte, viene scaricato nella posizione specificata.

Avvio, arresto, riavvio dell'applicazione

È possibile avviare, arrestare e riavviare le applicazioni in un dispositivo client.

Per avviare, arrestare o riavviare un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni selezionare l'applicazione che si desidera avviare, arrestare o riavviare.
4. Selezionare un'azione facendo clic su uno dei seguenti pulsanti:

   - **Arresta applicazione**

     Questo pulsante è disponibile solo se l'applicazione è attualmente in esecuzione.
   - **Riavvia applicazione**

     Questo pulsante è disponibile solo se l'applicazione è attualmente in esecuzione.
   - **Avvia applicazione**

     Questo pulsante è disponibile solo se l'applicazione non è attualmente in esecuzione.

   A seconda dell'azione selezionata, l'applicazione richiesta viene avviata, arrestata o riavviata nel dispositivo client.

Se si riavvia Network Agent, viene visualizzato un messaggio che indica che la connessione corrente del dispositivo ad Administration Server andrà persa.

Esecuzione della diagnostica remota di un'applicazione e download dei risultati

Per avviare la diagnostica per un'applicazione in un dispositivo remoto e scaricarne i risultati:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni selezionare l'applicazione per la quale si desidera eseguire la diagnostica remota.

   Si apre l'elenco delle opzioni di diagnostica remota.
4. Nella sezione **Rapporto di diagnostica**, fare clic sul pulsante **Esegui diagnostica**.

   In questo modo si avvia la procedura di diagnostica remota e si genera un rapporto di diagnostica. Al termine della procedura di diagnostica, il pulsante **Scarica il rapporto di diagnostica** diventa disponibile.
5. Fare clic sul pulsante **Scarica il rapporto di diagnostica** per scaricare il rapporto.

Il rapporto viene scaricato nella posizione specificata.

Esecuzione di un'applicazione in un dispositivo client

Potrebbe essere necessario eseguire un'applicazione nel dispositivo client, se richiesto da uno specialista dell'assistenza Kaspersky. Non è necessario installare l'applicazione nel dispositivo. Non è necessario installare l'applicazione nel dispositivo.

Per eseguire un'applicazione nel dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Esecuzione di un'applicazione remota**.
3. Nella sezione **File dell'applicazione**, fare clic sul pulsante **Sfoglia** per selezionare un archivio ZIP contenente l'applicazione che si desidera eseguire nel dispositivo client.

   L'archivio ZIP deve includere la cartella dell'utilità. Questa cartella contiene il file eseguibile da eseguire in un dispositivo remoto.

   È possibile specificare il nome del file eseguibile e gli argomenti della riga di comando, se necessario. A tale scopo, compilare i campi **Executable file in an archive to be run on a remote device** e **Argomenti della riga di comando**.
4. Facendo clic sul pulsante **Carica ed esegui** per eseguire l'applicazione specificata in un dispositivo client.
5. Seguire le istruzioni dell'esperto dell'Assistenza Kaspersky.

Generazione di un file di dump per un'applicazione

Un file di dump dell'applicazione consente di visualizzare i parametri dell'applicazione in esecuzione in un dispositivo client in un determinato momento. Questo file contiene anche informazioni sui moduli che sono stati caricati per un'applicazione.

La generazione di file dump è disponibile solo per i processi a 32 bit in esecuzione nei dispositivi client basati su Windows. Per i dispositivi client in cui viene eseguito Linux e per i processi a 64 bit, questa funzionalità non è supportata.

Per creare un file di dump per un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Esecuzione di un'applicazione remota**.
3. Nella sezione **Generazione del file di dump della memoria del processo in corso**, specificare il file eseguibile dell'applicazione per la quale si desidera generare un file dump.
4. Fare clic sul pulsante **Scarica** per salvare il file di dump per l'applicazione specificata.

   Se l'applicazione specificata non è in esecuzione nel dispositivo client, verrà visualizzato il messaggio di errore.

Esecuzione della diagnostica remota in un dispositivo client basato su Linux

Kaspersky Security Center Cloud Console consente di scaricare le informazioni diagnostiche di base da un dispositivo client. In alternativa, è possibile ottenere le informazioni diagnostiche su un dispositivo basato su Linux utilizzando lo script collect.sh di Kaspersky. Questo script viene eseguito nel dispositivo client basato su Linux che deve essere diagnosticato, quindi genera un file con le informazioni diagnostiche, le informazioni di sistema su questo dispositivo, i file di traccia delle applicazioni, i registri del dispositivo e un file di dump per le applicazioni terminate di emergenza.

È consigliabile utilizzare lo script collect.sh per ottenere tutte le informazioni diagnostiche sul dispositivo client basato su Linux contemporaneamente. Se si scaricano le informazioni diagnostiche da remoto tramite Kaspersky Security Center Cloud Console, sarà necessario esaminare tutte le sezioni dell'interfaccia di diagnostica remota. Inoltre, è probabile che le informazioni diagnostiche di un dispositivo basato su Linux non vengano ottenute completamente.

Se è necessario inviare il file generato con le informazioni diagnostiche all'Assistenza tecnica di Kaspersky, eliminare tutte le informazioni riservate prima di inviare il file.

Per scaricare le informazioni diagnostiche da un dispositivo client basato su Linux utilizzando lo script collect.sh:

1. Scaricare lo script collect.sh contenuto nell'archivio collect.tar.gz.
2. Copiare l'archivio scaricato nel dispositivo client basato su Linux da diagnosticare.
3. Eseguire il seguente comando per decomprimere l'archivio collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Eseguire il seguente comando per specificare i diritti di esecuzione dello script:

   ```
   # chmod +x collect.sh
   ```

5. Eseguire lo script collect.sh utilizzando un account con diritti di amministratore:

   ```
   # ./collect.sh
   ```

Un file con le informazioni diagnostiche viene generato e salvato nella cartella /tmp/$HOST_NAME-collect.tar.gz.

Esportazione di eventi nei sistemi SIEM

Questa sezione descrive come configurare l'esportazione degli eventi nei sistemi SIEM.

Scenario: configurazione dell'esportazione di eventi nei sistemi SIEM

Questa sezione fornisce uno scenario per la configurazione dell'esportazione degli eventi da Administration Server a sistemi SIEM esterni. L'esportazione delle informazioni sugli eventi nei sistemi SIEM esterni consente agli amministratori dei sistemi SIEM di rispondere tempestivamente agli eventi del sistema di protezione che si verificano in un dispositivo gestito o nei gruppi di dispositivi gestiti.

Prerequisiti

Prima di avviare la configurazione dell'esportazione degli eventi in Kaspersky Security Center Cloud Console:

- Ulteriori informazioni sui metodi di esportazione degli eventi.
- Assicurarsi di conoscere i valori delle impostazioni di sistema.

È possibile eseguire i passaggi di questo scenario in qualsiasi ordine.

Passaggi

Il processo di esportazione degli eventi nel sistema SIEM prevede i seguenti passaggi:

- **Configurazione del sistema SIEM per la ricezione di eventi da Kaspersky Security Center Cloud Console**

  È necessario configurare la ricezione degli eventi da Kaspersky Security Center Cloud Console nel sistema SIEM.

- **Contrassegno degli eventi per l'esportazione**

  È necessario contrassegnare gli eventi da esportare nel sistema SIEM. Prima di tutto, contrassegnare gli eventi generici che si verificano in tutte le applicazioni Kaspersky gestite. È inoltre possibile contrassegnare gli eventi per applicazioni Kaspersky gestite specifiche.

- **Configurazione di Kaspersky Security Center Cloud Console per l'esportazione degli eventi nel sistema SIEM**

  È necessario configurare Kaspersky Security Center Cloud Console per avviare l'esportazione degli eventi in un sistema SIEM.

Risultati

Dopo aver configurato l'esportazione degli eventi in un sistema SIEM, è possibile visualizzare i risultati dell'esportazione se sono stati selezionati gli eventi da esportare.

Prima di iniziare

Durante la configurazione dell'esportazione automatica degli eventi in Kaspersky Security Center Cloud Console, è necessario specificare alcune impostazioni del sistema SIEM. È consigliabile verificare preventivamente queste impostazioni per la preparazione della configurazione di Kaspersky Security Center Cloud Console.

Per configurare l'invio automatico degli eventi in un sistema SIEM, è necessario conoscere le seguenti impostazioni:

- **Indirizzo server del sistema SIEM**

  L'indirizzo IP del server in cui è installato il sistema SIEM utilizzato attualmente. Verificare questo valore nelle impostazioni del sistema SIEM.

- **Porta server del sistema SIEM**

  Numero della porta utilizzato per stabilire la connessione tra Kaspersky Security Center Cloud Console e il server del sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center Cloud Console e nelle impostazioni del destinatario del sistema SIEM.

- **Protocollo**

  Protocollo utilizzato per il trasferimento dei messaggi da Kaspersky Security Center Cloud Console al sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center Cloud Console e nelle impostazioni del destinatario del sistema SIEM.

Informazioni sull'esportazione degli eventi

Kaspersky Security Center Cloud Console consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Le informazioni sugli eventi vengono salvate nel database di Administration Server.

È possibile utilizzare l'esportazione degli eventi in sistemi centralizzati che gestiscono i problemi di protezione a livello tecnico e organizzativo, garantiscono servizi di monitoraggio della sicurezza e consolidano informazioni da diverse soluzioni. Si tratta di sistemi SIEM, che offrono analisi in tempo reale degli avvisi e degli eventi di protezione generati da applicazioni e hardware di rete o SOC (Security Operation Center).

Questi sistemi ricevono i dati da numerose origini, tra cui reti, sicurezza, server, database e applicazioni. I sistemi SIEM forniscono anche funzionalità per consolidare i dati monitorati ed evitare la perdita di eventi critici. Inoltre, questi sistemi eseguono analisi automatizzate di avvisi ed eventi correlati per inviare immediatamente agli amministratori una notifica dei problemi di protezione. Gli avvisi possono essere implementati tramite un dashboard o inviati tramite canali di terzi, ad esempio via e-mail.

Il processo di esportazione degli eventi da Kaspersky Security Center Cloud Console ai sistemi SIEM esterni coinvolge due parti: un mittente degli eventi (Kaspersky Security Center Cloud Console) e il destinatario di un evento (il sistema SIEM). Per eseguire l'esportazione degli eventi, è necessario configurare questa funzionalità nel sistema SIEM e in Kaspersky Security Center Cloud Console. Non è importante quale lato viene configurato per primo. È possibile configurare la trasmissione degli eventi in Kaspersky Security Center Cloud Console, quindi configurare la ricezione degli eventi dal sistema SIEM o viceversa.

Formato Syslog di esportazione degli eventi

È possibile inviare eventi nel formato Syslog a qualsiasi sistema SIEM. Utilizzando il formato Syslog è possibile inviare gli eventi che si verificano in Administration Server e nelle applicazioni Kaspersky installate nei dispositivi gestiti. Durante l'esportazione degli eventi nel formato Syslog, è possibile selezionare con precisione i tipi di eventi da inviare al sistema SIEM.

Ricezione degli eventi da parte del sistema SIEM

Il sistema SIEM deve ricevere e analizzare correttamente gli eventi ricevuti da Kaspersky Security Center Cloud Console. A tale scopo, è necessario configurare correttamente il sistema SIEM. La configurazione dipende dallo specifico sistema SIEM in uso. Sono comunque previsti diversi passaggi generali per la configurazione di tutti i sistemi SIEM, ad esempio la configurazione del ricevitore e del parser.

Configurazione dell'esportazione di eventi in un sistema SIEM

Il processo di esportazione degli eventi da Kaspersky Security Center Cloud Console ai sistemi SIEM esterni coinvolge due parti: un mittente degli eventi (Kaspersky Security Center Cloud Console) e il destinatario di un evento (il sistema SIEM). È necessario configurare l'esportazione degli eventi nel sistema SIEM e in Kaspersky Security Center Cloud Console.

Le impostazioni specificate nel sistema SIEM dipendono dal particolare sistema in uso. In genere, per tutti i sistemi SIEM è necessario impostare un ricevitore ed eventualmente un parser dei messaggi per l'analisi degli eventi ricevuti.

Configurazione del ricevitore

Per la ricezione degli eventi inviati da Kaspersky Security Center Cloud Console, è necessario impostare il ricevitore nel sistema SIEM. In generale, le seguenti impostazioni devono essere specificate nel sistema SIEM:

- **Porta**

  Specificare il numero di porta per la connessione a Kaspersky Security Center Cloud Console. Deve trattarsi della stessa porta specificata in Kaspersky Security Center Cloud Console durante la configurazione con un sistema SIEM.

- **Protocollo dei messaggi o tipo di origine**

  Specificare il formato Syslog.

A seconda del sistema SIEM in uso, potrebbe essere necessario specificare alcune impostazioni aggiuntive del ricevitore.

Parser dei messaggi

Gli eventi esportati vengono inviati ai sistemi SIEM come messaggi. Questi messaggi devono essere analizzati correttamente per consentire l'utilizzo delle informazioni sugli eventi nel sistema SIEM. I parser dei messaggi fanno parte del sistema SIEM: vengono utilizzati per suddividere il contenuto del messaggio nei campi appropriati, ad esempio l'ID degli eventi, la gravità, la descrizione, i parametri e così via. Questo consente al sistema SIEM di elaborare gli eventi ricevuti da Kaspersky Security Center Cloud Console in modo che possano essere memorizzati nel database del sistema SIEM.

Contrassegno degli eventi per l'esportazione nei sistemi SIEM in formato Syslog

Questa sezione descrive come contrassegnare gli eventi per un'ulteriore esportazione nei sistemi SIEM in formato Syslog.

Informazioni sul contrassegno degli eventi per l'esportazione nel sistema SIEM in formato Syslog

Dopo aver abilitato l'esportazione automatica degli eventi, è necessario contrassegnare gli eventi da esportare nel sistema SIEM esterno.

È possibile configurare l'esportazione degli eventi in formato Syslog in un sistema esterno in base alle seguenti condizioni:

- Contrassegno di eventi generali. Se si contrassegnano gli eventi da esportare in un criterio, nelle impostazioni di un evento o nelle impostazioni di Administration Server, il sistema SIEM riceverà gli eventi contrassegnati che si sono verificati in tutte le applicazioni gestite dal criterio specifico. Se sono stati selezionati eventi esportati nel criterio, non sarà possibile ridefinirli per una singola applicazione gestita da questo criterio.
- Contrassegno degli eventi per un'applicazione gestita. Se si contrassegnano gli eventi da esportare per un'applicazione gestita installata in un dispositivo gestito, il sistema SIEM riceverà solo gli eventi che si sono verificati nell'applicazione.

Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog

Se si desidera esportare gli eventi che si sono verificati in un'applicazione gestita specifica installata nei dispositivi gestiti, contrassegnare gli eventi per l'esportazione nel criterio dell'applicazione. In questo caso, gli eventi contrassegnati vengono esportati da tutti i dispositivi inclusi nell'ambito del criterio.

Per contrassegnare gli eventi per l'esportazione per una singola applicazione gestita:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio dell'applicazione per cui si desidera contrassegnare gli eventi.

   Verrà visualizzata la finestra delle impostazioni del criterio.
3. Accedere alla sezione **Configurazione eventi**.
4. Selezionare le caselle di controllo accanto agli eventi che si desidera esportare in un sistema SIEM.
5. Fare clic sul pulsante **Contrassegna per l'esportazione nel sistema SIEM utilizzando Syslog**.

È inoltre possibile contrassegnare un evento per l'esportazione nel sistema SIEM nella sezione **Registrazione eventi** visualizzata facendo clic sul collegamento dell'evento.

6. Un segno di spunta (✓) viene visualizzato nella colonna **Syslog** dell'evento o degli eventi contrassegnati per l'esportazione nel sistema SIEM.

7. Fare clic sul pulsante **Salva**.

Gli eventi contrassegnati dell'applicazione gestita sono pronti per l'esportazione in un sistema SIEM.

È possibile contrassegnare quali eventi esportare in un sistema SIEM per un dispositivo gestito specifico. Se sono stati contrassegnati eventi esportati in precedenza in un criterio dell'applicazione, non sarà possibile ridefinire gli eventi contrassegnati per un singolo dispositivo gestito.

