kaspersky

Kaspersky Managed Detection and Response

Sommario

Guida di Kaspersky Managed Detection and Response

Novità

Informazioni su Kaspersky Managed Detection and Response

- Principio operativo di Kaspersky Managed Detection and Response
- Informazioni sulle origini dei dati
- Aree di responsabilità
- Informazioni sul Contratto di MDR
- Informazioni sull'Accordo di elaborazione dei dati

Requisiti hardware e software

Architettura di Kaspersky Managed Detection and Response

Interfacce di Kaspersky Managed Detection and Response

- Sezione MDR in Kaspersky Security Center
  - Configurazione del plug-in MDR in Kaspersky Security Center
    - Configurazione del plug-in MDR
    - Impostazione dei diritti di accesso in Kaspersky Security Center
    - Visualizzazione e modifica delle impostazioni MDR in Kaspersky Security Center
    - Utilizzo delle funzionalità del plug-in MDR in un Administration Server virtuale
    - Utilizzo delle funzionalità MDR in Kaspersky Security Center tramite un server proxy
    - Modifica dei certificati per l'utilizzo delle funzioni MDR in Kaspersky Security Center con un server proxy o un software anti-virus
  - Nascondere e mostrare le funzionalità MDR in Kaspersky Security Center
- Web Console MDR
- Modifica della lingua dell'interfaccia in Kaspersky Security Center
- Modifica della lingua per le notifiche e i rapporti in Kaspersky Security Center
- Modifica della lingua dell'interfaccia in Web Console MDR

Attivazione di Kaspersky Managed Detection and Response

- Attivazione di Kaspersky Managed Detection and Response in Kaspersky Security Center
- Attivazione di Kaspersky Managed Detection and Response in Web Console MDR
- Attivazione della soluzione MDR nelle applicazioni Kaspersky
  - Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenze del componente aggiuntivo Kaspersky MDR
  - Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenze Kaspersky MDR
  - Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenze Kaspersky Symphony MDR e NEXT Complete Security
  - Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenza del componente aggiuntivo Kaspersky Managed Detection and Response for Industrial CyberSecurity
  - Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenza del componente aggiuntivo Kaspersky Managed Detection and Response for Embedded Systems Security

Disattivazione di Kaspersky Managed Detection and Response

- Interruzione dell'utilizzo di Kaspersky Managed Detection and Response
- Sospensione temporanea dell'utilizzo di Kaspersky Managed Detection and Response
- Revoca del consenso alle condizioni per l'utilizzo della soluzione MDR

Distribuzione di Kaspersky Managed Detection and Response

- Distribuzione on-premise
  - Distribuzione tramite Kaspersky Security Center

- Distribuzione tramite Kaspersky Security Center Web Console
- Distribuzione basata su cloud
- Componenti necessari per il funzionamento di MDR

Informazioni sul file di configurazione MDR
- Download del file di configurazione MDR in Kaspersky Security Center
- Download del file di configurazione MDR in Web Console MDR

Gestione delle licenze
- Confronto dei livelli delle licenze commerciali
- Informazioni sulla licenza
- Informazioni sul codice di attivazione
- Fornire un nuovo codice di attivazione
- Gestione delle licenze in Kaspersky Security Center
- Risoluzione dei problemi di licensing

Trasmissione dei dati
- Aree geografiche del trattamento dei dati

Informazioni su Kaspersky Security Network
- Aggiornamento periodico dei file di configurazione di KPSN
- Passaggio della soluzione MDR al funzionamento senza file di configurazione di KPSN

Monitoraggio dei dashboard in Web Console MDR

Ricezione di informazioni di riepilogo
- Ricezione di un riepilogo di tutte le risorse in un file CSV (Web Console MDR)
- Ricezione delle informazioni sull'incidente in formato PDF (Web Console MDR)
- Impostazione dell'invio di rapporti periodici in Web Console MDR

Ricezione di notifiche
- Impostazione delle notifiche in Web Console MDR
- Impostazione delle notifiche in Kaspersky Security Center
- Ricezione delle notifiche estese
  - Abilitazione delle notifiche estese in Web Console MDR
  - Abilitazione delle notifiche estese in Kaspersky Security Center

Gestione degli utenti
- Invito di nuovi utenti in Web Console MDR
- Modifica dei ruoli utente in Web Console MDR
- Modifica dei metodi di notifica all'utente in Web Console MDR
- Modifica dell'accesso degli utenti ai tenant in Web Console MDR

Gestione delle risorse
- Visualizzazione e ricerca delle risorse in Web Console MDR
- Filtro delle risorse in Web Console MDR
- Visualizzazione di informazioni dettagliate sulle risorse in Web Console MDR
- Stati delle risorse
  - Controllo dello stato delle risorse in Kaspersky Security Center
- Come evitare la perdita dei dati di telemetria dalle risorse

Gestione degli incidenti
- Informazioni sugli incidenti
- Visualizzazione e ricerca degli incidenti in Web Console MDR
- Filtro degli incidenti in Web Console MDR
- Creazione di incidenti personalizzati in Web Console MDR
- Visualizzazione di informazioni dettagliate sugli incidenti in Web Console MDR

- Tipi di reazioni
- Elaborazione delle reazioni agli incidenti in Web Console MDR
- Accettazione automatica delle reazioni in Web Console MDR
- Accettazione automatica delle risposte in Kaspersky Security Center
- Chiusura degli incidenti in Web Console MDR
- Invio di un incidente al team di Reazione agli Incidenti per ulteriori indagini

Utilizzo delle funzionalità di Kaspersky Endpoint Detection and Response Optimum

Multi-tenancy

- Gestione dei tenant in Kaspersky Security Center
  - Visualizzazione dei tenant in Kaspersky Security Center
  - Visualizzazione delle impostazioni dei tenant in Kaspersky Security Center
  - Modifica delle impostazioni dei tenant in Kaspersky Security Center
  - Aggiunta di nuovi tenant in Kaspersky Security Center
  - Eliminazione di tenant in Kaspersky Security Center
  - Spostamento delle risorse tra tenant
- Gestione dei tenant in Web Console MDR
  - Visualizzazione dei tenant in Web Console MDR
  - Visualizzazione delle impostazioni dei tenant in Web Console MDR
  - Modifica delle impostazioni dei tenant in Web Console MDR
  - Aggiunta di nuovi tenant in Web Console MDR
  - Eliminazione di tenant in Web Console MDR

Gestione della soluzione tramite l'API REST

- Scenario: esecuzione dell'autorizzazione basata su token
- Creazione di una connessione API in Kaspersky Security Center
- Creazione di una connessione API in Web Console MDR
- Modifica di una connessione API in Kaspersky Security Center
- Modifica di una connessione API in Web Console MDR
- Creazione di un token di accesso in Kaspersky Security Center
- Creazione di un token di accesso in Web Console MDR
- Utilizzo dell'API REST
- Revoca di un token di aggiornamento in Kaspersky Security Center
- Eliminazione di una connessione API in Kaspersky Security Center
- Eliminazione di una connessione API in Web Console MDR

Problemi noti

Contattare il Servizio di assistenza tecnica

- Come ottenere assistenza tecnica
- Assistenza tecnica tramite Kaspersky CompanyAccount

Fonti di informazioni sulla soluzione

Glossario

- Applicazione EPP
- Endpoint Protection Platform (EPP)
- Incidente
- IOC
- Reazione
- Risorsa
- Tattica MITRE
- Tecnica MITRE

Telemetria
Tenant
Informazioni sul codice di terze parti
Note relative ai marchi registrati

Guida di Kaspersky Managed Detection and Response

Nuove funzionalità

- Novità dell'ultima versione della soluzione

Requisiti hardware e software

- Verificare quali sistemi operativi e applicazioni EPP sono supportati

Confronto delle funzionalità

- Confronto delle soluzioni con licenza commerciale: MDR Optimum, MDR Expert, MDR Basic, MDR Advanced e MDR Prime

Come iniziare

- Distribuzione on-premise
- Distribuzione basata su cloud
- Attivazione di Kaspersky Managed Detection and Response

Monitoraggio e rapporti

- Ricezione di notifiche
- Ricezione delle notifiche estese
- Ricezione di informazioni di riepilogo
- Dashboard di monitoraggio

Trasmissione dei dati/protezione dei dati personali

- Trasmissione dei dati
- Kaspersky Security Network

Novità

Kaspersky Managed Detection and Response presenta numerosi miglioramenti e nuove funzionalità.