Per contrassegnare gli eventi per l'esportazione per un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Fare clic sul collegamento con il nome del dispositivo desiderato nell'elenco dei dispositivi gestiti.

   Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.

3. Accedere alla sezione **Applicazioni**.

4. Fare clic sul collegamento con il nome dell'applicazione desiderata nell'elenco delle applicazioni.

5. Accedere alla sezione **Configurazione eventi**.

6. Selezionare le caselle di controllo accanto agli eventi che si desidera esportare in SIEM.

7. Fare clic sul pulsante **Contrassegna per l'esportazione nel sistema SIEM utilizzando Syslog**.

   È inoltre possibile contrassegnare un evento per l'esportazione nel sistema SIEM nella sezione **Registrazione eventi** visualizzata facendo clic sul collegamento dell'evento.

8. Un segno di spunta (✓) viene visualizzato nella colonna **Syslog** dell'evento o degli eventi contrassegnati per l'esportazione nel sistema SIEM.

D'ora in poi, Administration Server invia gli eventi contrassegnati al sistema SIEM se è configurata l'esportazione nel sistema SIEM.

Contrassegno di eventi generici per l'esportazione nel formato Syslog

È possibile contrassegnare gli eventi generici che Administration Server esporterà nei sistemi SIEM utilizzando il formato Syslog.

Per contrassegnare eventi generici per l'esportazione in un sistema SIEM:

1. Eseguire una delle seguenti operazioni:

- Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.
- Nel menu principale, passare a **Risorse (dispositivi)** → **Criteri e profili**, quindi fare clic sul collegamento di un criterio.

2. Nella finestra visualizzata accedere alla scheda **Configurazione eventi**.
3. Fare clic su **Contrassegna per l'esportazione nel sistema SIEM utilizzando Syslog**.

   È inoltre possibile contrassegnare un evento per l'esportazione nel sistema SIEM nella sezione **Registrazione eventi** visualizzata facendo clic sul collegamento dell'evento.

4. Un segno di spunta ( ) viene visualizzato nella colonna **Syslog** dell'evento o degli eventi contrassegnati per l'esportazione nel sistema SIEM.

D'ora in poi, Administration Server invia gli eventi contrassegnati al sistema SIEM se è configurata l'esportazione nel sistema SIEM.

Informazioni sull'esportazione degli eventi utilizzando il formato Syslog

È possibile utilizzare il formato Syslog per esportare nei sistemi SIEM gli eventi che si verificano in Administration Server e in altre applicazioni Kaspersky installate nei dispositivi gestiti.

Syslog è un protocollo standard per la registrazione dei messaggi. Consente una separazione tra il software che genera i messaggi, il sistema che li archivia e il software che li segnala e li analizza. Ogni messaggio dispone di un codice che indica il tipo di software che ha generato il messaggio e di un livello di criticità.

Il formato Syslog è definito dai documenti RFC (Request for Comments) pubblicati da Internet Engineering Task Force (standard Internet). Per l'esportazione degli eventi da Kaspersky Security Center Cloud Console nei sistemi esterni viene utilizzato lo standard RFC 5424.

In Kaspersky Security Center Cloud Console è possibile configurare l'esportazione degli eventi per i sistemi esterni tramite il formato Syslog.

Il processo di esportazione comprende due passaggi:

1. Abilitazione dell'esportazione automatica degli eventi. In questo passaggio Kaspersky Security Center Cloud Console viene configurato in modo da inviare gli eventi al sistema SIEM. Kaspersky Security Center Cloud Console inizia a inviare gli eventi subito dopo l'abilitazione dell'esportazione automatica.
2. Selezione degli eventi da esportare nel sistema esterno. In questo passaggio è possibile selezionare gli eventi da esportare nel sistema SIEM.

Configurazione di Kaspersky Security Center Cloud Console per l'esportazione degli eventi nel sistema SIEM

Per esportare gli eventi nel sistema SIEM, è necessario configurare il processo di esportazione in Kaspersky Security Center Cloud Console.

Per configurare l'esportazione nei sistemi SIEM in Kaspersky Security Center Cloud Console:

1. Nel menu principale, fare clic sull'icona delle impostazioni (⚙) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **SIEM**.

3. Fare clic sul collegamento **Impostazioni**.

   Si aprirà la sezione **Esporta impostazioni**.

4. Specificare le impostazioni nella sezione **Esporta impostazioni**:

   - **Indirizzo server del sistema SIEM**

     L'indirizzo IP del server in cui è installato il sistema SIEM utilizzato attualmente. Verificare questo valore nelle impostazioni del sistema SIEM.

   - **Porta del sistema SIEM**

     Numero della porta utilizzato per stabilire la connessione tra Kaspersky Security Center Cloud Console e il server del sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center Cloud Console e nelle impostazioni del destinatario del sistema SIEM.

   - **Protocollo**

È possibile utilizzare solo il protocollo TLS su TCP per trasferire i messaggi nel sistema SIEM. A tale scopo, specificare le impostazioni TLS:

- **Autenticazione server**

  Nel campo **Autenticazione server**, è possibile selezionare i valori **Certificati affidabili** o **Impronte digitali SHA**:

  - **Certificati affidabili**. È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione (CA) attendibile e caricare il file in Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console verifica se anche il certificato del server di sistema SIEM è firmato da un'autorità di certificazione attendibile o meno.

    Per aggiungere un certificato attendibile, fare clic sul pulsante **Cerca il file dei certificati CA**, quindi caricare il certificato.

  - **Impronte digitali SHA**. È possibile specificare le identificazioni personali SHA-1 dei certificati di sistema SIEM in Kaspersky Security Center Cloud Console. Per aggiungere un'identificazione personale SHA-1, immetterla nel campo **Identificazioni personali**, quindi fare clic sul pulsante **Aggiungi**.

    Utilizzando l'impostazione **Aggiungi autenticazione client**, è possibile generare un certificato per autenticare Kaspersky Security Center Cloud Console. Pertanto, verrà utilizzato un certificato autofirmato emesso da Kaspersky Security Center Cloud Console. In questo caso, è possibile utilizzare sia un certificato attendibile che un'impronta digitale SHA per autenticare il server di sistema SIEM.

- **Aggiungi nome soggetto/nome alternativo soggetto**

  Il nome del soggetto è un nome di dominio per il quale viene ricevuto il certificato. Kaspersky Security Center Cloud Console non può connettersi al server di sistema SIEM se il nome di dominio del server di sistema SIEM non corrisponde al nome del soggetto del certificato del server di sistema SIEM. Tuttavia, il server di sistema SIEM può modificare il proprio nome di dominio se il nome è stato modificato nel certificato. In questo caso, è possibile specificare i nomi dei soggetti nel campo **Aggiungi nome soggetto/nome alternativo soggetto**. Se uno dei nomi dei soggetti specificati corrisponde al nome del soggetto del certificato di sistema SIEM, Kaspersky Security Center Cloud Console convalida il certificato del server di sistema SIEM.

- **Aggiungi autenticazione client**

  Per l'autenticazione del client, è possibile inserire il certificato o generarlo in Kaspersky Security Center Cloud Console.

  - **Inserire il certificato**. È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. È necessario specificare il certificato e la relativa chiave privata utilizzando uno dei seguenti tipi di certificato:

    - **Certificato X.509 PEM**. Caricare un file con un certificato nel campo **File con certificato** e un file con una chiave privata nel campo **File con la chiave**. Entrambi i file non dipendono l'uno dall'altro e l'ordine di caricamento dei file non è significativo. Quando entrambi i file sono stati caricati, specificare la password per la decodifica della chiave privata nel campo **Verifica password o certificato**. La password può avere un valore vuoto se la chiave privata non è codificata.

    - **Certificato X.509 PKCS12**. Caricare un singolo file che contenga un certificato e la relativa chiave privata nel campo **File con certificato**. Quando il file viene caricato, specificare la password per la decodifica della chiave privata nel campo **Verifica password o certificato**. La password può avere un valore vuoto se la chiave privata non è codificata.

- **Genera chiave**. È possibile generare un certificato autofirmato in Kaspersky Security Center Cloud Console. Di conseguenza, Kaspersky Security Center Cloud Console archivia il certificato autofirmato generato ed è possibile passare la parte pubblica del certificato o l'impronta digitale SHA1 al sistema SIEM.

5. Facoltativamente è possibile esportare gli eventi archiviati dal database di Administration Server e impostare la data di inizio da cui si desidera avviare l'esportazione degli eventi archiviati:

   a. Fare clic sul collegamento **Impostare la data di inizio dell'esportazione**.

   b. Nella sezione visualizzata specificare la data di inizio nel campo **Data da cui iniziare l'esportazione**.

   c. Fare clic sul pulsante **OK**.

6. Spostare l'opzione sulla posizione **Esporta automaticamente gli eventi nel database del sistema SIEM Abilitato**.

7. Per verificare che la connessione al sistema SIEM sia configurata correttamente, fare clic sul pulsante **Verifica connessione**.

   Verrà visualizzato lo stato della connessione.

8. Fare clic sul pulsante **Salva**.

L'esportazione nel sistema SIEM è configurata. D'ora in poi, se è stata configurata la ricezione degli eventi in un sistema SIEM, Administration Server esporta gli eventi contrassegnati in un sistema SIEM. Se si imposta la data di inizio dell'esportazione, Administration Server esporta anche gli eventi contrassegnati archiviati nel database di Administration Server dalla data specificata.

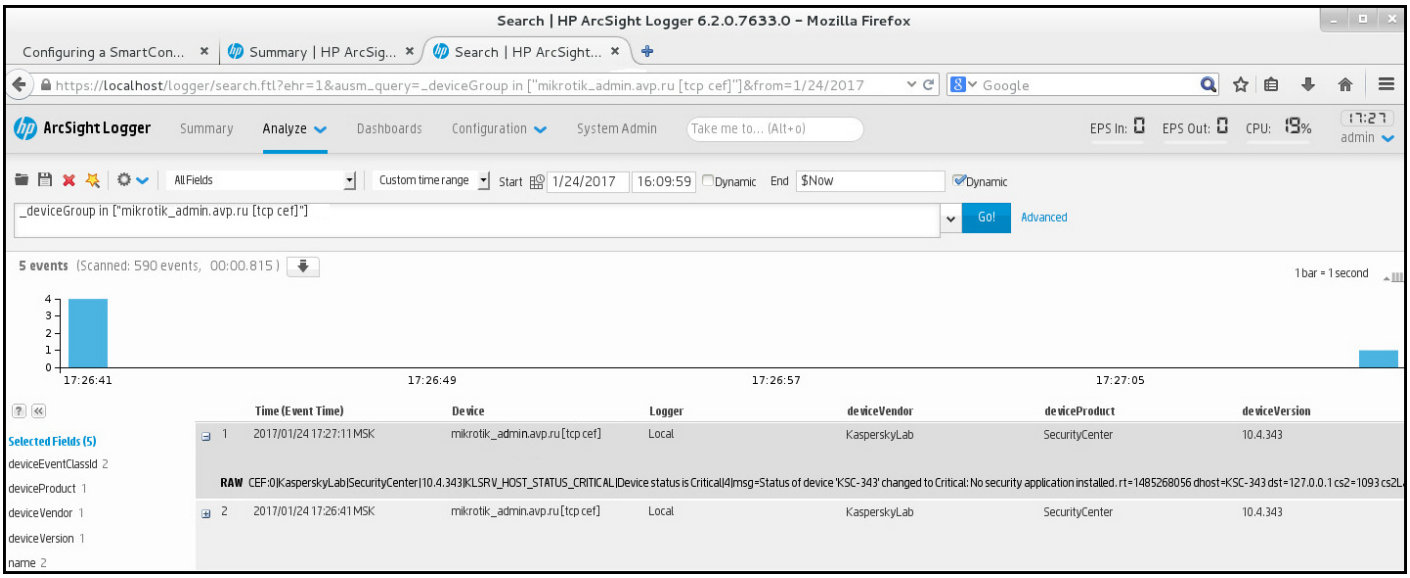
Visualizzazione dei risultati dell'esportazione

È possibile controllare il completamento della procedura di esportazione degli eventi. A tale scopo, controllare se i messaggi con gli eventi esportati vengono ricevuti dal sistema SIEM.

Se gli eventi inviati da Kaspersky Security Center Cloud Console vengono ricevuti e analizzati correttamente dal sistema SIEM, la configurazione su entrambi i lati è stata eseguita correttamente. In caso contrario, controllare le impostazioni specificate in Kaspersky Security Center Cloud Console rispetto alla configurazione del sistema SIEM.

La figura seguente illustra gli eventi esportati in ArcSight. Ad esempio, il primo evento è un evento critico di Administration Server: "*Lo stato del dispositivo è Critico*".

La rappresentazione degli eventi esportati nel sistema SIEM varia in base al sistema SIEM in uso.



Esempio di eventi

Guida introduttiva per MSP (Managed Service Providers)

La presente Guida introduttiva è destinata agli amministratori di MSP (Managed Service Provider).

Kaspersky Security Center Cloud Console supporta la funzionalità multi-tenancy. La Guida contiene suggerimenti e best practice per la gestione degli account dei clienti (tenant) e l'installazione di applicazioni di protezione nei relativi dispositivi.

Informazioni di Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console è un'applicazione ospitata e gestita da Kaspersky. Non è necessario installare Kaspersky Security Center Cloud Console nel computer o nel server. Kaspersky Security Center Cloud Console consente all'amministratore di installare le applicazioni di protezione Kaspersky nei dispositivi in una rete aziendale, eseguire in remoto attività di scansione e aggiornamento e gestire i criteri di sicurezza delle applicazioni gestite. L'amministratore può utilizzare una dashboard dettagliata che fornisce una panoramica degli stati dei dispositivi aziendali, rapporti dettagliati e impostazioni granulari nei criteri di protezione.

Funzionalità chiave di Kaspersky Security Center Cloud Console

Kaspersky Security Center Cloud Console consente di eseguire le seguenti operazioni:

- Installare le applicazioni Kaspersky nei dispositivi della rete e gestire le applicazioni installate.
- Creare una gerarchia di gruppi di amministrazione per gestire una selezione di dispositivi client come una singola unità.
- Creare Administration Server virtuali e disporli in una gerarchia.
- Proteggere i dispositivi della rete, inclusi workstation e server:
  - Gestire un sistema di protezione anti-malware basato sulle applicazioni Kaspersky.
  - Utilizzare le funzionalità di rilevamento e risposta EDR e MDR (è necessaria una licenza per Kaspersky Endpoint Detection and Response e/o per Kaspersky Managed Detection and Response), tra cui:
    - Analisi e ricerca degli incidenti
    - Visualizzazione degli incidenti attraverso la creazione di un grafico della catena di sviluppo delle minacce
    - Accettazione o rifiuto manuale delle risposte o impostazione dell'accettazione automatica di tutte le risposte
- Utilizzare Kaspersky Security Center Cloud Console come applicazione multi-tenant.
- Gestire in remoto le applicazioni Kaspersky installate nei dispositivi client.
- Eseguire la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi client.
- Creare e gestire criteri di protezione per i dispositivi nella rete.
- Creare e gestire account utente.

- Creare e gestire ruoli utente (RBAC).
- Creare e gestire attività per le applicazioni installate nei dispositivi della rete.
- Visualizzare i rapporti sullo stato del sistema di sicurezza singolarmente per ogni organizzazione client.

Informazioni sulla gestione delle licenze di Kaspersky Security Center Cloud Console per MSP

Quando si inizia a utilizzare Kaspersky Security Center Cloud Console, è possibile richiedere un'area di lavoro di prova (in questo caso viene concessa una licenza di prova di 30 giorni integrata nell'area di lavoro) o immettere un codice di attivazione per una licenza commerciale.

Non è possibile convertire un'area di lavoro di prova in un'area di lavoro commerciale. Per continuare a utilizzare Kaspersky Security Center Cloud Console dopo la scadenza della licenza di prova, è necessario eliminare l'area di lavoro di prova e crearne un'altra con una licenza commerciale.

Successivamente è possibile aggiungere una o più chiavi di licenza commerciali all'archivio dell'Administrator Server.