Dicembre 2025

- È stato aggiunto il supporto per le seguenti applicazioni EPP:
  - Kaspersky Embedded Systems Security for Windows versione 4.0
  - Kaspersky Industrial CyberSecurity for Nodes versione 4.5
- Ora è possibile impostare notifiche Telegram estese nel plug-in MDR oltre che in Web Console MDR.
- È possibile inviare gli incidenti al team di Incident Response per ulteriori indagini utilizzando l'interfaccia di Web Console MDR.

Ottobre 2025

Ora è possibile impostare notifiche Telegram estese nel plug-in Web Console MDR.

Luglio 2025

- Aggiunta la possibilità di utilizzare codici di attivazione per attivare la soluzione MDR nelle seguenti applicazioni:
  - Kaspersky Endpoint Security for Linux versione 12.3
  - Kaspersky Endpoint Security for Linux versione 12.3 in modalità Light Agent
  - Kaspersky Endpoint Security for Windows versione 12.6 o successiva
  - Kaspersky Endpoint Security for Windows versione 12.8 o successiva in modalità Light Agent
  - Kaspersky Endpoint Security for Mac versione 12.2

    Per maggiori dettagli, fare riferimento al seguente articolo: Attivazione della soluzione MDR nelle applicazioni Kaspersky.
- La soluzione MDR può ora funzionare senza il file di configurazione di KPSN con le seguenti applicazioni:
  - Kaspersky Endpoint Security for Linux versione 12.3
  - Kaspersky Endpoint Security for Linux versione 12.3 in modalità Light Agent
  - Kaspersky Endpoint Security for Windows versione 12.6 o successiva
  - Kaspersky Endpoint Security for Windows versione 12.8 o successiva in modalità Light Agent
  - Kaspersky Endpoint Security for Mac versione 12.2
  - Per maggiori dettagli fare riferimento al seguente articolo: Passaggio della soluzione MDR al funzionamento senza file di configurazione di KPSN.
- La soluzione MDR supporta ora Kaspersky Endpoint Security for Windows versione 12.8 o successiva in modalità Light Agent.
- La versione 2.5.1 del plug-in MDR supporta ora il funzionamento di MDR senza il file di configurazione di KPSN.
- Kaspersky Endpoint Security for Linux versione 12.3 supporta ora le seguenti azioni di reazione:
  - Isola
  - Disabilita isolamento
  - Sposta in Quarantena
  - Ripristina il file dalla Quarantena
  - Termina processo
  - Esegui processo

Maggio 2025

- Nella sezione Licenze del plug-in MDR per Kaspersky Security Center:
  - Per ogni licenza MDR viene ora visualizzato il nome del client a cui è stata rilasciata la licenza.
  - È ora disponibile la matrice di utilizzo delle licenze specifiche nei tenant.
- Nella sezione Tenant del plug-in MDR per Kaspersky Security Center:
  - Quando si crea un file di configurazione MDR per un problema di licenza specifico, ora viene visualizzato il nome del client per il quale è stata rilasciata la licenza.
  - L'elenco dei tenant ora visualizza il tenant radice, creato per impostazione predefinita dopo l'attivazione del client. È possibile scaricare i file di configurazione per tutte le licenze correnti per il tenant radice.

Febbraio 2025

- MDR Web Console ora presenta la sezione **Licensing**. Sono disponibili le seguenti funzionalità:
  - Visualizzazione delle licenze MDR correnti, inutilizzare e scadute.
  - Visualizzazione del numero totale di risorse e del relativo limite per ciascuna licenza.
  - Download del file di configurazione MDR per il tenant principale.

    Utilizzare la sezione **Tenant** per creare e scaricare i file di configurazione MDR per altri tenant.
  - Inserimento di un nuovo codice di attivazione.

    Se l'organizzazione dispone di più licenze, è possibile gestirle solo nel plug-in MDR per Kaspersky Security Center. La sezione **Licensing** in MDR Web Console diventa di sola lettura.
- Il plug-in MDR per Kaspersky Security Center supporta ora l'applicazione di più licenze nell'organizzazione. Sono disponibili le seguenti funzionalità:
  - Visualizzazione delle licenze MDR correnti, inutilizzare e scadute.
  - Terminazione di una licenza MDR corrente.
  - Inserimento di un nuovo codice di attivazione.
  - Download del file di configurazione MDR del tenant radice per una licenza.
  - Scelta di una licenza per un file di configurazione MDR durante la creazione o la modifica di un tenant nella sezione **Tenant**.

Dicembre 2024

- Attivazione semplificata di Kaspersky Managed Detection and Response sui dispositivi Kaspersky Endpoint Security for Windows (a partire dalla versione 12.4). È sufficiente una licenza standard per la soluzione Kaspersky MDR.

  Tenere presente che sarà comunque necessario utilizzare il file di configurazione MDR (BLOB) in uno qualsiasi dei seguenti scenari:

  - Si dispone di più di un tenant.
  - Si utilizza la soluzione MDR insieme a Kaspersky Endpoint Detection and Response Optimum.

- Aggiunto supporto per la gestione della soluzione MDR in Kaspersky Security Center Linux (a partire dalla versione 15.1).

- Aggiunte informazioni dettagliate sui requisiti dei canali di comunicazione nella Guida.

Ottobre 2024

È stato rilasciato il plug-in MDR per Kaspersky Security Center versione 2.4.1. Contiene i seguenti miglioramenti:

- La possibilità di configurare l'accettazione automatica delle azioni di reazione per i tenant selezionati è stata aggiunta nel plug-in MDR per Kaspersky Security Center.

- Funzionalità e interfaccia utente avanzate della sezione che fornisce l'elenco delle risorse inattive. Tali risorse sono state aggiunte a Kaspersky Security Center, con il componente MDR installato, ma che non hanno mai inviato la telemetria a Kaspersky Managed Detection and Response. È possibile filtrare le risorse in base allo stato di MDR, visualizzare informazioni dettagliate su ciascuna risorsa ed esportare l'elenco delle risorse in un file CSV.

  > Questa funzionalità funziona correttamente in Kaspersky Security Center 15.1 Windows e versioni successive, Kaspersky Security Center 15.1 Linux e versioni successive e Kaspersky Security Center Cloud Console.

- Un'attività per l'invio periodico di un rapporto sugli incidenti aperti ora può essere creata solo in MDR Web Console. Questa funzionalità è stata rimossa dalla sezione MDR in Kaspersky Security Center.

Luglio 2024

MDR Web Console ora consente di configurare l'accettazione automatica delle azioni di reazione per i tenant selezionati.

Giugno 2024

- Sono ora disponibili nuove azioni di reazione:
  - Sposta il file in Quarantena
  - Ripristina il file dalla Quarantena
  - Esegui uno script su una risorsa
- Documentazione dell'API REST aggiornata, inclusi nuovi esempi di script.
- Rapporti notevolmente riprogettati:
  - Mappatura di MITRE ATT&CK per un'analisi approfondita delle minacce.
  - Elenco dei computer più frequentemente presi di mira dagli autori di attacchi per aiutare i clienti a concentrarsi sui rischi critici.
- Supporto multi-tenant:
  - Generazione di rapporti e configurazione della pianificazione dei rapporti di riepilogo per tenant specifici.
  - Passaggio senza problemi dai widget alle statistiche specifiche del tenant nella dashboard di monitoraggio.
  - Configurazione della conferma automatica dell'esecuzione dell'attività di reazione per tenant specifici.
  - API MDR migliorata per la gestione dei tenant.

Dicembre 2023

- Web Console MDR ora contiene il dashboard delle **statistiche di telemetria**, che mostra il numero di eventi di telemetria, avvisi di sicurezza e incidenti.
- Kaspersky Managed Detection and Response ora supporta Kaspersky Endpoint Security for Windows nella configurazione di Endpoint Detection and Response Agent (EDR Agent) (con le limitazioni).

Novembre 2023

- Visualizzazione migliorata degli stati delle risorse in MDR Web Console e nel plug-in MDR per Kaspersky Security Center: lo stato delle risorse ora mostra l'operabilità dei componenti dell'applicazione EPP della risorsa, lo stato di aggiornamento del database anti-virus della risorsa e lo stato della trasmissione della telemetria.
- Lo stato delle risorse ora mostra la presenza di perdite di telemetria, consentendo di identificare le risorse con problemi di distribuzione della telemetria. Questa funzionalità è abilitata per impostazione predefinita per i nuovi clienti e verrà abilitata gradualmente per i clienti esistenti.

Ottobre 2023

È stata aggiunta l'area di residenza dei clienti **Arabia Saudita**. Per questi clienti i dati di telemetria vengono archiviati nel Regno dell'Arabia Saudita.

Settembre 2023

È stato rilasciato il plug-in MDR per Kaspersky Security Center versione 2.3.1. In questa versione le funzioni di gestione degli incidenti sono state rimosse dalla sezione MDR in Kaspersky Security Center. È possibile gestire gli incidenti in Web Console MDR.

Luglio 2023

È stato rilasciato il plug-in MDR per Kaspersky Security Center versione 2.3.0. Contiene i seguenti miglioramenti:

- Ora è possibile impostare notifiche estese nel plug-in MDR.
- Ora è possibile utilizzare le funzionalità MDR in Kaspersky Security Center con il plug-in MDR tramite un server proxy.
- Ora è possibile modificare i certificati per l'utilizzo delle funzioni MDR in Kaspersky Security Center con un server proxy o un software anti-virus.

Luglio 2022

Rilascio della versione 2.1.17 del plug-in MDR. Questa versione del plug-in è compatibile con Kaspersky Security Center versione 14 e successive.

Maggio 2022

Miglioramenti generali:

- È stata aggiunta l'area geografica di residenza dei clienti **Stati Uniti/Canada**. Per questi clienti i dati di telemetria vengono archiviati nel Nord Europa.
- È stata modificata la descrizione del processo di distribuzione MDR nella guida.

Miglioramenti nel plug-in MDR:

- Nella sezione **Impostazioni** ora è possibile modificare la lingua per le notifiche in Telegram e nell'e-mail e per la comunicazione in chat sugli incidenti.
- Interfaccia migliorata per l'utilizzo di immagini e tabelle nelle schede degli incidenti.
- MDR Expert. Nella sezione **Utilizzo dei servizi** è possibile verificare quanti incidenti possono essere creati in base allo SLA.

Correzioni di bug e altri miglioramenti:

- La ricerca negli elenchi delle risorse e degli incidenti adesso viene eseguita da un'occorrenza completa della sottostringa cercata in qualsiasi punto della stringa.
- In Kaspersky Endpoint Security per Mac versione 11.2 e successive, dopo aver immesso il codice di attivazione MDR e aggiunto il file di configurazione di KPSN, non è più necessario riavviare il dispositivo Mac per avviare un trasferimento di telemetria.
- Quando si calcolano le licenze per le macchine virtuali con Kaspersky Security for Virtualization Light Agent 5.2 e versioni successive, non vengono incluse le risorse che non trasferiscono dati di telemetria da più di 24 ore.

Marzo 2022

Gli utenti MDR Optimum adesso possono chattare con gli analisti Kaspersky SOC in merito a un incidente con la seguente limitazione: le richieste vengono elaborate solo in relazione a un determinato incidente e non viene applicato alcuno SLA.

Ottobre 2021

- Il plug-in Kaspersky Managed Detection and Response per Kaspersky Security Center Web Console e Cloud Console è stato aggiornato con la funzionalità relativa agli stati delle risorse MDR avanzata:
  - Interfaccia migliorata degli stati delle risorse MDR.
  - L'elenco delle risorse mostra tutte le risorse di tutti gli stati precedentemente disponibili solo in Web Console MDR.
  - Sono state aggiunte opzioni di filtro e ordinamento per lavorare con l'elenco delle risorse.

Luglio 2021

- Supporto di Kaspersky Managed Detection and Response in Kaspersky Security Center Cloud Console, che consente la gestione della soluzione nella console di amministrazione singola di Kaspersky Security Center. Le seguenti funzionalità sono disponibili con la soluzione Kaspersky Managed Detection and Response:

  - Gestione degli incidenti:

    - Visualizzazione, creazione, commento degli incidenti
    - Comunicazione con Kaspersky Security Operation Center in merito a un incidente, accettazione o rifiuto delle reazioni suggerite dagli analisti SOC
    - Reazione a un incidente con l'utilizzo di Kaspersky Endpoint Detection and Response

    Sono disponibili le seguenti reazioni:

    - Applicazione dell'isolamento di rete dei dispositivi
    - Creazione di regole di blocco tramite hash
    - Creazione di attività per l'eliminazione, lo spostamento in quarantena, la conclusione del processo e la ricerca tramite indicatori di compromissione (IOC), relativi a un incidente

  - Monitoraggio degli eventi di Kaspersky Managed Detection and Response nei dashboard nella console di monitoraggio di Kaspersky Security Center Web Console
  - Configurazione delle notifiche sugli eventi di Kaspersky Managed Detection and Response tramite e-mail e Telegram
  - Configurazione della pianificazione del riepilogo delle prestazioni MDR inviata tramite e-mail
  - Visualizzazione dei dispositivi con problemi a livello di prestazioni MDR
  - Nuova procedura guidata di attivazione, che consente di connettere MDR in Kaspersky Security Center Web Console
  - Configurazione automatica di KPSN, che non richiede più il download e il caricamento manuali del file di configurazione nelle impostazioni di Kaspersky Security Center
  - Gestione delle connessioni all'API MDR pubblica: visualizzazione, creazione, modifica ed eliminazione di token
  - Gestione dei tenant dell'organizzazione, inclusa la relativa creazione
  - Acquisizione delle informazioni sul numero di incidenti disponibili per la registrazione da parte dell'utente, che possono essere elaborati in base ai termini del contratto di servizio (SLA)

    > Queste funzionalità sono disponibili anche in Kaspersky Security Center Web Console.

- In Web Console MDR è stata aggiunta la gestione di più account amministratore MDR: creazione degli account e gestione dei relativi privilegi

- Le nuove versioni delle applicazioni compatibili non richiedono più l'installazione aggiuntiva di Kaspersky Endpoint Agent. La funzionalità Kaspersky Managed Detection and Response integrata è compatibile con le seguenti applicazioni EPP:

  - Kaspersky Endpoint Security for Windows 11.6 e versioni successive
  - Kaspersky Endpoint Security for Mac 11.2
  - Kaspersky Endpoint Security for Linux 11.2
  - Kaspersky Security for Virtualization 5.2 Light Agent

  Per informazioni dettagliate sui diversi scenari di distribuzione, fare riferimento alla Distribuzione di Kaspersky Managed Detection and Response.

- È stato aggiunto il filtro per tipo di evento per Kaspersky Endpoint Security for Windows e for Linux con la funzionalità Kaspersky Managed Detection and Response integrata, che consente di ridurre il carico sui canali e il consumo di traffico durante l'invio di dati tramite telemetria

- Supporto dei seguenti tipi di reazione: acquisizione del file dal dispositivo, isolamento del dispositivo, disabilitazione dell'isolamento del dispositivo, eliminazione della chiave del Registro di sistema, terminazione del processo

  L'esecuzione di queste azioni è possibile con la conferma da parte dell'utente con il ruolo di amministratore MDR.

- Supporto delle seguenti nuove localizzazioni nel plug-in Web per Kaspersky Security Center Web Console e Cloud Console: francese, tedesco, italiano e spagnolo.