Informazioni sulle funzionalità di rilevamento e risposta per MSP

Kaspersky Security Center Cloud Console può integrare le funzionalità di altre applicazioni Kaspersky nell'interfaccia della console. È ad esempio possibile aggiungere le funzionalità di rilevamento e risposta alla funzionalità di Kaspersky Security Center Cloud Console integrando le seguenti applicazioni:

- Kaspersky Endpoint Detection and Response Optimum

  Kaspersky Endpoint Detection and Response Optimum è una soluzione progettata per proteggere l'infrastruttura IT di un'organizzazione da minacce informatiche complesse. La funzionalità della soluzione combina il rilevamento automatico delle minacce con la capacità di rispondere a queste minacce per resistere ad attacchi complessi, inclusi nuovi exploit, ransomware, attacchi senza file e metodi che utilizzano strumenti di sistema legittimi.

  Dopo che un'applicazione Kaspersky Endpoint Protection Platform (EPP) rileva un incidente di sicurezza, in Kaspersky Security Center Cloud Console viene generata una scheda dettagliata con dati importanti sull'incidente di sicurezza. La scheda dell'incidente viene generata da una delle seguenti applicazioni:

  - Kaspersky Endpoint Agent installato insieme a un'applicazione Kaspersky EPP
  - Kaspersky Endpoint Security 11.7.0 for Windows o versione successiva con la funzionalità EDR Optimum integrata non richiede l'installazione aggiuntiva di Kaspersky Endpoint Agent

  Una scheda incidente consente di condurre analisi e indagini sull'incidente. È inoltre possibile visualizzare l'incidente creando un grafico della catena di sviluppo delle minacce. Il grafico descrive le fasi di distribuzione dell'attacco rilevato nel tempo. Il grafico creato include informazioni sui moduli coinvolti nell'attacco e sulle azioni eseguite da questi moduli.

  È inoltre possibile avviare una catena di azioni di risposta: creare una regola di prevenzione dell'esecuzione per un oggetto non attendibile; cercare incidenti simili nel gruppo di dispositivi, in base agli indicatori di compromissione (IOC) selezionati; isolare un oggetto non attendibile; isolare un dispositivo compromesso dalla rete.

  Per informazioni sull'attivazione dell'applicazione, vedere la documentazione di Kaspersky Endpoint Detection and Response Optimum.

Se integrata, questa applicazione aggiunge la sezione **Avvisi** all'interfaccia di Kaspersky Security Center Cloud Console (**Monitoraggio e generazione dei rapporti** → **Avvisi**).

- Kaspersky Managed Detection and Response

  Kaspersky Managed Detection and Response offre protezione 24 ore su 24 dal crescente volume di minacce che aggirano le barriere di sicurezza automatizzate delle organizzazioni che faticano a trovare le competenze e il personale adeguati o che hanno risorse interne limitate. Gli analisti MDR SOC di Kaspersky o di un'azienda di terze parti indagano sugli incidenti e offrono risposte per risolverli. È possibile accettare o rifiutare le misure offerte manualmente o abilitare l'opzione per l'accettazione automatica di tutte le risposte.

  Per informazioni sull'attivazione dell'applicazione, vedere la documentazione di Kaspersky Managed Detection and Response.

  Se integrata, questa applicazione aggiunge la sezione **Incidenti** all'interfaccia di Kaspersky Security Center Cloud Console (**Monitoraggio e generazione dei rapporti** → **Incidenti**).

È possibile mostrare o nascondere gli elementi dell'interfaccia che fanno riferimento alle funzionalità di Kaspersky Endpoint Detection and Response o Kaspersky Managed Detection and Response in qualsiasi momento nella sezione **Opzioni di interfaccia** di Kaspersky Security Center Cloud Console.

Introduzione a Kaspersky Security Center Cloud Console

Dopo aver completato lo scenario in questa sezione, è possibile utilizzare Kaspersky Security Center Cloud Console.

Scenario iniziale

Lo scenario procede per fasi:

1. **Creare un account**

   Per iniziare a utilizzare Kaspersky Security Center Cloud Console, è necessario un account.

   Per creare un account:

   1. Aprire il browser e inserire la seguente URL: https://ksc.kaspersky.com.
   2. Fare clic sul pulsante **Crea account**.
   3. Seguire le istruzioni visualizzate.

2. **Creare un'area di lavoro**

   Dopo aver creato l'account, è possibile registrare la propria azienda e creare l'area di lavoro.

   Quando si inizia a utilizzare Kaspersky Security Center Cloud Console, è possibile richiedere un'area di lavoro di prova (in questo caso viene concessa una licenza di prova di 30 giorni integrata nell'area di lavoro) o immettere un codice di attivazione per una licenza commerciale.

   > Non è possibile convertire un'area di lavoro di prova in un'area di lavoro commerciale. Per continuare a utilizzare Kaspersky Security Center Cloud Console dopo la scadenza della licenza di prova, è necessario eliminare l'area di lavoro di prova e crearne un'altra con una licenza commerciale.

   Per registrare un'azienda e creare un'area di lavoro:

   1. Aprire il browser e inserire la seguente URL: https://ksc.kaspersky.com.

2. Fare clic sul pulsante **Accedi**.

3. Seguire le istruzioni visualizzate.

3. **Eseguire la configurazione iniziale di Kaspersky Security Center Cloud Console**

   Al primo accesso nell'area di lavoro creata, viene automaticamente richiesto di eseguire l'avvio rapido guidato. L'avvio rapido guidato consente di creare una quantità minima di attività e criteri necessari, regolare una quantità minima di impostazioni e iniziare a creare i pacchetti di installazione delle applicazioni Kaspersky. Seguire le istruzioni visualizzate.

Al termine della configurazione iniziale, è possibile utilizzare Kaspersky Security Center Cloud Console.

Consigli sulla gestione dei dispositivi dei clienti

Questa sezione contiene suggerimenti per l'organizzazione dei dispositivi dei clienti che si desidera proteggere.

I suggerimenti dipendono dal fatto che si stia utilizzando Kaspersky Security Center per la prima volta o che sia già stata utilizzata la versione locale:

- Se Kaspersky Security Center non è mai stato utilizzato in precedenza, sono disponibili due opzioni:
  - Creare un Administration Server virtuale per i dispositivi di ciascun cliente (opzione consigliata). In questo caso, i dispositivi di ciascun cliente possono essere gestiti tramite un Administration Server virtuale dedicato indipendentemente dagli altri clienti. Allo stesso tempo, è possibile utilizzare l'Administration Server primario per creare criteri e attività comuni per tutti i clienti. I rapporti generati sull'Administration Server primario possono includere i dati di tutti gli Administration Server virtuali.
  - Creare un gruppo di amministrazione per i dispositivi di ciascun cliente. Se si desidera suddividere ulteriormente i dispositivi dei clienti, è possibile creare una gerarchia di gruppi di amministrazione subordinati in ciascun gruppo padre. Potrebbero ad esempio essere necessari gruppi subordinati se si desidera utilizzare impostazioni di protezione diverse per i dispositivi dei dipendenti che lavorano in reparti diversi.
- Se Kaspersky Security Center è già stato utilizzato in locale, è possibile eseguire la migrazione dei gruppi di amministrazione esistenti e degli oggetti correlati da Kaspersky Security Center in locale a Kaspersky Security Center Cloud Console.

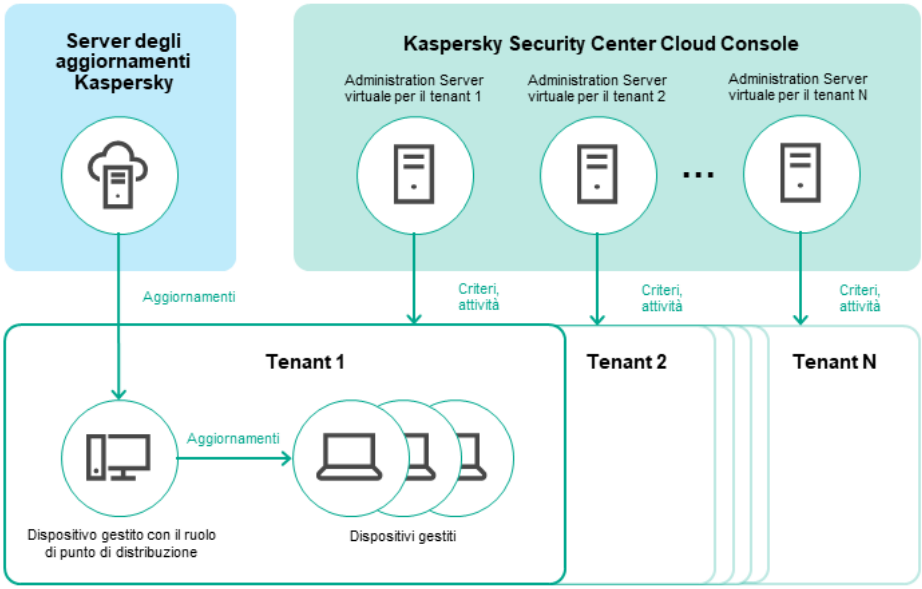
  Non è possibile eseguire la migrazione di Administration Server virtuali. Dopo aver eseguito la migrazione dei gruppi di amministrazione e di altri oggetti, è possibile creare Administration Server virtuali in Kaspersky Security Center Cloud Console.

  Procedere alla configurazione della migrazione.

L'amministratore di un Administration Server virtuale può procedere a questo server virtuale solo dall'Administration Server primario. Tutti gli oggetti creati nell'Administration Server primario sono disponibili per la lettura da parte dell'amministratore di un Administration Server virtuale (ad esempio, widget, rapporti o ruoli utente).

Schema di distribuzione tipico per MSP

Questa sezione fornisce una descrizione dello schema di distribuzione generalmente utilizzato dagli MSP per gestire più tenant. Lo schema si basa sulla gestione tramite Administration Server virtuali creati singolarmente per ciascun tenant.



Schema di distribuzione tipico per MSP

Lo schema comprende i seguenti componenti principali:

- *Kaspersky Security Center Cloud Console*. Fornisce un'interfaccia utente ai servizi di amministrazione dell'area di lavoro. Kaspersky Security Center Cloud Console si utilizza per la distribuzione, la gestione e la manutenzione del sistema di protezione della rete di un'organizzazione client.
- *Server di aggiornamento Kaspersky*. I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.
- *Administration Server virtuali*. Un amministratore MSP in genere crea un Administration Server virtuale per ciascun tenant per distribuire, gestire ed eseguire la manutenzione del sistema di protezione della rete dell'organizzazione client corrispondente.
- *Tenant*. Organizzazioni client i cui dispositivi devono essere protetti.
- *Dispositivi gestiti*. Dispositivi dell'azienda client protetti da Kaspersky Security Center Cloud Console. In ogni dispositivo che deve essere protetto devono essere installati Network Agent e una delle applicazioni di protezione Kaspersky.
- *Dispositivo gestito che funge da punto di distribuzione*. Computer in cui è installato Network Agent e che viene utilizzato per la distribuzione di aggiornamenti, il polling della rete, l'installazione remota di applicazioni, il recupero di informazioni sui computer in un gruppo di amministrazione e/o la trasmissione in un dominio. L'amministratore seleziona i dispositivi appropriati e assegna manualmente i punti di distribuzione.

Scenario: distribuzione della protezione (gestione dei tenant tramite Administration Server virtuali)

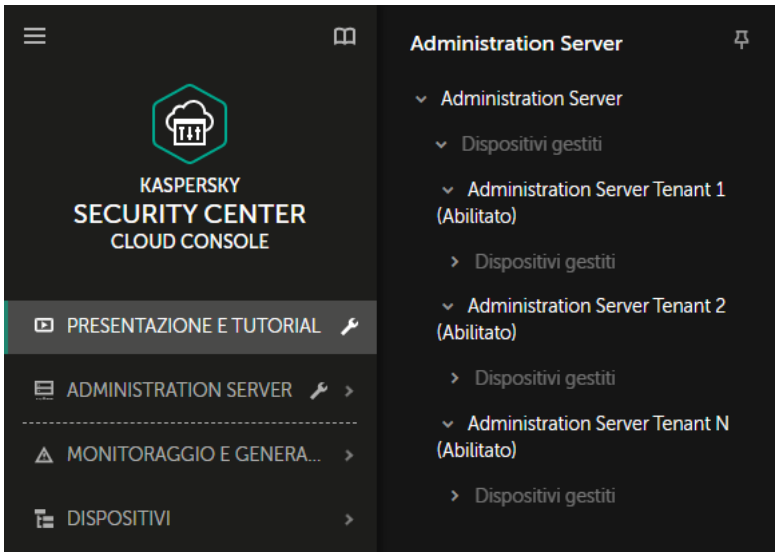
Se Kaspersky Security Center non è mai stato utilizzato e si desidera gestire i tenant tramite Administration Server virtuali, procedere come descritto in questa sezione. Dopo aver completato questo scenario, i dispositivi dei clienti saranno protetti.

Se si gestiscono più tenant, eseguire lo scenario per ciascun tenant separatamente.

Lo scenario procede per fasi:

1 Creazione di un Administration Server virtuale

Creare un Administration Server virtuale per il cliente. Il nuovo Administration Server virtuale viene visualizzato nella gerarchia di Administration Server:



Administration Server virtuali nella gerarchia di Administration Server

2 Selezione di un dispositivo a cui assegnare il ruolo di punto di distribuzione

Tra i dispositivi del cliente, decidere quale dispositivo fungerà da punto di distribuzione.

Non è possibile disporre di più di 100 punti di distribuzione all'interno di un'unica area di lavoro.

3 Creazione di un pacchetto di installazione indipendente per Network Agent

Passare all'Administration Server virtuale creato, quindi creare un pacchetto di installazione indipendente per Network Agent. È possibile passare da un Administration Server all'altro nel menu principale facendo clic sull'icona della freccia di espansione (▸) a destra del nome dell'Administration Server corrente, per poi selezionare l'Administration Server desiderato. Durante la creazione del pacchetto di installazione indipendente, specificare il gruppo di amministrazione Dispositivi gestiti in cui spostare il dispositivo.

4 Installazione di Network Agent nel dispositivo selezionato per fungere da punto di distribuzione

È possibile utilizzare qualsiasi metodo idoneo:

- Installazione manuale

  Per distribuire il pacchetto di installazione indipendente al dispositivo, è ad esempio possibile copiarlo in un'unità rimovibile (come un'unità flash) o posizionarlo in una cartella condivisa.

- Distribuzione tramite Active Directory

- Distribuzione tramite la soluzione software RMM (Remote Monitoring And Management)

5 Assegnazione di un punto di distribuzione

Assegnare al dispositivo in cui è installato Network Agent il ruolo di punto di distribuzione.

6 Polling della rete

Configurare ed eseguire il polling della rete tramite il punto di distribuzione.

Kaspersky Security Center Cloud Console offre i seguenti metodi di polling della rete:

- Polling intervallo IP

- Polling della rete Windows
- Polling Active Directory

Al termine del polling della rete in base alla pianificazione, i dispositivi dei clienti vengono rilevati e inseriti nel gruppo **Dispositivi non assegnati**.

7. **Spostamento dei dispositivi rilevati nei gruppi di amministrazione**

   Configurare le regole per lo spostamento automatico dei dispositivi rilevati nei gruppi di amministrazione desiderati; in alternativa spostare questi dispositivi nei gruppi di amministrazione desiderati manualmente. Se si prevede di gestire i dispositivi del cliente in un singolo gruppo di amministrazione, è possibile spostare i dispositivi nel gruppo Dispositivi gestiti.

8. **Creazione di pacchetti di installazione per Network Agent e le applicazioni Kaspersky gestite**

   Creare pacchetti di installazione per le applicazioni Kaspersky.

9. **Rimozione di applicazioni di protezione di terze parti**

   Se nei dispositivi dei clienti sono installate applicazioni di protezione di terze parti, rimuoverle prima di installare applicazioni Kaspersky.

10. **Installazione delle applicazioni Kaspersky nei dispositivi client**

    Creare attività di installazione remota per installare Network Agent e le applicazioni Kaspersky gestite nei dispositivi dei clienti.

    Se necessario, è possibile creare diverse attività di installazione remota per installare le applicazioni Kaspersky gestite per diversi gruppi di amministrazione o diverse selezioni dispositivi.