Marzo 2021

Un nuovo plug-in Web per Kaspersky Security Center Web Console consente di utilizzare la seguente funzionalità Kaspersky Managed Detection and Response:

- Visualizzazione degli incidenti
- Creazione di incidenti
- Aggiunta di commenti agli incidenti
- Comunicazione con Kaspersky Security Operation Center in merito a un incidente
- Accettazione o rifiuto delle reazioni suggerite dagli analisti SOC
- Possibilità di reazione indipendente a un incidente:

  - Isolamento delle risorse dalla rete
  - Creazione di regole di blocco tramite hash
  - Creazione di attività per l'eliminazione, lo spostamento in quarantena, la conclusione del processo e la ricerca tramite indicatori di compromissione (IOC), relativi a un incidente

- Monitoraggio degli eventi di Kaspersky Managed Detection and Response nei dashboard nella console di monitoraggio di Kaspersky Security Center Web Console

- Configurazione delle notifiche e-mail e Telegram sugli eventi di Kaspersky Managed Detection and Response
- Configurazione della pianificazione del riepilogo degli incidenti inviati tramite e-mail

Informazioni su Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response è una soluzione che rileva e analizza automaticamente gli incidenti di sicurezza nell'infrastruttura utilizzando la telemetria e avanzate tecnologie di machine learning, quindi trasferisce le informazioni sull'incidente agli esperti Kaspersky. Gli esperti possono quindi elaborare l'incidente da soli o fornire raccomandazioni su come elaborarlo.

Kaspersky Managed Detection and Response (anche denominato MDR) garantisce una protezione 24 ore su 24 dal crescente volume di minacce che aggirano le barriere di sicurezza automatizzate per le organizzazioni con risorse interne limitate o che hanno difficoltà a trovare le competenze e il personale necessari. A differenza di offerte simili sul mercato, questa soluzione sfrutta una comprovata esperienza nella ricerca di attacchi mirati per garantire una difesa continua anche contro le minacce più complesse. La soluzione aiuta a migliorare la resilienza aziendale alle minacce informatiche, liberando le risorse esistenti in modo che possano concentrare la loro attenzione su altre attività.

La soluzione Kaspersky Managed Detection and Response (MDR) non è disponibile negli Stati Uniti o per i cittadini statunitensi. L'utilizzo della soluzione MDR nel territorio specificato o da parte dei cittadini statunitensi costituisce una violazione dei termini di utilizzo della soluzione MDR. Per evitare di violare i termini di utilizzo della soluzione MDR è necessario terminare l'utilizzo di MDR in modo permanente in tutte le risorse che si trovano nel territorio specificato o utilizzate dai cittadini statunitensi. Quando i soggetti non statunitensi si trovano temporaneamente negli Stati Uniti, è necessario sospendere l'utilizzo di MDR sulle proprie risorse.

Principio operativo di Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response analizza i dati di telemetria provenienti dalle applicazioni EPP e genera eventi di sicurezza che possono essere classificati come incidenti dalla tecnologia di rilevamento.

Per elaborare gli incidenti viene utilizzata la Web Console MDR. In alternativa, è possibile integrare Kaspersky Managed Detection and Response con una soluzione di terzi, come descritto nell'articolo: Gestione della soluzione tramite l'API REST.

La soluzione Kaspersky Managed Detection and Response può risolvere automaticamente un incidente o richiedere una reazione da parte dell'utente in caso di una potenziale minaccia per la protezione. Per maggiori dettagli, fare riferimento all'articolo Tipi di reazione. Per garantire una reazione tempestiva a potenziali minacce per la protezione, la soluzione Kaspersky Managed Detection and Response potrebbe richiedere chiarimenti all'utente in caso di eventi sospetti. Si consiglia di elaborare tali richieste in tempo.

> L'indagine dettagliata sugli incidenti (ad esempio l'accertamento degli eventi precedenti, delle circostanze e del meccanismo dettagliato dell'attacco) è gestita dal componente Kaspersky Incident Response, che non è incluso in Kaspersky Managed Detection and Response e deve essere acquistato separatamente.

L'utilizzo Kaspersky Managed Detection and Response prevede che l'utente elabori gli incidenti con il supporto degli esperti di Kaspersky. Per maggiori informazioni, consulta l'articolo: Aree di responsabilità.

Informazioni sulle origini dei dati

Kaspersky Managed Detection and Response riceve i dati dalle applicazioni EPP che supportano MDR, elabora i dati e li invia tramite i flussi Kaspersky Security Network a Kaspersky Managed Detection and Response. Per l'elenco dei dati elaborati, fare riferimento alla sezione Trasmissione dei dati. Le applicazioni EPP vengono installate nelle risorse all'interno dell'infrastruttura IT di un'organizzazione (ad esempio dispositivi mobili, computer o laptop). Un esempio di applicazione EPP è Kaspersky Endpoint Security for Windows.

È inoltre possibile integrare Kaspersky Managed Detection and Response con altre soluzioni Kaspersky: Kaspersky Managed Detection and Response consente di analizzare e monitorare i dati dalla piattaforma Kaspersky Anti Targeted Attack (KATA). Per configurare l'integrazione tra Kaspersky Managed Detection and Response e Kaspersky Anti-Targeted Attack Platform, è prima necessario ricevere un file di configurazione MDR. Per informazioni dettagliate su come configurare l'integrazione, fare riferimento alla Guida in linea della piattaforma Kaspersky Anti-Targeted Attack.

La piattaforma Kaspersky Anti Targeted Attack non fa parte di Kaspersky Managed Detection and Response. Se si desidera utilizzare la piattaforma Kaspersky Anti Targeted Attack Platform, è necessario acquistarla separatamente. L'integrazione con Kaspersky Anti Targeted Attack Platform non è disponibile quando si applica un codice di attivazione per l'Arabia Saudita.

In caso di problemi durante l'installazione delle applicazioni EPP o la configurazione dell'integrazione MDR con altre soluzioni Kaspersky, contattare l'assistenza tecnica.

Aree di responsabilità

L'utilizzo Kaspersky Managed Detection and Response prevede che gli utenti elaborino gli incidenti con il supporto degli esperti di Kaspersky. Inoltre, l'Assistenza tecnica di Kaspersky gestisce i problemi relativi alle soluzioni.

Nella tabella riportata di seguito sono indicate le aree di responsabilità degli utenti, degli esperti do Kaspersky e dell'Assistenza tecnica di Kaspersky.

Attività	Esperti di Kaspersky	Assistenza tecnica di Kaspersky	Utenti MDR
Attivazione di MDR, distribuzione di MDR, gestione delle risorse, impostazione delle notifiche, gestione degli utenti, cessazione dell'utilizzo di MDR.	–	Consultazione	Esecuzione dell'attività
Utilizzo di MDR Web Console per gestire gli incidenti	–	Consultazione	Esecuzione dell'attività
Rilevamento, indagine, emissione di suggerimenti di reazione per gli incidenti basati sui dati di telemetria	Esecuzione dell'attività	–	Ricezione di informazioni
Chiarire i dettagli durante l'indagine, rispondere alle domande degli esperti di Kaspersky per ottenere migliori suggerimenti di reazione.	Ricezione di informazioni	–	Esecuzione dell'attività
Creazione di richieste per utilizzare gli strumenti e le funzionalità di MDR per gestire gli incidenti	Esecuzione dell'attività	–	Ricezione di informazioni
Coordinamento delle richieste di utilizzo degli strumenti e delle funzionalità di MDR per gestire gli incidenti	Ricezione di informazioni	–	Esecuzione dell'attività
Esecuzione di attività al di fuori delle capacità funzionali di MDR	Consultazione	–	Esecuzione dell'attività
Creazione manuale di un incidente (è importante scegliere una risorsa MDR e descrivere l'incidente in dettaglio)	Ricezione di informazioni	–	Esecuzione dell'attività

Gestione dei problemi con i componenti dell'infrastruttura Kaspersky che influenzano MDR	Ricezione di informazioni	Consultazione	Esecuzione dell'attività
Gestione delle regole di rilevamento	Esecuzione dell'attività	–	–

Informazioni sul Contratto di MDR

Il Contratto di MDR è un accordo vincolante tra l'utente e AO Kaspersky Lab, che stabilisce i termini per l'utilizzo della soluzione.

Leggere attentamente il Contratto di MDR prima di iniziare a utilizzare la soluzione.