    Dopo la creazione delle attività, è possibile configurarne le impostazioni. Assicurarsi che la pianificazione per ciascuna attività soddisfi i requisiti. Prima di tutto è necessario eseguire l'attività di installazione di Network Agent. Dopo aver installato Network Agent nei dispositivi dei clienti, è necessario eseguire l'attività per installare le applicazioni Kaspersky gestite.

11. **Verifica della distribuzione iniziale delle applicazioni Kaspersky**

    Generare e visualizzare il **Rapporto sulle versioni del software Kaspersky**. Assicurarsi che le applicazioni Kaspersky gestite siano installate in tutti i dispositivi del cliente.

12. **Creazione dei criteri per le applicazioni Kaspersky**

    Creare un criterio per l'applicazione Kaspersky desiderata. Se si desidera creare un criterio universale per tutti i clienti, passare dall'Administration Server virtuale corrente all'Administration Server primario, quindi creare un criterio per l'applicazione Kaspersky desiderata.

Scenario: Distribuzione della protezione (gestione dei tenant tramite gruppi di amministrazione)

Se Kaspersky Security Center non è mai stato utilizzato e si desidera gestire i tenant tramite gruppi di amministrazione, procedere come descritto in questa sezione. Dopo aver completato questo scenario, i dispositivi dei clienti saranno protetti.

Lo scenario procede per fasi:

1. **Creazione dei gruppi di amministrazione**

   Creare un gruppo di amministrazione per ogni cliente.

2. **Pianificazione della struttura dei punti di distribuzione**

   Tra i dispositivi di ogni cliente, decidere quale dispositivo fungerà da punto di distribuzione.

   > Non è possibile disporre di più di 100 punti di distribuzione all'interno di un'unica area di lavoro.

3. **Creazione di un pacchetto di installazione indipendente per Network Agent**

   Creare un pacchetto di installazione indipendente per Network Agent.

4. **Installazione di Network Agent nei dispositivi selezionati con il ruolo di punti di distribuzione**

   Installare Network Agent nei dispositivi selezionati con il ruolo di punti di distribuzione.

   È possibile utilizzare qualsiasi metodo idoneo:

   - Installazione manuale

     Per distribuire il pacchetto di installazione indipendente ai dispositivi, è ad esempio possibile copiarlo in un'unità rimovibile (ad esempio un'unità flash) o posizionarlo in una cartella condivisa.

   - Distribuzione tramite Active Directory

   - Distribuzione tramite la soluzione software RMM (Remote Monitoring And Management)

5. **Assegnazione dei punti di distribuzione**

   Assegnare ai dispositivi in cui è installato Network Agent il ruolo di punti di distribuzione.

6. **Polling della rete**

   Configurare ed eseguire il polling della rete tramite il punto di distribuzione.

   Kaspersky Security Center Cloud Console offre i seguenti metodi di polling della rete:

   - Polling intervallo IP

   - Polling della rete Windows

   - Polling Active Directory

   Al termine del polling della rete in base alla pianificazione, i dispositivi dei clienti vengono rilevati e inseriti nel gruppo **Dispositivi non assegnati**.

7. **Spostamento dei dispositivi rilevati nei gruppi di amministrazione**

   Configurare le regole per lo spostamento automatico dei dispositivi rilevati nei gruppi di amministrazione desiderati; in alternativa spostare questi dispositivi nei gruppi di amministrazione desiderati manualmente.

8. **Creazione di pacchetti di installazione per Network Agent e le applicazioni Kaspersky gestite**

   Se non è stato avviato l'Avvio rapido guidato o è stato ignorato il passaggio di creazione dei pacchetti di installazione, creare pacchetti di installazione per le applicazioni Kaspersky.

9. **Rimozione di applicazioni di protezione di terze parti**

   Se nei dispositivi dei clienti sono installate applicazioni di protezione di terze parti, rimuoverle prima di installare applicazioni Kaspersky.

10. **Installazione delle applicazioni Kaspersky nei dispositivi dei clienti**

    Creare attività di installazione remota per installare Network Agent e le applicazioni Kaspersky gestite nei dispositivi dei clienti.

Se necessario, è possibile creare diverse attività di installazione remota per installare le applicazioni Kaspersky gestite per diversi gruppi di amministrazione o diverse selezioni dispositivi.

Dopo la creazione delle attività, è possibile configurarne le impostazioni. Assicurarsi che la pianificazione per ciascuna attività soddisfi i requisiti. Prima di tutto è necessario eseguire l'attività di installazione di Network Agent. Dopo aver installato Network Agent nei dispositivi dei clienti, è necessario eseguire l'attività per installare le applicazioni Kaspersky gestite.

11. **Verifica della distribuzione iniziale delle applicazioni Kaspersky**

    Generare e visualizzare il **Rapporto sulle versioni del software Kaspersky**. Assicurarsi che le applicazioni Kaspersky gestite siano installate in tutti i dispositivi dei clienti.

12. **Creazione dei criteri per le applicazioni Kaspersky**

    Accedere al menu **Risorse (dispositivi)** → **Gruppi**; se si desidera creare un criterio universale per tutti i clienti, selezionare **Administration Server.** Se si desidera creare un criterio specifico per un singolo cliente, selezionare il gruppo di amministrazione corrispondente a tale cliente. Creare un criterio per l'applicazione Kaspersky desiderata.

Utilizzo combinato di Kaspersky Security Center locale e Kaspersky Security Center Cloud Console

Se è già stato utilizzato Kaspersky Security Center in esecuzione in locale, è possibile convertire gli Administration Server esistenti in esecuzione in locale in Administration Server secondari del nuovo Administration Server di Kaspersky Security Center Cloud Console, come descritto in questa sezione.

> Se si configura l'utilizzo combinato di Kaspersky Security Center locale e Kaspersky Security Center Cloud Console, non sarà possibile eseguire la migrazione da Kaspersky Security Center locale a Kaspersky Security Center Cloud Console, a meno che non si rimuova la gerarchia di Administration Server.

Per creare una gerarchia di Administration Server,

Aggiungere gli Administration Server esistenti in esecuzione in locale come Administration Server secondari.

Gestione delle licenze delle applicazioni Kaspersky per MSP

Kaspersky Security Center Cloud Console consente la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi dei clienti, il monitoraggio del relativo utilizzo e il rinnovo delle licenze.

Se si gestiscono più tenant, è possibile distribuire le chiavi di licenza nei seguenti modi:

- Una chiave di licenza per tutti i tenant.
- Una chiave di licenza singola per ciascun tenant.

Per distribuire le chiavi di licenza nei dispositivi dei clienti:

1. Aggiungere le chiavi di licenza richieste all'archivio di Administration Server.
2. Eseguire una delle seguenti operazioni:
    - Configurare la distribuzione automatica di una chiave di licenza.

In questo caso, Kaspersky Security Center Cloud Console seleziona una delle chiavi di licenza applicabili e la distribuisce automaticamente ogni volta che viene rilevato un nuovo dispositivo.

- Configurare l'attività Aggiungi una chiave per distribuire una chiave di licenza ai dispositivi.

  Durante la configurazione dell'attività, selezionare la chiave di licenza che deve essere distribuita ai dispositivi e selezionare il gruppo di amministrazione contenente i dispositivi richiesti.

  Una singola attività può distribuire una sola chiave di licenza. Ciò significa che se si desidera distribuire più chiavi di licenza, è necessario creare un'attività per ognuna di esse.

Le applicazioni Kaspersky installate nei dispositivi dei clienti sono attivate.

Funzionalità di monitoraggio e generazione di rapporti per MSP

Kaspersky Security Center Cloud Console offre funzionalità di monitoraggio e reporting. Queste funzionalità offrono una panoramica dell'infrastruttura dell'organizzazione, degli stati di protezione e delle statistiche.

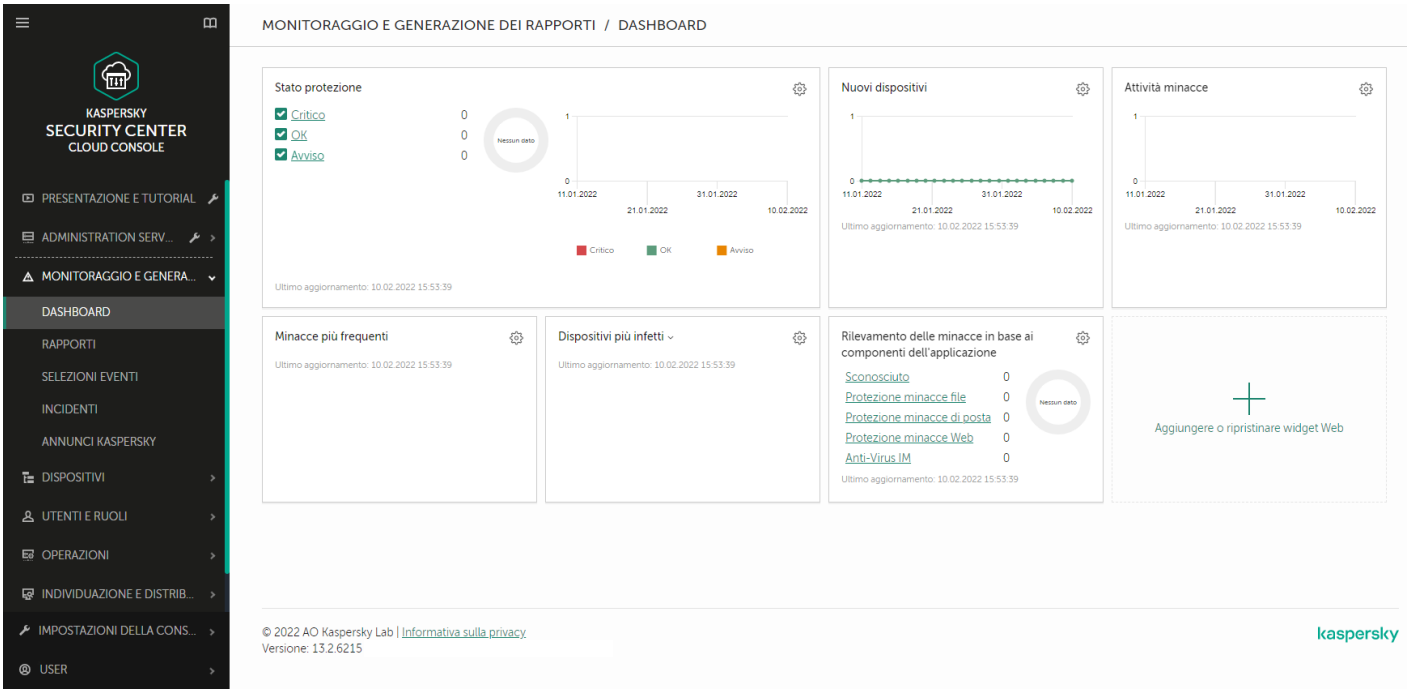
Dopo aver distribuito Kaspersky Security Center Cloud Console, è possibile configurare le funzionalità di monitoraggio e reporting in base alle proprie esigenze.

Kaspersky Security Center Cloud Console offre i seguenti tipi di funzionalità di monitoraggio e reporting:

- Dashboard
- Rapporti
- Selezioni eventi
- Notifiche e-mail

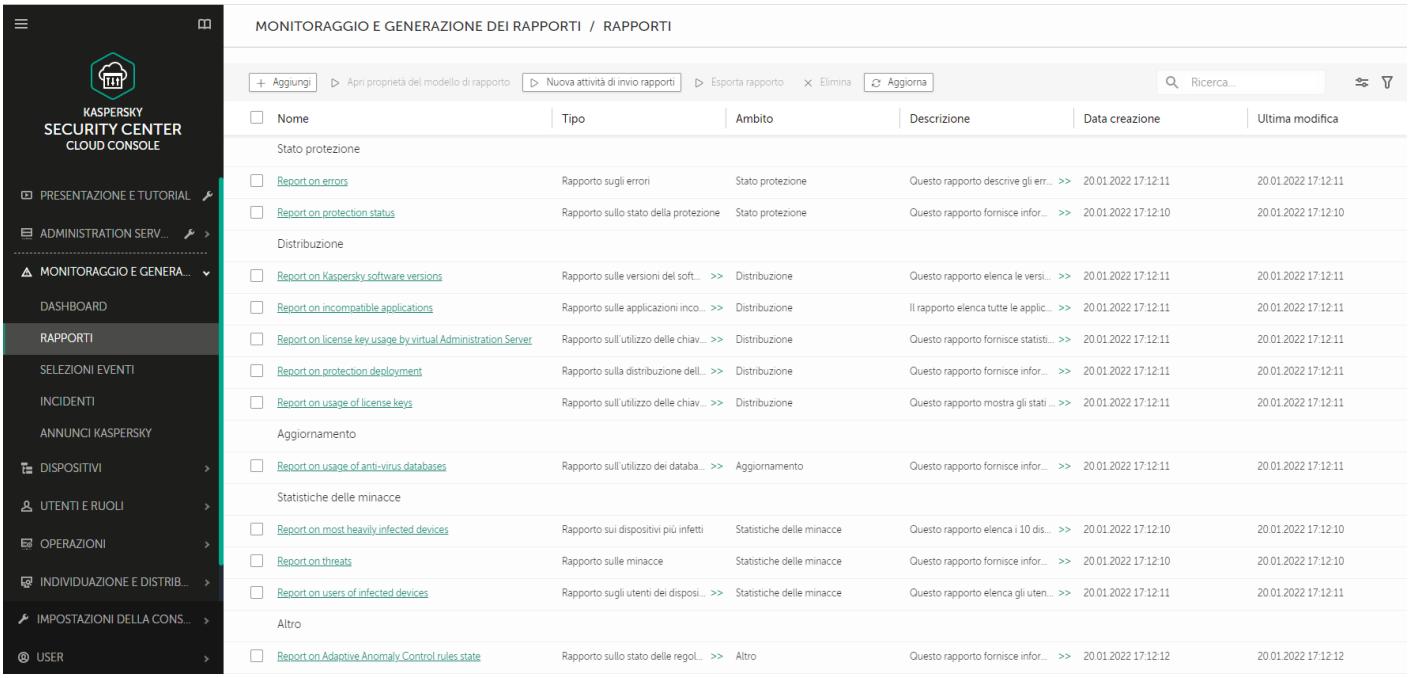
Dashboard

Il dashboard consente di monitorare le tendenze relative alla sicurezza nella rete dell'organizzazione fornendo una visualizzazione grafica delle informazioni (vedere la figura sottostante).



Rapporti

La funzionalità Rapporti consente di ottenere informazioni numeriche dettagliate sulla sicurezza della rete dell'organizzazione, nonché di salvare le informazioni in un file, inviarlo tramite e-mail e stamparlo. È inoltre possibile pianificare l'invio dei rapporti tramite e-mail (vedere la figura di seguito).



Sezione Rapporti

Selezioni eventi

Le selezioni eventi consentono di visualizzare i set denominati degli eventi selezionati dal database di Administration Server. Kaspersky Security Center Cloud Console contiene una serie di selezioni eventi predefinite (ad esempio **Eventi recenti** e **Eventi critici**). È inoltre possibile creare selezioni eventi personalizzate.

Notifiche e-mail

È possibile configurare notifiche e-mail per gli eventi che si verificano in Kaspersky Security Center Cloud Console e nei dispositivi dei clienti.

Utilizzo di Kaspersky Security Center Cloud Console in un ambiente cloud

Questa sezione fornisce informazioni sulle funzionalità di Kaspersky Security Center Cloud Console relative al funzionamento e alla manutenzione di Kaspersky Security Center Cloud Console negli ambienti cloud, ad esempio Amazon Web Services, Microsoft Azure o Google Cloud.

Per l'utilizzo in un ambiente cloud è necessaria una licenza speciale. Se non si dispone di tale licenza, gli elementi dell'interfaccia relativi ai dispositivi cloud non sono funzionanti.

Opzioni di licenza in un ambiente cloud

L'utilizzo in un ambiente cloud è possibile sia nella modalità di prova che nella modalità commerciale di Kaspersky Security Center Cloud Console:

- Nella modalità di prova tutte le funzionalità dell'ambiente cloud sono disponibili per l'intero periodo di validità dell'area di lavoro. Non è richiesta alcuna licenza.
- Nella modalità commerciale le funzionalità dell'ambiente cloud sono disponibili solo se è stata aggiunta una chiave di licenza Kaspersky Hybrid Cloud Security come attiva nelle proprietà di Administration Server.