È possibile visualizzare il Contratto di MDR:

- Durante l'attivazione di Kaspersky Managed Detection and Response.
- Facendo clic sul collegamento **Condizioni per l'utilizzo della soluzione MDR** nella sezione **Condizioni per l'utilizzo della soluzione MDR**: sezione **MDR** di Kaspersky Security Center → **Utilizzo di MDR** → **Condizioni per l'utilizzo della soluzione MDR**.

L'utente accetta i termini del Contratto di MDR confermando di accettare il Contratto di MDR all'attivazione della soluzione. Se non si accetta il Contratto di MDR, annullare l'attivazione di Kaspersky Managed Detection and Response e non utilizzare la soluzione.

Informazioni sull'Accordo di elaborazione dei dati

L'Accordo di elaborazione dei dati (DPA) è parte integrante del Contratto di Kaspersky Managed Detection and Response. L'Accordo di elaborazione dei dati si applica al trattamento dei dati dell'utente da parte di AO Kaspersky Lab per conto di un utente.

Il contenuto dell'*Accordo di elaborazione dei dati* (DPA), la relativa disponibilità nelle interfacce della soluzione e l'elenco dei dati dell'utente dipendono dall'area geografica in cui viene utilizzata la soluzione.

È possibile visualizzare l'Accordo di elaborazione dei dati:

- Durante l'attivazione di Kaspersky Managed Detection and Response (solo per alcune regioni).
- Nella sezione **Informazioni** di Web Console MDR: https://mdr.kaspersky.com/about (solo per alcune regioni).

  La sezione **Informazioni** è disponibile solo per gli utenti che hanno effettuato l'accesso.

- Nel set di documenti che si ottiene acquistando la soluzione Kaspersky Managed Detection and Response (solo per alcune regioni).

Leggere attentamente l'Accordo di elaborazione dei dati prima di iniziare a utilizzare la soluzione.

L'utente conferma di aver letto e compreso completamente l'Accordo di elaborazione dei dati quando attiva la soluzione o quando acquista la soluzione Kaspersky Managed Detection and Response. Se non si accetta l'elaborazione dei dati secondo le modalità descritte nell'Accordo di elaborazione dei dati, annullare l'attivazione di Kaspersky Managed Detection and Response e non utilizzare la soluzione.

Requisiti hardware e software

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Applicazioni EPP richieste e configurazioni supportate

Per utilizzare Kaspersky Managed Detection and Response, è necessario distribuire nell'infrastruttura almeno una delle seguenti applicazioni EPP:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- Kaspersky Security for Windows Server con Kaspersky Endpoint Agent for Windows

  Per utilizzare la funzionalità MDR nei server che eseguono il sistema operativo Windows, si consiglia di utilizzare Kaspersky Endpoint Security for Windows in questi server invece di Kaspersky Security for Windows Server con Kaspersky Endpoint Agent.
- Kaspersky Security for Virtualization 5.2 Light Agent
- Kaspersky Embedded Systems Security for Windows
- Kaspersky Industrial CyberSecurity for Nodes Windows

Sistemi operativi

Kaspersky Managed Detection and Response è compatibile con gli stessi sistemi operativi delle applicazioni EPP elencate di seguito. Per informazioni dettagliate, fare riferimento alla sezione *Requisiti hardware e software* nella documentazione delle applicazioni EPP compatibili elencate nella tabella di seguito.

Applicazioni e soluzioni Kaspersky compatibili

Kaspersky Managed Detection and Response è compatibile con le versioni delle applicazioni e delle soluzioni Kaspersky elencate nella tabella seguente.

Applicazione Kaspersky	Versioni consigliate e relativo periodo di supporto	Versioni compatibili e relativo periodo di supporto *	Note
Kaspersky Endpoint Security for Windows	12.8 o versione successiva	12.6 o versione successiva	Kaspersky Endpoint Security for Windows versione 12.6–12.9 supporta l'attivazione della soluzione MDR con un codice di attivazione. Kaspersky Endpoint Security for Windows versione 12.10 o successiva supporta anche l'attivazione della soluzione MDR con un file chiave.
Kaspersky Endpoint Security for Windows in modalità Light Agent	12.9 o versione successiva	12.8	Kaspersky Endpoint Security for Windows versione 12.6–12.9 in modalità Light Agent supporta l'attivazione della soluzione MDR con un codice di attivazione. Kaspersky Endpoint Security for Windows 12.10 o versione successiva in modalità Light Agent supporta anche l'attivazione della soluzione MDR con un file chiave.
Kaspersky Endpoint Security for Windows nella configurazione di Endpoint Detection and Response Agent (EDR Agent) A partire da Kaspersky Endpoint Security for Windows versione 12.3, l'applicazione include la configurazione Endpoint Detection and Response Agent (EDR Agent). Endpoint Detection and Response Agent è un'applicazione che viene installata nelle singole workstation e nei server nell'infrastruttura IT dell'organizzazione per supportare le soluzioni Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform (EDR). EDR Agent monitora continuamente i processi in esecuzione su questi computer, le connessioni di rete aperte e i file in fase di modifica. I componenti di protezione e controllo non sono disponibili per EDR Agent. EDR Agent è compatibile con le applicazioni EPP di terze parti. Ciò consente di utilizzare strumenti di protezione dell'infrastruttura di terze parti insieme a Detection and Response di Kaspersky. Per ulteriori dettagli, consultare la Guida in linea di Kaspersky Endpoint Security for Windows.	12.8 o versione successiva	12.6 o versione successiva	• Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione di EDR Agent, gli stati *Avviso* e *Critico* per i componenti di controllo e protezione non vengono visualizzati. • Non è possibile utilizzare le funzionalità di Kaspersky Endpoint Detection and Response Optimum per le risorse con Kaspersky Endpoint Security for Windows nella configurazione di EDR Agent. • L'elenco delle applicazioni EPP di terze parti compatibili con EDR Agent è disponibile nella Guida in linea di Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Windows versione 12.6–12.9 nella configurazione di Endpoint Detection and Response Agent (agente EDR) supporta l'attivazione della soluzione MDR con un codice di attivazione. Kaspersky Endpoint Security for Windows 12.10 o versione successiva, nella configurazione di Endpoint Detection and Response Agent (agente EDR), supporta anche l'attivazione della soluzione MDR con un file chiave.

Applicazione Kaspersky	Versioni consigliate e relativo periodo di supporto	Versioni compatibili e relativo periodo di supporto *	Note
Kaspersky Endpoint Security for Linux	12.3 o versione successiva	12.1 o versione successiva	Se si utilizza Kaspersky Endpoint Security for Linux e non è installato il pacchetto Linux Audit Daemon (denominato anche auditd), gli eventi di controllo del sistema vengono registrati nel log del kernel `dmesg`. È consigliabile installare il pacchetto auditd per una maggiore praticità nella gestione della rotazione dei log di Kaspersky Endpoint Security for Linux. Kaspersky Endpoint Security for Linux 12.3 o versione successiva supporta l'attivazione della soluzione MDR sia con un file chiave che con un codice di attivazione.
Kaspersky Endpoint Security for Linux in modalità Light Agent	12.3 o versione successiva	12.1 o versione successiva	Kaspersky Endpoint Security for Linux 12.3 o versione successiva nella modalità Light Agent supporta l'attivazione della soluzione MDR sia con un file chiave che con un codice di attivazione.
Kaspersky Endpoint Security for Mac	12.2 o versione successiva	12 o versione successiva	Kaspersky Endpoint Security for Mac supporta l'attivazione della soluzione MDR con un codice di attivazione.
Kaspersky Security for Virtualization Light Agent	6.3 o versione successiva	5.2 o versione successiva	Kaspersky Security for Virtualization 5.2 Light Agent non è supportato se si utilizza Kaspersky Security Center Linux. Per Kaspersky Security for Virtualization 6.3 Light Agent consigliamo di utilizzare Kaspersky Endpoint Security for Windows 12.10 o versione successiva oppure Kaspersky Endpoint Security for Linux 12.3 o versione successiva in modalità Light Agent.
Kaspersky Embedded Systems Security for Windows	4.0	4.0	Applicazione di un codice di attivazione per Kaspersky Managed Detection and Response for Embedded Systems Security Add-on è disponibile solo nel plug-in MDR e richiede una licenza MDR Expert.
Kaspersky Industrial CyberSecurity for Nodes	4.5	4.5	

Applicazione Kaspersky	Versioni consigliate e relativo periodo di supporto	Versioni compatibili e relativo periodo di supporto *	Note
Kaspersky Endpoint Agent	4.0 o versione successiva	3.15 o versione successiva	Kaspersky Endpoint Agent è necessario solo se si utilizza Kaspersky Security for Windows Server. La soluzione Kaspersky Managed Detection and Response è compatibile con Kaspersky Endpoint Agent versioni 3.9, 3.10 e 3.11, ma il periodo di assistenza tecnica per queste versioni è terminato. Se si utilizza Kaspersky Endpoint Agent versioni 3.9, 3.10 e 3.11 come agente per la soluzione Kaspersky Managed Detection and Response, Kaspersky consiglia di aggiornare Kaspersky Endpoint Agent alla versione 3.15 o a una versione successiva. L'utilizzo di Kaspersky Security Center Cloud Console è disponibile solo per Kaspersky Endpoint Agent for Windows 3.12 o versioni successive.
Kaspersky Security for Windows Server	Si consiglia di utilizzare Kaspersky Endpoint Security for Windows 12 o versione successiva	11.x	Per utilizzare la funzionalità MDR nei server che eseguono Windows, si consiglia di utilizzare Kaspersky Endpoint Security for Windows in questi server invece di Kaspersky Security for Windows Server con Kaspersky Endpoint Agent: • Il rilevamento delle minacce MDR funziona meglio con Kaspersky Endpoint Security for Windows. • La funzionalità MDR per Kaspersky Security for Windows Server non è in fase di sviluppo, poiché il supporto limitato di Kaspersky Security for Windows Server termina il 30 giugno 2025.
Kaspersky Security Center Windows	15.1 o versione successiva	15.1 o versione successiva	Con il plug-in MDR per Kaspersky Security Center.
Kaspersky Security Center Linux	15.1 o versione successiva	15.1 o versione successiva	Con il plug-in MDR per Kaspersky Security Center.
Kaspersky Security Center Cloud Console	n/d	n/d	La versione più recente viene sempre utilizzata nel cloud.
Plug-in MDR per Kaspersky Security Center	Versione più recente	Versione più recente	Il plug-in MDR 2.1.15 e versioni successive è disponibile solo in Kaspersky Security Center 15.1 Windows o versioni successive e in Kaspersky Security Center 15.1 Linux o versioni successive.
Kaspersky Security Center Network Agent	La versione fornita con Kaspersky Security Center Windows installata	13 o versione successiva	Quando si aggiorna Kaspersky Security Center, è necessario aggiornare anche Kaspersky Security Center Network Agent alla versione corrispondente.

Applicazione Kaspersky	Versioni consigliate e relativo periodo di supporto	Versioni compatibili e relativo periodo di supporto *	Note
Kaspersky Anti Targeted Attack Platform + Kaspersky Endpoint Detection and Response	6.1	6.0 o versione successiva	La soluzione cloud Kaspersky Endpoint Detection and Response Expert non è supportata.
Kaspersky Endpoint Detection and Response Optimum	3.0 o versione successiva	2.3 o versione successiva	Se si utilizza Kaspersky Endpoint Security for Windows 11.7 o versione successiva, EDR Optimum deve essere utilizzato senza Kaspersky Endpoint Agent. Per attivare le funzioni di Kaspersky Endpoint Detection and Response Optimum, è necessario immettere uno dei seguenti codici di attivazione per le risorse tramite Kaspersky Security Center: • Kaspersky Endpoint Detection and Response Optimum • Componente aggiuntivo Kaspersky Endpoint Detection and Response Optimum

* La soluzione MDR ha una funzionalità limitata quando utilizzata con le versioni delle applicazioni Kaspersky precedenti a quelle specificate nella colonna **Versioni compatibili e relativi termini di supporto**. Le limitazioni includono un minor numero di tipi di eventi e di azioni di reazione supportati.

Per ulteriori informazioni sulle versioni supportate delle applicazioni e delle soluzioni Kaspersky, fare riferimento alla pagina Web relativa al ciclo di vita dell'assistenza del prodotto.

Web Console MDR

MDR Web Console ha i seguenti requisiti hardware e software:

- Monitor che supporta una risoluzione dello schermo di 1024x768 o superiore
- Uno dei seguenti browser:
  - Apple Safari: 15 su macOS
  - Google Chrome: 100.0.4896.88 o versioni successive (build ufficiale)
  - Microsoft Edge: 100 o versioni successive
  - Mozilla Firefox: 91.8.0 o versione successiva

Canale di rete

La tabella seguente mostra la produttività del canale di rete calcolata in base ai nostri dati statistici.

Sistema operativo	Larghezza di banda stimata per 1000 risorse
Windows	4,3 Mbit/s
Server Windows	5,2 Mbit/s

Linux (media per host e server)	14,7 Mbit/s
macOS	8,5 Mbit/s

Questi valori di larghezza di banda sono approssimativi, poiché la larghezza di banda necessaria dipende in gran parte dal tipo di carico delle risorse che genera eventi di telemetria. Il throughput di picco può essere significativamente più elevato. Se l'infrastruttura funziona regolarmente al massimo del throughput, sarà necessario fornire una larghezza di banda di rete superiore. Diverse condizioni possono presumere che il carico sia superiore. Ad esempio:

- compilazione del codice di programma da parte degli sviluppatori
- scansione completa del sistema
- server a carico elevato (ad esempio DNS e controller di dominio)
- più connessioni di rete

Architettura di Kaspersky Managed Detection and Response

Descrizione dei componenti di Kaspersky Managed Detection and Response:

- Una risorsa è un dispositivo di un'organizzazione protetto dalle soluzioni Kaspersky.
- L'applicazione Endpoint Protection Platform (EPP) è un'applicazione Kaspersky che protegge le risorse e i dati archiviati su di essi da malware e altre minacce.
- Kaspersky Endpoint Agent è un componente del programma installato nelle workstation e nei server dell'infrastruttura IT aziendale. Kaspersky Endpoint Agent monitora continuamente i processi in esecuzione nei computer, le connessioni di rete attive e i file modificati. Nelle versioni recenti delle applicazioni EPP è stato sostituito dalla funzionalità integrata.
- Kaspersky Network Agent è un componente di Kaspersky Security Center che consente l'interazione tra l'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 di tipo Unix e per macOS.
- Kaspersky Security Center è un'applicazione destinata agli amministratori di rete aziendali e ai dipendenti responsabili della protezione delle risorse in un'ampia gamma di organizzazioni.
- Kaspersky Security Network è un'infrastruttura di servizi cloud che fornisce l'accesso alla Knowledge Base online 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 reazioni più rapide da parte delle applicazioni Kaspersky alle minacce, migliora le prestazioni di alcuni componenti della protezione e riduce la probabilità di falsi allarmi.
- Kaspersky Managed Detection and Response (anche denominato MDR) è una soluzione che offre una protezione gestita continua, consentendo alle organizzazioni di individuare le minacce elusive automaticamente e ai team di sicurezza IT di concentrarsi sulle attività critiche che richiedono il loro coinvolgimento.
- Web Console MDR fornisce un'interfaccia Web per la gestione e la manutenzione del sistema di protezione della rete di un'organizzazione client gestita da Kaspersky Managed Detection and Response. Oltre a Web Console MDR è stato aggiunto il plug-in Web di Kaspersky Security Center per consentire la gestione di Kaspersky Managed Detection and Response all'interno di un'unica Administration Console.
- L'API MDR è l'Application Programming Interface per la gestione e il supporto del sistema di protezione della rete di un'organizzazione client gestita da Kaspersky Managed Detection and Response.

Interfacce di Kaspersky Managed Detection and Response

Questa sezione contiene informazioni sulle interfacce utente di Kaspersky Managed Detection and Response.

È possibile utilizzare Kaspersky Managed Detection and Response tramite le seguenti interfacce:

- Portale di Kaspersky Managed Detection and Response (di seguito anche denominato Web Console MDR).