In entrambi i casi, Vulnerability e patch management è automaticamente attivata.

È possibile che si verifichi un errore durante il tentativo di attivare la funzionalità Supporto dell'ambiente cloud utilizzando la licenza per Kaspersky Hybrid Cloud Security.

Preparazione per l'utilizzo nell'ambiente cloud tramite Kaspersky Security Center Cloud Console

In questa sezione viene descritto come eseguire la preparazione per l'utilizzo di Kaspersky Security Center Cloud Console nei seguenti ambienti cloud:

- Amazon Web Services
- Microsoft Azure
- Google Cloud

Utilizzo dell'ambiente cloud Amazon Web Services

In questa sezione viene descritto come eseguire la preparazione per l'utilizzo di Kaspersky Security Center Cloud Console in Amazon Web Services.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center Cloud Console.

Informazioni sull'utilizzo dell'ambiente cloud Amazon Web Services

Per utilizzare la piattaforma AWS e, in particolare, per creare istanze, è necessario un account Amazon Web Services. È possibile creare un account gratuito all'indirizzo https://aws.amazon.com/it. È anche possibile utilizzare un account Amazon esistente.

Per ulteriori informazioni su un'AMI e sul funzionamento di AWS Marketplace, visitare la pagina della Guida di AWS Marketplace. Per ulteriori informazioni sull'utilizzo della piattaforma AWS, l'utilizzo delle istanze e i relativi concetti, fare riferimento alla documentazione di Amazon Web Services.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center Cloud Console.

Creazione di account utente IAM per le istanze Amazon EC2

In questa sezione sono descritte le azioni da eseguire per garantire il corretto funzionamento di Kaspersky Security Center Cloud Console. Queste azioni includono l'utilizzo degli account utente IAM (Identity and Access Management) AWS. Sono inoltre descritte le azioni che devono essere eseguite nei dispositivi client per installare Network Agent in tali dispositivi e quindi installare Kaspersky Security for Windows Server e Kaspersky Endpoint Security for Linux.

Verifica delle autorizzazioni di Kaspersky Security Center Cloud Console per l'utilizzo di AWS

Per operare nell'ambiente cloud di Amazon Web Services utilizzando Kaspersky Security Center Cloud Console, è necessario creare un *account utente IAM*, che verrà utilizzato da Kaspersky Security Center Cloud Console per l'utilizzo dei servizi AWS. Prima di iniziare a utilizzare Administration Server, creare un account utente IAM con una *chiave di accesso AWS IAM* (di seguito denominata anche *chiave di accesso IAM*).

La creazione di un account utente IAM richiede la console di gestione AWS. Per utilizzare la console di gestione AWS, saranno necessari il nome utente e la password di un account AWS.

Creazione di un account utente IAM per l'utilizzo di Kaspersky Security Center Cloud Console

Un account utente IAM è necessario per l'utilizzo di Kaspersky Security Center Cloud Console. È possibile creare un solo account utente IAM con tutte le autorizzazioni necessarie oppure due account utente distinti.

Per l'utente IAM viene creata automaticamente una *chiave di accesso IAM* che sarà necessario fornire a Kaspersky Security Center Cloud Console durante la configurazione iniziale. Una chiave di accesso IAM è costituita da un ID chiave di accesso e da una chiave segreta. Per ulteriori informazioni sul servizio IAM, consultare le seguenti pagine di riferimento su AWS:

- https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- https://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Per creare un account utente IAM con le autorizzazioni richieste:

1. Aprire la console di gestione AWS e accedere con il proprio account.
2. Nell'elenco dei servizi AWS selezionare **IAM**.

   Verrà visualizzata una finestra che contiene un elenco di nomi utente e un menu che consente di utilizzare lo strumento.
3. Spostarsi tra le aree della console per gestire gli account utente e aggiungere uno o più nomi utente.
4. Per gli utenti aggiunti, specificare le seguenti proprietà AWS:
   - Tipo di accesso: **Programmatic Access**.
   - Limite per le autorizzazioni non impostato.
   - Autorizzazione: **ReadOnlyAccess**.

     Dopo aver aggiunto l'autorizzazione, verificarne la correttezza. Se la selezione è errata, tornare alla finestra precedente e ripetere la selezione.
5. Dopo la creazione dell'account utente, verrà visualizzata una tabella contenente la chiave di accesso IAM del nuovo utente IAM. L'ID chiave di accesso sarà visualizzato nella colonna **Access key ID**. La chiave segreta sarà visualizzata tramite asterischi nella colonna **Secret access key**. Per visualizzare la chiave segreta, fare clic su **Show**.

Il nuovo account creato verrà visualizzato nell'elenco degli account utente IAM corrispondente all'account in AWS.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center Cloud Console.

Utilizzo dell'ambiente cloud Microsoft Azure

Questa sezione fornisce informazioni sulla manutenzione e sul funzionamento di Kaspersky Security Center Cloud Console in un ambiente cloud fornito da Microsoft Azure, nonché i dettagli sulla distribuzione della protezione nelle macchine virtuali in questo ambiente cloud.

Informazioni sull'utilizzo di Microsoft Azure

Per utilizzare la piattaforma Microsoft Azure e, in particolare, per acquistare app in Azure Marketplace e creare macchine virtuali, è necessaria una sottoscrizione Azure. Prima di iniziare a utilizzare Microsoft Azure in Kaspersky Security Center Cloud Console, creare un ID applicazione Azure con le autorizzazioni necessarie per l'installazione delle applicazioni nelle macchine virtuali.

Creazione di una sottoscrizione, un ID applicazione e una password

Per utilizzare Kaspersky Security Center Cloud Console nell'ambiente Microsoft Azure, sono necessari una sottoscrizione Azure, l'ID applicazione Azure e la password dell'applicazione Azure. È possibile utilizzare una sottoscrizione esistente, se si dispone già di una sottoscrizione.

Una sottoscrizione Azure consente al proprietario di accedere al portale di gestione della piattaforma Microsoft Azure e ai servizi Microsoft Azure. Il proprietario può utilizzare la piattaforma Microsoft Azure per gestire servizi come Azure SQL e Archiviazione di Azure.

Per creare una sottoscrizione Microsoft Azure:

Visitare l'indirizzo https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription e seguire le istruzioni.

Ulteriori informazioni sulla creazione di una sottoscrizione sono disponibili nel sito Web di Microsoft. Verrà creato un ID sottoscrizione, che in un secondo momento sarà necessario specificare in Kaspersky Security Center Cloud Console insieme con l'ID applicazione e la password.

Per creare e salvare l'ID applicazione Azure e la password:

1. Visitare https://portal.azure.com e verificare di aver eseguito l'accesso.
2. Creare l'ID applicazione, seguendo le istruzioni nella pagina di riferimento.
3. Passare alla sezione **Chiavi** delle impostazioni dell'applicazione.
4. Nella sezione **Chiavi** compilare i campi **Descrizione** e **Scadenza** e lasciare vuoto il campo **Valore**.
5. Fare clic su **Salva**.

   Facendo clic su **Salva**, il sistema inserisce automaticamente nel campo **Valore** una lunga sequenza di caratteri. La sequenza è la password dell'applicazione Azure (ad esempio yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). La descrizione è visualizzata così come viene immessa.
6. Copiare la password e salvarla in modo da poter specificare in un secondo momento l'ID applicazione e la password in Kaspersky Security Center Cloud Console.

   È possibile copiare la password solo al momento della creazione. Successivamente, la password non verrà più visualizzata e non potrà essere ripristinata.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center Cloud Console.

Assegnazione di un ruolo all'ID applicazione Azure

Se si desidera rilevare le macchine virtuali solo tramite la device discovery, l'ID applicazione Azure deve disporre del ruolo Lettura. Se si desidera non solo rilevare le macchine virtuali, ma anche distribuire la protezione tramite l'API Azure, l'ID applicazione Azure deve disporre del ruolo Collaboratore macchine virtuali.

Seguire le istruzioni nel sito Web di Microsoft per assegnare un ruolo all'ID applicazione Azure.

Utilizzo in Google Cloud

Questa sezione contiene informazioni sull'utilizzo di Kaspersky Security Center Cloud Console in un ambiente cloud fornito da Google.

È possibile avvalersi dell'API di Google per utilizzare Kaspersky Security Center Cloud Console in Google Cloud Platform. È richiesto un account Google. Per ulteriori informazioni, fare riferimento alla documentazione di Google all'indirizzo https://cloud.google.com.

Sarà necessario creare e fornire a Kaspersky Security Center Cloud Console le seguenti credenziali:

- **E-mail client**

  L'e-mail client è l'indirizzo e-mail utilizzato per la registrazione del progetto in Google Cloud.

- **ID progetto**

  L'ID progetto è l'ID ricevuto durante la registrazione del progetto in Google Cloud.

- **Chiave privata**

  La chiave privata è la sequenza di caratteri ricevuta come chiave privata durante la registrazione del progetto in Google Cloud. È consigliabile copiare e incollare questa sequenza per evitare errori.

Configurazione guidata ambiente cloud in Kaspersky Security Center Cloud Console

Per configurare Kaspersky Security Center Cloud Console tramite questa procedura guidata, sono necessari i seguenti prerequisiti:

- Credenziali specifiche per un ambiente cloud:
  - Un account utente IAM a cui è stato concesso il diritto di eseguire il polling del segmento cloud (per l'utilizzo con Amazon Web Services)
  - ID applicazione Azure, password e sottoscrizione (per l'utilizzo con Microsoft Azure)
  - E-mail client Google, ID progetto e chiave privata (per l'utilizzo con Google Cloud)
- Pacchetti di installazione:
  - Network Agent per Windows
  - Network Agent per Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in Web per Kaspersky Endpoint Security for Linux
- Almeno uno dei seguenti componenti:
  - Pacchetto di installazione e plug-in Web per Kaspersky Endpoint Security for Windows (consigliato)

- Pacchetto di installazione e plug-in Web per Kaspersky Security for Windows Server

La Configurazione guidata ambiente cloud viene avviata automaticamente alla prima connessione a Kaspersky Security Center Cloud Console se l'area di lavoro è stata creata utilizzando la licenza Kaspersky Hybrid Cloud Security. È anche possibile avviare manualmente la Configurazione guidata ambiente cloud in qualsiasi momento.

Per avviare manualmente la Configurazione guidata ambiente cloud:

Nel menu principale accedere a **Individuazione e distribuzione → Distribuzione e assegnazione → Configura ambiente cloud**.

Verrà avviata la procedura guidata.

Il tempo medio per una sessione di lavoro con questa procedura guidata è di circa 15 minuti.

Passaggio 1. Controllo dei plug-in e dei pacchetti di installazione necessari

Questo passaggio non viene visualizzato se si dispone di tutti i plug-in Web e dei pacchetti di installazione necessari elencati di seguito.

Per configurare un ambiente cloud, è necessario disporre dei seguenti componenti:

- Pacchetti di installazione:
  - Network Agent per Windows
  - Network Agent per Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in Web per Kaspersky Endpoint Security for Linux
- Almeno uno dei seguenti componenti:
  - Pacchetto di installazione e plug-in Web per Kaspersky Endpoint Security for Windows (consigliato)
  - Pacchetto di installazione e plug-in Web per Kaspersky Security for Windows Server

    Si consiglia di utilizzare Kaspersky Endpoint Security for Windows anziché Kaspersky Security for Windows Server.

Kaspersky Security Center Cloud Console rileva automaticamente i componenti di cui si dispone già ed elenca solo quelli mancanti. Scaricare i componenti elencati facendo clic su **Seleziona le applicazioni da scaricare**, quindi selezionare i plug-in e i pacchetti di installazione necessari. Dopo aver scaricato un componente, è possibile utilizzare il pulsante **Aggiorna** per aggiornare l'elenco dei componenti mancanti.

Passaggio 2. Selezione del metodo di attivazione dell'applicazione

Questo passaggio viene visualizzato solo se durante la creazione dell'area di lavoro è stata utilizzata una licenza diversa da Kaspersky Hybrid Cloud Security e non è mai stata aggiunta una chiave di licenza di Kaspersky Hybrid Cloud Security nel campo di attivazione di Administration Server. In questo caso, è necessario attivare Administration Server utilizzando una licenza di Kaspersky Hybrid Cloud Security.

Passaggio 3. Selezione dell'ambiente cloud e autorizzazione

Specificare le seguenti impostazioni:

- **Ambiente cloud**

  Selezionare l'ambiente cloud in cui distribuire Kaspersky Security Center Cloud Console: AWS, Azure o Google Cloud.

  Se si prevede di utilizzare più di un ambiente cloud, selezionare un ambiente ed eseguire nuovamente la procedura guidata.

- **Nome della connessione**

  Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

  Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

  Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

Immettere le credenziali per ricevere l'autorizzazione nell'ambiente cloud specificato.

AWS

Se è stato selezionato AWS come tipo di segmento cloud, utilizzare una chiave di accesso AWS IAM per eseguire ulteriormente il polling del segmento cloud. Immettere i seguenti dati chiave:

- **ID chiave di accesso**

  L'ID chiave di accesso IAM è una sequenza di caratteri alfanumerici. L'ID chiave è stato ricevuto al momento della creazione dell'account utente IAM.

  Il campo è disponibile dopo aver selezionato una chiave di accesso AWS IAM per l'autorizzazione.

- **Chiave segreta**

  Chiave segreta ricevuta con l'ID chiave di accesso al momento della creazione dell'account utente IAM.

  I caratteri della chiave segreta sono visualizzati come asterischi. Quando si inizia a immettere la chiave segreta, viene visualizzato il pulsante **Mostra**. Tenere premuto questo pulsante per visualizzare i caratteri immessi.

  Il campo è disponibile dopo aver selezionato una chiave di accesso AWS IAM per l'autorizzazione.

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

Azure

Se è stato selezionato Azure come tipo di segmento cloud, specificare le seguenti impostazioni per la connessione da utilizzare per il polling del segmento cloud:

- **ID applicazione Azure**

  L'ID applicazione è stato creato dall'utente nel portale di Azure.

  È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

- **ID sottoscrizione Azure**

  La sottoscrizione è stata creata dall'utente nel portale di Azure.

- **Password dell'applicazione Azure**

  La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

  I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

- **Nome dell'account di archiviazione di Azure**

  È stato creato il nome dell'account di archiviazione di Azure per l'account di archiviazione di Azure per l'utilizzo di Kaspersky Security Center Cloud Console.

- **Chiave di accesso all'archivio Azure**

  È stata ricevuta una password (chiave) durante la creazione dell'account di archiviazione di Azure per l'utilizzo di Kaspersky Security Center Cloud Console.

  La chiave è disponibile nella sezione "Panoramica dell'account di archiviazione di Azure", nella sottosezione "Chiavi".

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

Google Cloud

Se è stato selezionato Google Cloud come tipo di segmento cloud, specificare le seguenti impostazioni per la connessione da utilizzare per il polling del segmento cloud:

- **Indirizzo e-mail client**

  L'e-mail client è l'indirizzo e-mail utilizzato per la registrazione del progetto in Google Cloud.

- **ID progetto**

L'ID progetto è l'ID ricevuto durante la registrazione del progetto in Google Cloud.

- **Chiave privata**

  La chiave privata è la sequenza di caratteri ricevuta come chiave privata durante la registrazione del progetto in Google Cloud. È consigliabile copiare e incollare questa sequenza per evitare errori.

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

La connessione specificata viene salvata nelle impostazioni dell'applicazione.

La Configurazione guidata ambiente cloud consente di specificare un solo segmento. Successivamente è possibile specificare più connessioni per gestire altri segmenti cloud.

Fare clic su **Avanti** per continuare.

Passaggio 4. Polling dei segmenti e configurazione della sincronizzazione con il cloud

In questo passaggio viene avviato il polling dei segmenti cloud e viene automaticamente creato uno speciale gruppo di amministrazione per i dispositivi cloud. I dispositivi rilevati durante il polling vengono inseriti in questo gruppo. La pianificazione del polling dei segmenti cloud è configurata su ogni 5 minuti per impostazione predefinita (è possibile modificare questa impostazione in un secondo momento).