  Web Console MDR è disponibile all'indirizzo https://mdr.kaspersky.com/ dopo aver effettuato l'accesso. Per accedere, utilizzare l'indirizzo e-mail e la password dell'account per il sito Web di Kaspersky creato durante l'attivazione di Kaspersky Managed Detection and Response.

- Sezione **MDR** in Kaspersky Security Center Web Console o in Kaspersky Security Center Cloud Console.

  Per utilizzare Kaspersky Security Center Web Console con Kaspersky Managed Detection and Response, è necessario scaricare e configurare il plug-in MDR in Kaspersky Security Center Web Console. In Kaspersky Security Center Cloud Console il plug-in MDR è preinstallato.

  Per accedere alle funzioni di Kaspersky Managed Detection and Response, in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console fare clic su **Monitoraggio e rapporti** → **MDR**.

Le capacità e le funzioni disponibili in queste interfacce sono sostanzialmente le stesse, ma è consigliabile eseguire alcune attività in una delle interfacce, poiché è disponibile un set più ampio di funzioni o dati. L'interfaccia consigliata è specificata nella descrizione delle attività e degli scenari di utilizzo.

L'interfaccia di Kaspersky Security Center è progettata principalmente per eseguire le seguenti attività:

- Attivazione della soluzione Kaspersky Managed Detection and Response
- Controllo dello stato delle risorse

L'interfaccia di Web Console MDR è progettata principalmente per eseguire le seguenti attività:

- Attività degli addetti alla sicurezza: gestione degli incidenti
- Attività dell'amministratore: gestione degli utenti MDR
- Visualizzazione e gestione delle risorse

Sezione MDR in Kaspersky Security Center

È possibile utilizzare Kaspersky Managed Detection and Response tramite la sezione **MDR** in Kaspersky Security Center Web Console o in Kaspersky Security Center Cloud Console. Per accedere alle funzioni di Kaspersky Managed Detection and Response, in Kaspersky Security Center fare clic su **Monitoraggio e rapporti** → **MDR**.

La sezione **MDR** nell'interfaccia Web di Kaspersky Security Center contiene le seguenti schede:

- **Incidenti**. Contiene il collegamento a Web Console MDR, in cui è possibile gestire gli incidenti.
- **Rapporti**. Contiene l'elenco delle attività di invio dei rapporti e le funzioni per modificare, eliminare o creare un'attività.

- **Impostazioni**. Consente di abilitare le notifiche estese e di modificare la lingua per i dati sugli incidenti, le notifiche e i rapporti.
- **Notifiche**. Consente di abilitare le notifiche tramite e-mail e Telegram.
- **API**. Contiene l'elenco delle connessioni API e le funzioni per gestirle.
- **Tenant**. Contiene l'elenco dei tenant e le funzioni per gestirli.
- **Stati delle risorse MDR**. Contiene gli elenchi delle risorse con malfunzionamenti e di tutte le risorse visualizzate.
- **Per iniziare** (Getting Started). Contiene le istruzioni per l'impostazione della soluzione MDR.
- **Utilizzo di MDR**. Contiene le informazioni sullo stato di attivazione della soluzione, la licenza, l'area per l'archiviazione dei dati di telemetria, il file di configurazione di KPSN e lo stato di accettazione delle condizioni per l'utilizzo.

Inoltre è possibile aggiungere il widget **Risorse MDR per stato** nel riquadro **Monitoraggio e rapporti** → **Dashboard** in Kaspersky Security Center.

Configurazione del plug-in MDR in Kaspersky Security Center

Questa sezione contiene informazioni sulla configurazione iniziale del plug-in MDR in Kaspersky Security Center per l'utilizzo con Kaspersky Managed Detection and Response.

Configurazione del plug-in MDR

Per utilizzare Kaspersky Managed Detection and Response tramite il plug-in MDR, è necessario configurare il plug-in MDR in una delle seguenti applicazioni:

- Kaspersky Security Center Web Console di Kaspersky Security Center Windows
- Kaspersky Security Center Web Console di Kaspersky Security Center Linux
- Kaspersky Security Center Cloud Console

Prerequisiti

Assicurarsi di avere accesso a Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console con le seguenti impostazioni minime:

- Il diritto di accesso in **Lettura** viene concesso per l'area funzionale **Caratteristiche generali: Integrazione delle applicazioni** di Kaspersky Security Center
- Il diritto di accesso **Consenti** è impostato per l'area funzionale **Accesso agli incidenti** di Kaspersky Managed Detection and Response

Fasi

La configurazione procede per fasi:

1. **Download del plug-in MDR**

   Ignorare questa fase se si utilizza Kaspersky Security Center Cloud Console poiché il plug-in MDR è preinstallato in Kaspersky Security Center Cloud Console.

   In Kaspersky Security Center Web Console, scaricare il plug-in MDR selezionando **Kaspersky Managed Detection and Response** nell'elenco dei plug-in disponibili. Per informazioni dettagliate su come ottenere i plug-in Web, fare riferimento alla Guida di Kaspersky Security Center Windows o alla Guida di Kaspersky Security Center Linux.

2. **Impostazione dei diritti di accesso**

   Impostare i diritti di accesso manualmente per ogni utente che deve utilizzare il plug-in MDR o creare automaticamente i ruoli MDR con i diritti di accesso predefiniti facendo clic sul collegamento nel primo passaggio nella scheda **Per iniziare** (Getting Started) del plug-in MDR.

Risultati

Al termine di questo scenario, il plug-in MDR è configurato per l'utilizzo con Kaspersky Managed Detection and Response.

Impostazione dei diritti di accesso in Kaspersky Security Center

È necessario impostare i diritti di accesso per ogni utente di Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console che utilizzerà le funzioni MDR in Kaspersky Security Center. I diritti di accesso dipendono dalle azioni che gli utenti devono essere in grado di eseguire.

È possibile creare automaticamente i ruoli MDR con i diritti di accesso predefiniti facendo clic sul collegamento nel primo passaggio nella scheda **Per iniziare** (Getting Started) della sezione **MDR** di Kaspersky Security Center.

Per impostare i diritti di accesso:

1. In Kaspersky Security Center passare alla sezione **Utenti e ruoli** → **Ruoli** e creare un nuovo ruolo. Per i dettagli su come creare i ruoli, fare riferimento alla Guida di Kaspersky Security Center Windows, alla Guida di Kaspersky Security Center Linux o alla Guida di Kaspersky Security Center Cloud Console.

2. Nella scheda **Diritti di accesso** di un nuovo ruolo impostare il diritto **Consenti** per le aree funzionali seguenti:

   - **Integrazione applicazioni**

     Consente agli utenti di configurare l'interazione tra Kaspersky Security Center e un'altra applicazione o soluzione Kaspersky.

     È necessario impostare il diritto di accesso **Consenti** per l'area funzionale **Integrazione applicazioni** per gli utenti che gestiscono il plug-in MDR. Questo diritto di accesso concede agli utenti i diritti per attivare, configurare, utilizzare e terminare l'utilizzo di Kaspersky Managed Detection and Response.

   - **Accesso agli incidenti**

     È necessario impostare il diritto di accesso **Consenti** per l'area funzionale **Accesso agli incidenti** affinché gli utenti possano accedere alla sezione **MDR** di Kaspersky Security Center. Se per l'area funzionale **Accesso agli incidenti** è impostato il diritto di accesso **Nega**, gli utenti possono visualizzare solo la scheda **Per iniziare** (Getting Started) della sezione **MDR** di Kaspersky Security Center.

   - **Gestione dei tenant**

     Consente agli utenti di creare, visualizzare e modificare i tenant.

   - **Accesso all'API REST**

     Consente agli utenti di gestire Kaspersky Managed Detection and Response tramite l'API REST.

   La tabella seguente mostra il set minimo di diritti di accesso.

   Set minimo di diritti di accesso

Area funzionale	Consenti	Nega
Integrazione applicazioni	—	✓
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	—	✓
Gestione delle reazioni	—	✓
Gestione dei tenant	—	✓
Pianificazione per il riepilogo incidenti	—	✓
Accesso all'API REST	—	✓

3. Assegnare il ruolo creato a tutti gli utenti che utilizzeranno le funzioni MDR in Kaspersky Security Center.

I diritti di accesso verranno impostati.