Viene inoltre creata una regola di spostamento automatico **Sincronizza con il cloud**. Per ogni successiva scansione della rete cloud, i dispositivi virtuali rilevati verranno spostati nel sottogruppo corrispondente all'interno del gruppo **Dispositivi gestiti\Cloud**.

Definire l'impostazione **Sincronizza gruppi di amministrazione con la struttura cloud**.

Se questa opzione è abilitata, viene creato automaticamente il gruppo **Cloud** all'interno del gruppo **Dispositivi gestiti** e viene avviata una device discovery cloud. Le istanze e le macchine virtuali rilevate durante ciascuna scansione della rete cloud sono inserite nel gruppo Cloud. La struttura dei sottogruppi di amministrazione all'interno di questo gruppo corrisponde alla struttura del segmento cloud (in AWS, le zone di disponibilità e i gruppi di collocazione non sono rappresentati nella struttura; in Azure, le subnet non sono rappresentate nella struttura). I dispositivi che non sono stati identificati come istanze nell'ambiente cloud si trovano nel gruppo **Dispositivi non assegnati**. La struttura di questo gruppo consente di utilizzare le attività di installazione di gruppo per installare le applicazioni anti-virus nelle istanze, nonché di configurare diversi criteri per diversi gruppi.

Se questa opzione è disabilitata, viene creato il gruppo **Cloud** e viene avviata una device discovery cloud, tuttavia all'interno del gruppo non vengono creati i sottogruppi che corrispondono alla struttura del segmento cloud. Tutte le istanze rilevate si trovano nel gruppo di amministrazione **Cloud**, pertanto vengono visualizzate in un unico elenco. Se l'utilizzo di Kaspersky Security Center Cloud Console richiede la sincronizzazione, è possibile modificare le proprietà della regola **Sincronizza con il cloud** e quindi applicarla. Applicando la regola viene modificata la struttura dei sottogruppi nel gruppo Cloud in modo da creare la corrispondenza con la struttura del segmento cloud.

Per impostazione predefinita, questa opzione è disabilitata.

Fare clic su **Avanti** per continuare.

Passaggio 5. Selezione di un'applicazione per la quale creare criteri e attività

Questo passaggio viene visualizzato solo se si dispone dei pacchetti di installazione e dei plug-in per Kaspersky Endpoint Security for Windows e Kaspersky Security for Windows Server. Se si dispone di un plug-in e di un pacchetto di installazione solo di una di queste applicazioni, questo passaggio viene ignorato e Kaspersky Security Center Cloud Console crea un criterio e attività per l'applicazione esistente.

Selezionare un'applicazione per cui si desidera creare un criterio e attività.

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

Passaggio 6. Configurazione di Kaspersky Security Network per Kaspersky Security Center Cloud Console

Questo passaggio viene saltato durante l'esecuzione di Kaspersky Security Center Cloud Console in modalità di prova o su un Administration Server virtuale.

Specificare le impostazioni per la trasmissione delle informazioni sulle operazioni di Kaspersky Security Center Cloud Console alla Knowledge Base di Kaspersky Security Network (KSN). Selezionare una delle seguenti opzioni:

- **Accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center Cloud Console e le applicazioni gestite installate nei dispositivi client trasferiranno automaticamente i dettagli sull'esecuzione a Kaspersky Security Network. La partecipazione a Kaspersky Security Network garantisce aggiornamenti più rapidi dei database contenenti le informazioni sui virus e sulle altre minacce, assicurando una risposta più rapida alle minacce per la sicurezza emergenti.

- **Non accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center Cloud Console e le applicazioni gestite non forniranno informazioni a Kaspersky Security Network.

  Se si seleziona questa opzione, l'utilizzo di Kaspersky Security Network sarà disabilitato.

Kaspersky consiglia la partecipazione a Kaspersky Security Network.

È inoltre possibile visualizzare i contratti KSN per le applicazioni gestite. Se si accetta di utilizzare Kaspersky Security Network, l'applicazione gestita invierà i dati a Kaspersky. Se non si accetta di partecipare a Kaspersky Security Network, l'applicazione gestita non invierà i dati a Kaspersky. È possibile modificare questa impostazione in un secondo momento nel criterio dell'applicazione.

Fare clic su **Avanti** per continuare.

Passaggio 7. Creazione di una configurazione iniziale della protezione

È possibile esaminare un elenco dei criteri e delle attività creati.

Attendere il completamento della creazione di criteri e attività, quindi fare clic su **Avanti** per procedere. Nell'ultima pagina della procedura guidata, fare clic sul pulsante **Fine** per uscire.

Polling dei segmenti di rete tramite Kaspersky Security Center Cloud Console

Le informazioni sulla struttura (e sui dispositivi) della rete vengono ricevute tramite il polling periodico dei segmenti cloud mediante gli strumenti API AWS, API Azure o API Google. Kaspersky Security Center Cloud Console utilizza queste informazioni per aggiornare il contenuto delle cartelle Dispositivi non assegnati e Dispositivi gestiti. Se i dispositivi sono stati configurati in modo da essere spostati automaticamente nei gruppi di amministrazione, i dispositivi rilevati sono inclusi nei gruppi di amministrazione.

Per consentire il polling dei segmenti cloud, è necessario disporre dei diritti corrispondenti forniti con un account utente IAM (in AWS), con un ID applicazione e una password (in Azure) o con l'e-mail client di Google, l'ID progetto di Google e una chiave privata (in Google Cloud).

È possibile aggiungere ed eliminare le connessioni, nonché configurare la pianificazione di polling per ogni segmento cloud.

Aggiunta delle connessioni per il polling dei segmenti cloud tramite Kaspersky Security Center Cloud Console

Per aggiungere una connessione per il polling dei segmenti cloud all'elenco delle connessioni disponibili:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Cloud**.
2. Nella finestra visualizzata fare clic su **Proprietà**.
3. Nella finestra **Impostazioni** visualizzata fare clic su **Aggiungi**.

   Verrà visualizzata la finestra **Impostazioni segmento cloud**.
4. Specificare il nome dell'ambiente cloud per la connessione da utilizzare per il successivo polling del segmento cloud:

   - **Ambiente cloud**

     Selezionare l'ambiente cloud in cui distribuire Kaspersky Security Center Cloud Console: AWS, Azure o Google Cloud.

     Se si prevede di utilizzare più di un ambiente cloud, selezionare un ambiente ed eseguire nuovamente la procedura guidata.

   - **Nome della connessione**

Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

5. Immettere le credenziali per ricevere l'autorizzazione nell'ambiente cloud specificato.

- Se è stato selezionato AWS, specificare quanto segue:
  - **ID chiave di accesso**

    L'ID chiave di accesso IAM è una sequenza di caratteri alfanumerici. L'ID chiave è stato ricevuto al momento della creazione dell'account utente IAM.

    Il campo è disponibile dopo aver selezionato una chiave di accesso AWS IAM per l'autorizzazione.

  - **Chiave segreta**

    Chiave segreta ricevuta con l'ID chiave di accesso al momento della creazione dell'account utente IAM.

    I caratteri della chiave segreta sono visualizzati come asterischi. Quando si inizia a immettere la chiave segreta, viene visualizzato il pulsante **Mostra**. Tenere premuto questo pulsante per visualizzare i caratteri immessi.

    Il campo è disponibile dopo aver selezionato una chiave di accesso AWS IAM per l'autorizzazione.

    Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

- Se è stato selezionato Azure, specificare le seguenti impostazioni:
  - **ID applicazione Azure**

    L'ID applicazione è stato creato dall'utente nel portale di Azure.

    È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

  - **ID sottoscrizione Azure**

    La sottoscrizione è stata creata dall'utente nel portale di Azure.

  - **Password dell'applicazione Azure**

    La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

    I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

    Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

  - **Nome dell'account di archiviazione di Azure**

È stato creato il nome dell'account di archiviazione di Azure per l'account di archiviazione di Azure per l'utilizzo di Kaspersky Security Center Cloud Console.

- **Chiave di accesso all'archivio Azure**

  È stata ricevuta una password (chiave) durante la creazione dell'account di archiviazione di Azure per l'utilizzo di Kaspersky Security Center Cloud Console.

  La chiave è disponibile nella sezione "Panoramica dell'account di archiviazione di Azure", nella sottosezione "Chiavi".

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

Se è stato selezionato Google Cloud, specificare le seguenti impostazioni:

- **Indirizzo e-mail client**

  L'e-mail client è l'indirizzo e-mail utilizzato per la registrazione del progetto in Google Cloud.

- **ID progetto**

  L'ID progetto è l'ID ricevuto durante la registrazione del progetto in Google Cloud.

- **Chiave privata**

  La chiave privata è la sequenza di caratteri ricevuta come chiave privata durante la registrazione del progetto in Google Cloud. È consigliabile copiare e incollare questa sequenza per evitare errori.

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

6. Se lo si desidera, fare clic su **Imposta pianificazione di polling** e modificare le impostazioni predefinite.

La connessione viene salvata nelle impostazioni dell'applicazione.

Dopo la prima esecuzione del polling del nuovo segmento cloud, il sottogruppo corrispondente a tale segmento viene visualizzato nel gruppo di amministrazione **Dispositivi gestiti\Cloud**.

Se si specificano credenziali errate, non verranno individuate istanze durante il polling del segmento cloud e non verrà visualizzato un nuovo sottogruppo nel gruppo di amministrazione **Dispositivi gestiti\Cloud**.

Eliminazione di una connessione per il polling dei segmenti cloud

Se non è più necessario eseguire il polling di uno specifico segmento cloud, è possibile eliminare la connessione corrispondente dall'elenco delle connessioni disponibili. È anche possibile eliminare una connessione se, ad esempio, le autorizzazioni per il polling di un segmento cloud sono state trasferite a un altro utente con credenziali diverse.

Per eliminare una connessione:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Cloud**.
2. Nella finestra visualizzata fare clic su **Proprietà**.
3. Nella finestra **Impostazioni** visualizzata fare clic sul nome del segmento che si desidera eliminare.
4. Fare clic su **Elimina**.
5. Nella finestra visualizzata fare clic sul pulsante **OK** per confermare la selezione.

La connessione viene eliminata. I dispositivi nel segmento cloud corrispondente a questa connessione vengono automaticamente eliminati dai gruppi di amministrazione.

Configurazione della pianificazione di polling tramite Kaspersky Security Center Cloud Console

Il polling dei segmenti cloud viene eseguito in base a una pianificazione. È possibile impostare la frequenza di polling.

La frequenza di polling è impostata automaticamente a 5 minuti dalla Configurazione guidata ambiente cloud. È possibile modificare il valore in qualsiasi momento e impostare una pianificazione diversa. Non è tuttavia consigliabile configurare il polling per l'esecuzione con una frequenza inferiore a 5 minuti perché potrebbero verificarsi errori nel funzionamento dell'API.

Per configurare la pianificazione del polling dei segmenti cloud:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Cloud**.
2. Nella finestra visualizzata fare clic su **Proprietà**.
3. Nella finestra **Impostazioni** visualizzata fare clic sul nome del segmento per il quale si desidera configurare una pianificazione di polling.

   Verrà visualizzata la finestra **Impostazioni segmento cloud**.
4. Nella finestra **Impostazioni segmento cloud** fare clic sul pulsante **Imposta pianificazione di polling**.

   Verrà aperta la finestra **Pianificazione**.
5. Nella finestra **Pianificazione** specificare le seguenti impostazioni:

   - **Avvio pianificato**

     Opzioni per la pianificazione di polling:

     - Ogni N giorni

       Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

       Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

     - Ogni N minuti

Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

Per impostazione predefinita, il polling viene eseguito ogni 5 minuti, a partire dall'ora di sistema corrente.

- In base ai giorni della settimana

  Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, il polling viene eseguito ogni venerdì alle 18:00:00.

- Ogni mese nei giorni specificati delle settimane selezionate

  Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è 18:00:00.

- Intervallo di avvio (giorni)

  Specificare a cosa equivale N (per minuti o giorni).

- A partire da

  Specificare quando avviare il primo polling.

- Esegui attività non effettuate

  Se l'area di lavoro non è disponibile nel momento in cui è pianificato il polling, Kaspersky Security Center Cloud Console può avviare il polling subito dopo che l'area di lavoro torna a essere disponibile o attendere la successiva pianificazione del polling.

  Se questa opzione è abilitata, Kaspersky Security Center Cloud Console avvia il polling subito dopo che l'area di lavoro torna a essere disponibile.

  Se questa opzione è disabilitata, Kaspersky Security Center Cloud Console attende la successiva pianificazione del polling.

  Per impostazione predefinita, questa opzione è abilitata.

6. Fare clic su **Salva** per salvare le modifiche.

La pianificazione di polling per il segmento verrà configurata e salvata.

Visualizzazione dei risultati del polling dei segmenti cloud tramite Kaspersky Security Center Cloud Console

È possibile visualizzare i risultati del polling dei segmenti cloud, ovvero visualizzare l'elenco dei dispositivi cloud gestiti da Administration Server.

Per visualizzare i risultati del polling dei segmenti cloud,

Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Cloud**.

Vengono visualizzati i segmenti cloud disponibili per il polling.

Visualizzazione delle proprietà dei dispositivi cloud tramite Kaspersky Security Center Cloud Console

È possibile visualizzare le proprietà di ciascun dispositivo cloud.

Per visualizzare le proprietà di un dispositivo cloud:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo di cui si desidera visualizzare le proprietà.

   Verrà visualizzata una finestra delle proprietà con la sezione **Generale** selezionata.
3. Se si desidera visualizzare le proprietà specifiche per i dispositivi cloud, selezionare la sezione **Sistema** nella finestra delle proprietà.

   Le proprietà vengono visualizzate in base alla piattaforma cloud del dispositivo.

   Per i dispositivi in AWS, vengono visualizzate le seguenti proprietà:

   - **Dispositivo rilevato tramite API** (valore: **AWS**)
   - **Regione cloud**
   - **VPC cloud**
   - **Zona di disponibilità cloud**
   - **Sottorete cloud**
   - **Gruppo di collocazione Cloud** (questa unità viene visualizzata solo se l'istanza appartiene a un gruppo di collocazione; in caso contrario, non viene visualizzata)

   Per i dispositivi in Azure, vengono visualizzate le seguenti proprietà:

   - **Dispositivo rilevato tramite API** (valore: **Microsoft Azure**)
   - **Regione cloud**
   - **Sottorete cloud**

   Per i dispositivi in Google Cloud, vengono visualizzate le seguenti proprietà:

   - **Dispositivo rilevato tramite API** (valore: **Google Cloud**)
   - **Regione cloud**
   - **VPC cloud**

- **Zona di disponibilità cloud**
- **Sottorete cloud**

Sincronizzazione con il cloud: configurazione della regola di spostamento

Durante l'esecuzione della Configurazione guidata ambiente cloud, viene automaticamente creata la regola Sincronizza con il cloud. La regola consente di spostare automaticamente i dispositivi rilevati in ogni polling dal gruppo Dispositivi non assegnati al gruppo Dispositivi gestiti\Cloud per rendere disponibili tali dispositivi per la gestione centralizzata. Per impostazione predefinita, la regola è attiva dopo la creazione. È possibile disabilitare, modificare o applicare la regola in qualsiasi momento.

Per modificare le proprietà della regola Sincronizza con il cloud e/o applicare la regola:

1. Nel menu principale accedere a **Individuazione e distribuzione → Distribuzione e assegnazione → Regole di spostamento**.

   Verrà visualizzato un elenco delle regole di spostamento.

2. Nell'elenco delle regole di spostamento selezionare **Sincronizza con il cloud**.

   Verrà visualizzata la finestra delle proprietà della regola.

3. Se necessario, specificare le seguenti impostazioni nella scheda **Condizioni delle regole**, nella scheda **Segmenti cloud**:

   - **Il dispositivo si trova in un segmento cloud**

     La regola viene applicata solo ai dispositivi inclusi nel segmento cloud selezionato. In caso contrario, la regola viene applicata a tutti i dispositivi individuati.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Includi gli oggetti figlio**

     La regola viene applicata a tutti i dispositivi nel segmento selezionato e in tutte le sottosezioni cloud nidificate. In caso contrario, la regola viene applicata solo ai dispositivi inclusi nel segmento radice.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Sposta i dispositivi dagli oggetti nidificati nei sottogruppi corrispondenti**

     Se questa opzione è abilitata, i dispositivi vengono spostati automaticamente dagli oggetti nidificati ai sottogruppi corrispondenti alla relativa struttura.

     Se questa opzione è disabilitata, i dispositivi vengono spostati automaticamente dagli oggetti nidificati alla radice del sottogruppo Cloud senza ulteriori ramificazioni.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati**

Se questa opzione è abilitata, quando la struttura del gruppo **Dispositivi gestiti\Cloud** non ha sottogruppi corrispondenti alla sezione che contiene il dispositivo, Kaspersky Security Center Cloud Console crea tali sottogruppi. Ad esempio, se viene rilevata una nuova subnet durante la device discovery, verrà creato un nuovo gruppo con lo stesso nome nel gruppo **Dispositivi gestiti\Cloud**.

Se questa opzione è disabilitata, Kaspersky Security Center Cloud Console non crea nuovi sottogruppi. Ad esempio, se viene rilevata una nuova subnet durante il polling della rete, non verrà creato un nuovo gruppo con lo stesso nome nel gruppo **Dispositivi gestiti\Cloud** e i dispositivi presenti nella subnet verranno spostati nel gruppo **Dispositivi gestiti\Cloud**.

Per impostazione predefinita, questa opzione è abilitata.

- **Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud**

  Se questa opzione è abilitata, l'applicazione elimina dal gruppo Cloud tutti i sottogruppi a cui non corrisponde alcun oggetto cloud esistente.

  Se questa opzione è disabilitata, vengono mantenuti i sottogruppi a cui non corrisponde alcun oggetto cloud esistente.

  Per impostazione predefinita, questa opzione è abilitata.

Se è stata abilitata l'opzione **Sincronizza gruppi di amministrazione con la struttura cloud** durante l'utilizzo della Configurazione guidata ambiente cloud, la regola **Sincronizza con il cloud** viene creata con le opzioni **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati** e **Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud** abilitate.

Se non è stata abilitata l'opzione **Sincronizza gruppi di amministrazione con la struttura cloud**, la regola **Sincronizza con il cloud** viene creata con queste opzioni disabilitate (deselezionate). Se l'utilizzo di Kaspersky Security Center Cloud Console richiede che la struttura dei sottogruppi nel sottogruppo di **Dispositivi gestiti\Cloud** corrisponda alla struttura dei segmenti cloud, selezionare le caselle di controllo **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati** ed **Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud** nelle proprietà della regola e quindi applicare la regola.

4. Nell'elenco a discesa **Dispositivo rilevato tramite l'API** selezionare uno dei seguenti valori:

   - **No**. Il dispositivo non può essere rilevato tramite l'API AWS, Azure o Google, ad esempio perché si trova all'esterno dell'ambiente cloud oppure si trova nell'ambiente cloud ma non può essere rilevato tramite un'API per qualche motivo.
   - **AWS**. Il dispositivo viene rilevato tramite l'API AWS, quindi si trova senz'altro nell'ambiente cloud AWS.
   - **Azure**. Il dispositivo viene rilevato tramite l'API Azure, quindi si trova senz'altro nell'ambiente cloud Azure.
   - **Google Cloud**. Il dispositivo viene rilevato tramite l'API Google, quindi si trova senz'altro nell'ambiente cloud Google.
   - Nessun valore. Il criterio non può essere applicato.

5. Se necessario, configurare le proprietà delle altre regole nelle altre sezioni.

Verrà configurata la regola di spostamento.

Installazione remota delle applicazioni nelle macchine virtuali Azure

È necessario disporre di una licenza valida per installare le applicazioni nelle macchine virtuali di Microsoft Azure.

Kaspersky Security Center Cloud Console supporta i seguenti scenari:

- Un dispositivo client viene rilevato tramite l'API Azure; anche l'installazione viene eseguita tramite un'API. L'utilizzo dell'API di Azure indica che è possibile installare solo le seguenti applicazioni:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- Un dispositivo client viene rilevato tramite l'API Azure; l'installazione viene eseguita tramite un punto di distribuzione o, se non sono presenti punti di distribuzione, manualmente, utilizzando pacchetti di installazione indipendenti. È possibile installare qualsiasi applicazione supportata da Kaspersky Security Center Cloud Console in questo modo.

Per creare un'attività per l'installazione remota dell'applicazione nelle macchine virtuali Azure:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Seguire le istruzioni della procedura guidata:
   a. Selezionare **Installa l'applicazione in remoto** come tipo di attività.
   b. Nella pagina **Pacchetti di installazione**, selezionare **Installazione remota eseguita da Microsoft Azure API**.
   c. Quando si seleziona l'account per accedere ai dispositivi, utilizzare un account Azure esistente o fare clic su **Aggiungi** e inserire le credenziali dell'account Azure:
      - Nome account Azure

        Inserire un nome per le credenziali specificate. Questo nome verrà visualizzato nell'elenco degli account per l'esecuzione dell'attività.
      - ID applicazione Azure

        L'ID applicazione è stato creato dall'utente nel portale di Azure.

        È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.
      - Password dell'applicazione Azure

        La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

        I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.
   d. Selezionare i dispositivi interessati nel gruppo **Dispositivi gestiti\Cloud**.

Al termine della procedura guidata, l'attività di installazione remota dell'applicazione viene visualizzata nell'elenco delle attività.

Modifica della lingua dell'interfaccia di Kaspersky Security Center Cloud Console

È possibile selezionare la lingua dell'interfaccia di Kaspersky Security Center Cloud Console.

Per modificare la lingua dell'interfaccia:

1. Nel menu principale, passare a **Impostazioni** → **Lingua**.
2. Selezionare una delle lingue di localizzazione supportate.

Contatta Assistenza tecnica

Questa sezione descrive i modi e le condizioni per ottenere assistenza tecnica.

Come ottenere assistenza tecnica

Se non è possibile trovare una soluzione per il proprio problema nella documentazione di Kaspersky Security Center Cloud Console o in una delle fonti di informazioni su Kaspersky Security Center Cloud Console, contattare l'Assistenza tecnica di Kaspersky. Gli specialisti del Servizio di assistenza tecnica risponderanno a tutte le domande relative all'installazione e all'utilizzo di Kaspersky Security Center Cloud Console.

Kaspersky garantisce il supporto di Kaspersky Security Center Cloud Console durante il ciclo di vita (vedere la pagina del ciclo di vita di supporto del prodotto). Prima di contattare il Servizio di assistenza tecnica, consultare le regole dell'assistenza.

È possibile contattare il Servizio di assistenza tecnica in uno dei seguenti modi:

- Visitando il sito Web del Servizio di assistenza tecnica
- Inviando una richiesta al Servizio di assistenza tecnica dal portale Kaspersky CompanyAccount

Assistenza tecnica tramite Kaspersky CompanyAccount

Kaspersky CompanyAccount è un portale per le aziende che utilizzano le applicazioni Kaspersky. Il portale Kaspersky CompanyAccount è progettato per facilitare l'interazione tra gli utenti e gli esperti di Kaspersky tramite richieste online. È possibile utilizzare Kaspersky CompanyAccount per tenere traccia dello stato delle proprie richieste online e visualizzarne la cronologia.

È possibile registrare tutti i dipendenti dell'organizzazione in un singolo account su Kaspersky CompanyAccount. Un singolo account consente di gestire in modo centralizzato le richieste online inviate a Kaspersky dai dipendenti registrati e di gestire i privilegi dei 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 del Servizio di assistenza tecnica.

Informazioni richieste per gli specialisti del Servizio di assistenza tecnica di Kaspersky

Quando si contattano gli specialisti del Servizio di assistenza tecnica di Kaspersky, potrebbe essere richiesto di fornire le seguenti informazioni:

- Informazioni generali su Kaspersky Security Center Cloud Console
- ID area di lavoro
- Informazioni sulla licenza
- Numero di applicazioni installate
- ID e stato del tenant

Queste informazioni sono disponibili nella sezione **Your account menu** → **Servizio di assistenza tecnica**. Copiare e condividere queste informazioni per ottenere assistenza in merito al problema.

Fonti di informazioni sull'applicazione

Pagina di Kaspersky Security Center Cloud Console nel sito Web di Kaspersky

Nella pagina di Kaspersky Security Center Cloud Console nel sito Web di Kaspersky, sono disponibili informazioni generali sull'applicazione e le relative funzionalità e caratteristiche.

Pagina di Kaspersky Security Center Cloud Console nella Knowledge Base

La *Knowledge Base* è una sezione del sito Web del Servizio di assistenza tecnica di Kaspersky.

Nella pagina di Kaspersky Security Center Cloud Console nella Knowledge Base, è possibile leggere articoli che forniscono informazioni utili, raccomandazioni e risposte alle domande frequenti su come acquistare, installare e utilizzare l'applicazione.

Gli articoli nella Knowledge Base possono fornire risposte a domande relative sia a Kaspersky Security Center Cloud Console che ad altre applicazioni Kaspersky. Gli articoli nella Knowledge Base possono anche contenere notizie dal Servizio di assistenza tecnica.

Discutere delle applicazioni Kaspersky con la community

Se la domanda non richiede una risposta immediata, è possibile sottoporla agli esperti di Kaspersky e ad altri utenti nel nostro forum.

Nel forum, è possibile visualizzare gli argomenti di discussione, pubblicare i propri commenti e creare nuovi argomenti di discussione.

Per accedere alle risorse del sito Web, è necessaria una connessione a Internet.

Se non è possibile trovare una soluzione al problema, contattare il Servizio di assistenza tecnica.

Problemi noti

Kaspersky Security Center Cloud Console presenta una serie di limitazioni non critiche per il funzionamento dell'applicazione:

- Quando si importa l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* o *Aggiorna verifica*, l'opzione **Selezionare i dispositivi a cui assegnare l'attività** è abilitata. Queste attività non possono essere assegnate a una selezione di dispositivi o a dispositivi specifici. Se si assegna l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* o *Aggiorna verifica* a dispositivi specifici, l'attività verrà importata in modo errato.

- Al termine dell'attività di *scansione dell'inventario* per un dispositivo Linux, un tentativo di inviare i file ricevuti a Kaspersky per l'analisi restituisce un errore.

- Se si tenta di accedere a Kaspersky Security Center Cloud Console utilizzando Active Directory Federation Services (ADFS), ma mancano le autorizzazioni necessarie, Kaspersky Security Center Cloud Console restituisce comunque l'errore "Credenziali non valide" invece di avvisare l'utente delle autorizzazioni mancanti.

- L'attività Gestisci dispositivi non funziona correttamente per i dispositivi che eseguono macOS.

- Se nella finestra Diagnostica remota si fa clic sul pulsante **Scarica l'intero file**, il download potrebbe non essere eseguito correttamente.

Glossario

Account in Kaspersky Security Center Cloud Console

Account utente necessario per configurare Kaspersky Security Center Cloud Console, ad esempio aggiungendo e rimuovendo account utente e configurando i profili di protezione (criteri di protezione). Questo account utente consente di utilizzare il servizio My Kaspersky. Questo account viene creato quando si inizia a utilizzare Kaspersky Security Center Cloud Console.

Administration Server

Un componente di Kaspersky Security Center Cloud Console che archivia in modo centralizzato le informazioni su tutte le applicazioni Kaspersky installate nella rete aziendale. È inoltre possibile utilizzarlo per la gestione di tali applicazioni.

Administration Server principale

Per Administration Server principale si intende l'Administration Server che è stato specificato durante l'installazione di Network Agent. L'Administration Server principale può essere utilizzato nelle impostazioni dei profili di connessione di Network Agent.

Administration Server virtuale

Componente di Kaspersky Security Center Cloud Console progettato per la gestione del sistema di protezione della rete di un'organizzazione client.

Un Administration Server virtuale è un particolare tipo di Administration Server secondario e presenta le seguenti limitazioni rispetto a un Administration Server fisico:

- Gli Administration Server virtuali possono funzionare solo come Administration Server secondari.
- L'Administration Server virtuale non supporta la creazione di Administration Server secondari (inclusi server virtuali).

Agente di Autenticazione

Interfaccia che consente di completare l'autenticazione per l'accesso ai dischi rigidi criptati e il caricamento del sistema operativo dopo il criptaggio del disco rigido avviabile.

Aggiorna

Procedura di sostituzione o aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky.

Aggiornamento disponibile

Un set di aggiornamenti per i moduli dell'applicazione Kaspersky, inclusi gli aggiornamenti critici accumulati in un determinato periodo di tempo.

Amazon Machine Image (AMI)

Modello contenente la configurazione software necessaria per eseguire la macchina virtuale. È possibile creare più istanze in base a una singola AMI.

Amministratore di Kaspersky Security Center Cloud Console

La persona che gestisce le operazioni dell'applicazione tramite il sistema centralizzato di amministrazione remota Kaspersky Security Center Cloud Console.

API (Application Programming Interface) AWS

L'API della piattaforma AWS utilizzata da Kaspersky Security Center Cloud Console. In particolare, gli strumenti API AWS vengono utilizzati per il polling dei segmenti cloud.

Applicazione incompatibile

Un'applicazione anti-virus di uno sviluppatore di terze parti o un'applicazione Kaspersky che non supporta la gestione tramite Kaspersky Security Center Cloud Console.

Archivio eventi

Una parte del database di Administration Server dedicato all'archiviazione delle informazioni sugli eventi che si verificano in Kaspersky Security Center Cloud Console.

Area di lavoro

Un'istanza di Kaspersky Security Center Cloud Console creata per un'azienda specifica. Quando un cliente crea un'area di lavoro, Kaspersky crea e configura l'infrastruttura e l'Administration Console basata sul cloud che devono gestire le applicazioni di protezione installate nei dispositivi dell'azienda.

Attività

Le funzioni eseguite dall'applicazione Kaspersky sono implementate come attività, ad esempio Protezione in tempo reale, Scansione completa del computer e Aggiornamento database.

Attività di gruppo

Un'attività definita per un gruppo di amministrazione ed eseguita in tutti i dispositivi client inclusi nel gruppo di amministrazione.

Attività locale

Attività definita e in esecuzione in un singolo computer client.

Attività per dispositivi specifici

Attività assegnata a un set di dispositivi client appartenenti a gruppi di amministrazione arbitrari ed eseguita su tali dispositivi.

Chiave attiva

Chiave attualmente utilizzata dall'applicazione.

Chiave di abbonamento aggiuntiva

Una chiave che convalida il diritto di utilizzo dell'applicazione, ma non è attualmente utilizzata.

Chiave di accesso AWS IAM

Una combinazione che comprende l'ID della chiave (con un aspetto simile a "AKIAIOSFODNN7EXAMPLE") e la chiave segreta (con un aspetto simile a "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Questa coppia appartiene all'utente IAM e viene utilizzata per ottenere l'accesso ai servizi AWS.

Console di gestione AWS

Interfaccia Web per la visualizzazione e la gestione delle risorse AWS. La console di gestione AWS è disponibile sul Web all'indirizzo https://aws.amazon.com/it/console/

Criterio

Un criterio determina le impostazioni di un'applicazione e gestisce la capacità di configurare tale applicazione nei computer all'interno di un gruppo di amministrazione. Per ogni applicazione è necessario creare un criterio individuale. È possibile creare più criteri per le applicazioni installate nei computer di ciascun gruppo di amministrazione, ma a ogni applicazione è possibile applicare un solo criterio per volta all'interno di un gruppo di amministrazione.

Database anti-virus

Database che contengono informazioni sulle minacce per la protezione del computer note a Kaspersky al momento del rilascio dei database anti-virus. Le voci contenute nei database anti-virus consentono il rilevamento del codice dannoso negli oggetti esaminati. I database anti-virus sono creati dagli specialisti di Kaspersky e vengono aggiornati ogni ora.

Dispositivo di protezione UEFI

Dispositivo in cui Kaspersky Anti-Virus for UEFI è integrato al livello BIOS. La protezione integrata garantisce la sicurezza del dispositivo fin dall'avvio del sistema, mentre la protezione nei dispositivi senza software integrato inizia solo dopo l'avvio dell'applicazione di protezione.

Dispositivo gestito

Un computer in cui è installato Network Agent o un dispositivo mobile in cui è installata un'applicazione di protezione Kaspersky.

Dominio di trasmissione

Un'area logica di una rete in cui tutti i nodi possono scambiare dati utilizzando un canale di trasmissione al livello OSI (Open Systems Interconnection Basic Reference Model).

Epidemia di virus

Una serie di tentativi intenzionali di infettare un dispositivo con un virus.

File chiave

Un file nel formato xxxxxxxx.key che consente l'utilizzo di un'applicazione Kaspersky in base ai termini della licenza commerciale o di prova.

Finestra Kaspersky Security Network (KSN)

Un'infrastruttura di servizi cloud che consente di accedere al database di Kaspersky, con informazioni sempre aggiornate sulla reputazione di file, risorse Web e software. Kaspersky Security Network assicura una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora l'efficacia di alcuni componenti della protezione e riduce la probabilità di falsi positivi.

Gateway di connessione

Un *gateway di connessione* è un Network Agent che funziona in modalità speciale. Un gateway di connessione accetta le connessioni da altri Network Agent e le trasmette ad Administration Server tramite la propria connessione con il server. A differenza di un normale Network Agent, un gateway di connessione attende le connessioni da Administration Server anziché stabilire connessioni ad Administration Server.

Gestione centralizzata delle applicazioni

Gestione remota delle applicazioni tramite i servizi di amministrazione forniti da Kaspersky Security Center Cloud Console.

Gestione diretta delle applicazioni

Gestione applicazioni tramite un'interfaccia locale.

Gravità di un evento

Una proprietà di un evento verificatosi durante l'esecuzione di un'applicazione Kaspersky. Esistono i seguenti livelli di criticità:

- Evento critico
- Errore funzionale
- Avviso
- Informazioni

Eventi dello stesso tipo possono avere diversi livelli di criticità, a seconda della situazione in cui si è verificato l'evento.

Gruppo di amministrazione

Un set di dispositivi raggruppati in base alla funzione e alle applicazioni Kaspersky installate. I dispositivi sono raggruppati come una singola entità per semplificare la gestione. Un gruppo può includere altri gruppi. È possibile creare criteri di gruppo e attività di gruppo per ogni applicazione installata nel gruppo.

HTTPS

Protocollo sicuro per il trasferimento dei dati tramite criptaggio tra un browser e un server Web. HTTPS viene utilizzato per ottenere l'accesso a informazioni con restrizioni, quali dati aziendali o finanziari.

IAM (Identity and Access Management)

Il servizio AWS che consente la gestione dell'accesso degli utenti ad altri servizi e risorse AWS.

Impostazioni attività

Impostazioni dell'applicazione specifiche per ogni tipo di attività.

Impostazioni del programma

Impostazioni dell'applicazione comuni a tutti i tipi di attività e che determinano il funzionamento generale dell'applicazione, ad esempio: impostazioni relative alle prestazioni dell'applicazione, impostazioni dei rapporti e impostazioni di backup.

Installazione forzata

Metodo per l'installazione remota delle applicazioni Kaspersky che consente di installare il software in dispositivi client specifici. Per la corretta esecuzione dell'installazione forzata, l'account utilizzato per l'attività deve disporre di diritti sufficienti per l'avvio remoto delle applicazioni nei dispositivi client. Questo metodo è consigliato per l'installazione delle applicazioni nei dispositivi che eseguono i sistemi operativi Microsoft Windows e supportano questa funzionalità.

Installazione locale

Installazione di un'applicazione di protezione in un dispositivo di una rete aziendale che presuppone l'avvio manuale dell'installazione dal pacchetto di distribuzione dell'applicazione di protezione o l'avvio manuale di un pacchetto di installazione pubblicato che è stato scaricato preventivamente nel dispositivo.

Installazione remota

Installazione delle applicazioni Kaspersky utilizzando i servizi offerti da Kaspersky Security Center Cloud Console.

Istanza di Amazon EC2

Una macchina virtuale creata in base a un'immagine AMI utilizzando Amazon Web Services.

JavaScript

Linguaggio di programmazione che estende le prestazioni delle pagine Web. Le pagine Web create tramite JavaScript possono eseguire funzioni (ad esempio, modificare la visualizzazione di elementi di interfaccia o aprire ulteriori finestre) senza aggiornare la pagina Web con nuovi dati dal server Web. Per visualizzare le pagine create utilizzando JavaScript, abilitare il supporto per JavaScript nella configurazione del browser.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network è una soluzione che consente agli utenti dei dispositivi in cui sono installate le applicazioni Kaspersky di accedere ai database di reputazione di Kaspersky Security Network e ad altri dati statistici senza inviare dati dai propri dispositivi a Kaspersky Security Network. Kaspersky Private Security Network è progettato per i clienti aziendali che non sono in grado di partecipare al programma Kaspersky Security Network per uno dei seguenti motivi:

- I dispositivi non sono connessi a Internet.
- La trasmissione dei dati all'esterno del paese o della rete LAN aziendale è vietata dalla legge o dai criteri di protezione aziendali.

Livello di importanza patch

Attributo della patch. Esistono cinque livelli di importanza per le patch di Microsoft e di terze parti:

- Critico
- Alto
- Medio
- Basso
- Sconosciuto

Il livello di importanza di una patch di Microsoft o di terze parti è determinato in base al livello di criticità meno favorevole tra le vulnerabilità che le patch dovrebbero correggere.

Network Agent

Un componente di Kaspersky Security Center Cloud Console che consente l'interazione tra Administration Server e le applicazioni Kaspersky installate in un nodo di rete specifico (workstation o server). Questo componente è comune a tutte le applicazioni dell'azienda per Microsoft® Windows®. Esistono versioni distinte di Network Agent per le applicazioni Kaspersky sviluppate per i sistemi operativi Unix e macOS.

Operatore di Kaspersky Security Center Cloud Console

Utente che monitora lo stato e l'esecuzione di un sistema di protezione gestito tramite Kaspersky Security Center Cloud Console.

Pacchetto di installazione

Un set di file creati per l'installazione remota di un'applicazione Kaspersky tramite il sistema di amministrazione remota Kaspersky Security Center Cloud Console. Il pacchetto di installazione contiene numerose impostazioni necessarie per installare l'applicazione e renderla operativa subito dopo l'installazione. Le impostazioni corrispondono alle impostazioni predefinite dell'applicazione. Il pacchetto di installazione viene creato utilizzando i file con le estensioni kpd e kud inclusi nel kit di distribuzione dell'applicazione.

Periodo licenza

Il periodo di tempo durante il quale l'utente ha accesso alle funzionalità dell'applicazione e dispone dei diritti necessari per utilizzare i servizi aggiuntivi. I servizi che possono essere utilizzati dipendono dal tipo di licenza.

Plug-in Web di gestione

Un componente speciale viene utilizzato per l'amministrazione remota del software Kaspersky tramite Kaspersky Security Center Cloud Console. Il plug-in di gestione è un'interfaccia tra Kaspersky Security Center Cloud Console e un'applicazione Kaspersky specifica. Con un plug-in di gestione è possibile configurare le attività e i criteri per l'applicazione.

Profilo criterio

Un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita condizione di attivazione del profilo.

Proprietario dispositivo

Il proprietario del dispositivo è un utente che l'amministratore può contattare quando si rende necessario eseguire determinate operazioni con un dispositivo client.

Protezione anti-virus della rete

Set di misure tecniche e organizzative che riducono il rischio di penetrazione di virus e spam nella rete di un'organizzazione, oltre a impedire attacchi di rete, phishing e altre minacce. La sicurezza di rete aumenta quando si utilizzano applicazioni e servizi di protezione e quando si applicano e si rispettano i criteri di protezione dei dati aziendali.

Punto di distribuzione

Computer in cui è installato Network Agent e che viene utilizzato per la distribuzione di aggiornamenti, il polling della rete, l'installazione remota di applicazioni, il recupero di informazioni sui computer in un gruppo di amministrazione e/o la trasmissione in un dominio. L'amministratore seleziona i dispositivi appropriati e assegna manualmente i punti di distribuzione.

Quarantena

Un archivio speciale per i file potenzialmente infetti da virus e per i file che non è possibile disinfettare al momento del rilevamento.

Rete perimetrale (DMZ)

La rete perimetrale è un segmento di una rete locale in cui sono contenuti i server che risponde alle richieste del Web globale. Per garantire la protezione della rete locale di un'organizzazione, l'accesso alla LAN dalla rete perimetrale è protetto tramite firewall.

Ripristino

Riposizionamento dell'oggetto originale dalle cartelle Quarantena o Backup nella cartella originale in cui era memorizzato prima di essere messo in quarantena, disinfettato o eliminato, oppure in una cartella definita dall'utente.

Ruolo IAM

Set di diritti per effettuare le richieste ai servizi basati su AWS. I ruoli IAM non sono associati a un utente o a un gruppo specifico; forniscono diritti di accesso senza le chiavi di accesso AWS IAM. È possibile assegnare un ruolo IAM agli utenti IAM, alle istanze EC2 e ai servizi o alle applicazioni basate su AWS.

Server degli aggiornamenti Kaspersky

I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.

Soglia di attività virus

Numero massimo di eventi del tipo specificato consentiti in un determinato periodo di tempo; il superamento di questo numero viene interpretato come un aumento dell'attività dei virus e una minaccia di un attacco di un virus. Questa funzionalità è importante quando si verificano epidemie di virus, dal momento che consente agli amministratori di rispondere tempestivamente alle minacce associate agli attacchi dei virus.

SSL

Protocollo di criptaggio dei dati utilizzato per Internet e le reti locali. Secure Sockets Layer (SSL) viene utilizzato nelle applicazioni Web per creare una connessione protetta tra un client e un server.

Stato di protezione della rete

Stato di protezione corrente, che definisce la sicurezza dei dispositivi della rete aziendale. Lo stato di protezione della rete include fattori come le applicazioni di protezione installate, l'utilizzo delle chiavi di licenza e il numero e i tipi di minacce rilevate.

Stato protezione

Stato corrente della protezione, che riflette il livello di protezione del computer.

Tag applicazione

Un'etichetta di applicazioni di terze parti che può essere utilizzata per raggruppare o cercare le applicazioni. Un tag assegnato alle applicazioni può essere utilizzato come condizione nelle selezioni dispositivi.

Tag dispositivo

Un'etichetta di un dispositivo che può essere utilizzata per raggruppare, descrivere o cercare i dispositivi.

Utente IAM

L'utente dei servizi AWS. Un utente IAM può disporre dei diritti per eseguire il polling dei segmenti cloud.

Vulnerabilità

Una vulnerabilità di un sistema operativo o un'applicazione che può essere utilizzata dagli sviluppatori di malware per penetrare nel sistema operativo o nell'applicazione e violarne l'integrità. La presenza di un numero elevato di vulnerabilità rende un sistema operativo inaffidabile, dal momento che i virus penetrati possono causare interruzioni del sistema operativo stesso e delle applicazioni installate.

Informazioni sul codice di terze parti

Le informazioni sul codice di terze parti sono contenute nel file denominato legal_notices.txt.

Il file legal_notices.txt si trova anche nella cartella di installazione di Network Agent per Windows e Network Agent per Linux.

Per ulteriori informazioni sul codice di terze parti utilizzato per le aree di lavoro, fare riferimento alla documentazione Kaspersky Endpoint Security Cloud.

Note relative ai marchi registrati

I marchi registrati e i marchi di servizi sono di proprietà dei rispettivi titolari.

Adobe, Acrobat, Flash, PostScript, Reader, Shockwave sono marchi o marchi registrati di Adobe negli Stati Uniti e/o in altri paesi.

AMD64 è un marchio o marchio registrato di Advanced Micro Devices, Inc.

Amazon, Amazon EC2, Amazon Web Services, AWS e AWS Marketplace sono marchi registrati di Amazon.com, Inc. o delle relative consociate.

Apache è un marchio registrato o un marchio di Apache Software Foundation.

Apple, App Store, AppleScript, FileVault, iPhone, iTunes, Mac, Mac OS, macOS, OS X, Safari e QuickTime sono marchi di Apple Inc.

Arm è un marchio registrato di Arm Limited (o delle sue filiali) negli Stati Uniti e/o altrove.

La parola, il marchio e i logo Bluetooth sono di proprietà di Bluetooth SIG, Inc.

Ubuntu, LTS sono marchi registrati di Canonical Ltd.

Cisco, IOS, Cisco Jabber sono marchi o marchi registrati di Cisco Systems, Inc. e/o delle relative consociate negli Stati Uniti e in altri paesi.

Citrix e XenServer sono marchi di Citrix Systems, Inc. e/o una o più delle relative filiali e possono essere registrati presso lo United States Patent and Trademark Office e in altri paesi.

Cloudflare, il logo Cloudflare e Cloudflare Workers sono marchi e/o marchi registrati di Cloudflare, Inc. negli Stati Uniti e in altre giurisdizioni.

Corel, and CorelDRAW sono marchi o marchi registrati di Corel Corporation e/o delle relative filiali in Canada, negli Stati Uniti e/o in altri paesi.

Dropbox è un marchio di Dropbox, Inc.

Radmin è un marchio registrato di Famatech.

Firebird è un marchio registrato di Firebird Foundation.

Foxit è un marchio registrato di Foxit Corporation.

FreeBSD è un marchio registrato di The FreeBSD Foundation.

Google, Android, Chrome, Dalvik, Firebase, Google Chrome, Google Earth, Google Maps, Google Play, Google Public DNS sono marchi di Google LLC.

EulerOS è un marchio di Huawei Technologies Co., Ltd.

Intel, Core sono marchi di Intel Corporation negli Stati Uniti e / o in altri paesi.

IBM, QRadar sono marchi di International Business Machines Corporation, registrati presso diverse giurisdizioni a livello mondiale.

Node.js è un marchio di Joyent, Inc.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e in altri paesi.

Logitech è un marchio o un marchio registrato di Logitech negli Stati Uniti e in altri paesi.

Microsoft, Active Directory, ActiveSync, ActiveX, BitLocker, Excel, Hyper-V, InfoPath, Internet Explorer, Microsoft Edge, MS-DOS, MultiPoint, Office 365, OneNote, Outlook, PowerPoint, PowerShell, Segoe, Skype, SQL Server, Tahoma, Visio, Win32, Windows, Windows Azure, Windows Media, Windows Mobile, Windows Phone, Windows Server e Windows Vista sono marchi del gruppo di società Microsoft.

CVE è un marchio registrato di The MITRE Corporation.

Mozilla, Firefox, Thunderbird sono marchi di Mozilla Foundation negli Stati Uniti e in altri paesi.

Novell è un marchio registrato di Novell Enterprises Inc. negli Stati Uniti e in altri paesi.

NetWare è un marchio registrato di Novell Inc. negli Stati Uniti e in altri paesi.

Oracle, Java, JavaScript sono marchi registrati di Oracle e/o delle relative consociate.

Parallels, il logo Parallels e Coherence sono marchi o marchi registrati di Parallels International GmbH.

Python è un marchio o un marchio registrato di Python Software Foundation.

Red Hat, Red Hat Enterprise Linux, CentOS, Fedora sono marchi o marchi registrati di Red Hat, Inc. o delle relative consociate negli Stati Uniti e in altri paesi.

Il marchio BlackBerry è di proprietà di Research In Motion Limited ed è registrato negli Stati Uniti e potrebbe essere registrato o in attesa di registrazione in altri paesi.

SAMSUNG è un marchio di SAMSUNG negli Stati Uniti e in altri paesi.

Debian è un marchio registrato di Software in the Public Interest, Inc.

Splunk è un marchio e un marchio registrato di Splunk Inc. negli Stati Uniti e in altri paesi.

SUSE è un marchio registrato di SUSE LLC negli Stati Uniti e in altri paesi.

Symbian è un marchio registrato di proprietà di Symbian Foundation Ltd.

VMware, VMware vSphere, VMware Workstation sono marchi o marchi registrati di VMware, Inc. negli Stati Uniti e/o in altre giurisdizioni.

UNIX è un marchio registrato negli Stati Uniti e in altri paesi, concesso in licenza in esclusiva tramite X/Open Company Limited.