Visualizzazione e modifica delle impostazioni MDR in Kaspersky Security Center

È possibile visualizzare e modificare le impostazioni del plug-in MDR installato in Kaspersky Security Center.

Per visualizzare e modificare le impostazioni:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Impostazioni**.
2. Se si desidera abilitare le notifiche estese tramite e-mail, attivare l'opzione **Abilita notifiche estese tramite e-mail** e selezionare la casella di controllo per confermare di aver letto e compreso i termini per l'invio delle notifiche estese.
3. È possibile utilizzare l'impostazione **Lingua** per selezionare la lingua inglese o russa per visualizzare rapporti e notifiche.
4. Fare clic sul pulsante **Salva** nella parte inferiore della finestra per salvare le impostazioni.

   Il pulsante **Salva** diventa attivo solo se sono state modificate le impostazioni.

Utilizzo delle funzionalità del plug-in MDR in un Administration Server virtuale

Per utilizzare le funzionalità MDR in Kaspersky Security Center in un Administration Server virtuale:

- Se si utilizza Kaspersky Security Center Windows:
  1. Scaricare il file di configurazione MDR in Kaspersky Security Center Web Console o in MDR Web Console.
  2. In Kaspersky Security Center Web Console, selezionare l'Administration Server (fisico) principale in cui si trova l'Administration Server virtuale.
  3. Abilitare l'interruttore **Kaspersky Private Security Network** nelle proprietà (fisiche) principali di Administration Server.
  4. Fare clic sul pulsante **Seleziona file con impostazioni proxy KSN** e selezionare il file di configurazione MDR scaricato.
- Se si utilizza Kaspersky Security Center Cloud Console:
  1. Attivare Kaspersky Managed Detection and Response nell'Administration Server (fisico) principale.
  2. Nell'Administration Server principale (fisico), fare clic su **Monitoraggio e rapporti** → **MDR**, aprire la scheda **Utilizzo MDR** e assicurarsi che la sezione **KPSN** contenga lo stato e la versione corretti del file di configurazione di KPSN. Esempio di stato e versione corretti:

     ```
     Per inviare i dati di telemetria all'infrastruttura Kaspersky MDR, viene utilizzato
      il file di configurazione di KPSN versione {{version}}
     ```

     Se lo stato del file o la versione non sono corretti, contattare l'Assistenza tecnica.

Utilizzo delle funzionalità MDR in Kaspersky Security Center tramite un server proxy

Se viene utilizzato un server proxy nella rete in cui è in esecuzione Kaspersky Security Center, è necessario impostare due variabili di ambiente con le impostazioni del server proxy per i protocolli HTTP e HTTPS affinché le funzionalità MDR in Kaspersky Security Center funzionino correttamente. Queste variabili di ambiente devono essere impostate nell'host in cui è installato Kaspersky Security Center Web Console.

Le variabili di ambiente hanno il seguente formato:

```
HTTP_PROXY=<protocol>://<proxy_user_name>:<proxy_user_password>@<host>:<port>
```

dove:

- `<protocol>` è http o https.
- `<proxy_user_name>` è il nome utente per l'autorizzazione nel server proxy.
- `<proxy_user_password>` è la password per l'autorizzazione sul server proxy.
- `<host>:<port>` sono il nome o l'indirizzo IP del server proxy e il relativo numero di porta.

  Esempio delle variabili di ambiente:

  ```
  HTTP_PROXY=http://proxy_user_name:proxy_user_password@proxy.domain.com:8080
  HTTPS_PROXY=https://proxy_user_name:proxy_user_password@proxy.domain.com:443
  ```

È possibile impostare le variabili di ambiente in due modi:

- Se si desidera applicare le impostazioni del proxy a tutte le applicazioni nell'host in cui è installato Kaspersky Security Center Web Console, aggiungere queste variabili di ambiente utilizzando il componente **Modifica le variabili di ambiente di sistema** del sistema operativo Windows. Per informazioni sull'utilizzo di questo componente, fare riferimento alla documentazione della versione del sistema operativo in uso.
- Se si desidera applicare queste impostazioni del proxy solo a Kaspersky Security Center Web Console, aggiungere queste variabili di ambiente nel file .env che si trova nella cartella di installazione di Kaspersky Security Center Web Console (per impostazione predefinita, C:\Programmi\Kaspersky Lab\Kaspersky Security Center Web Console\). Se il file .env non è presente nella cartella di installazione, è necessario crearlo.

Dopo aver impostato le variabili di ambiente, è necessario riavviare l'host in cui è installato Kaspersky Security Center Web Console per applicare le modifiche.

Modifica dei certificati per l'utilizzo delle funzioni MDR in Kaspersky Security Center con un server proxy o un software anti-virus

È necessario ridefinire la catena di certificati per la connessione tra Kaspersky Security Center Web Console con il plug-in MDR e l'infrastruttura della soluzione MDR nei seguenti casi:

- Nella rete in cui è in esecuzione Kaspersky Security Center viene utilizzato un server proxy con connessione TLS.
- Il software anti-virus con crittografia del traffico TLS è in esecuzione su un host in cui è installato Kaspersky Security Center Web Console.

Per ridefinire la catena di certificati:

1. Salvare i certificati necessari come file nel computer.

   - Per salvare il file del certificato del traffico di crittografia del software, nell'host con Kaspersky Security Center Web Console aprire https://mdr-ksc.kaspersky.com/ nel browser Chrome, fare clic sull'icona del lucchetto nella barra degli indirizzi accanto all'indirizzo del sito, fare clic su **La connessione è sicura**, quindi su **Certificato valido**, accedere alla scheda **Dettagli** e fare clic sul pulsante **Esporta**. Per le istruzioni relative agli altri browser, fare riferimento alla documentazione di questi browser.

   - Per ottenere il certificato utilizzato per la connessione al server proxy, contattare l'amministratore di rete.

2. Aggiungere i certificati salvati al file con estensione .PEM (ad esempio, KL_Root.pem).

3. Posizionare il file .PEM creato nella cartella di installazione di Kaspersky Security Center Web Console (per impostazione predefinita, C:\Programmi\Kaspersky Lab\ Kaspersky Security Center Web Console\).

4. Aggiungere la variabile di ambiente NODE_EXTRA_CA_CERTS al file .env che si trova nella cartella di installazione di Kaspersky Security Center Web Console. Se il file .env non è presente nella cartella di installazione, è necessario crearlo.

   Esempio della variabile:
   NODE_EXTRA_CA_CERTS="C:\Programmi\ Kaspersky Lab\ Kaspersky Security Center Web Console\KL_Root.pem"

Per applicare le modifiche dopo aver impostato la variabile di ambiente, riavviare l'host in cui è installato Kaspersky Security Center Web Console.

Nascondere e mostrare le funzionalità MDR in Kaspersky Security Center

Per impostazione predefinita, gli elementi dell'interfaccia relativi a Kaspersky Managed Detection and Response vengono visualizzati nell'interfaccia di Kaspersky Security Center. Se non si utilizza Kaspersky Managed Detection and Response, è possibile nascondere le relative funzionalità dall'interfaccia. Successivamente, è possibile modificare le impostazioni dell'interfaccia per mostrare nuovamente gli elementi nascosti.

Per nascondere le funzionalità MDR in Kaspersky Security Center Cloud Console:

1. In Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console passare il cursore del mouse sul nome utente situato nel riquadro sinistro in fondo. Viene visualizzato il menu delle impostazioni dell'interfaccia.

2. Fare clic su **Opzioni interfaccia**.

3. Disattivare o attivare le **funzionalità Mostra MDR**.

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

   Kaspersky Security Center salva il valore di questa opzione solo per l'account utente. Altri utenti possono impostare un valore diverso.

   La sezione **MDR** viene nascosta o mostrata.

Web Console MDR

È possibile utilizzare Kaspersky Managed Detection and Response nell'interfaccia Web denominata Web Console MDR.

La finestra Web Console MDR contiene i seguenti elementi:

- Menu principale nel riquadro sinistro della finestra
- Area di lavoro nel riquadro destro della finestra

Menu principale

Il menu principale contiene le seguenti sezioni:

- **Monitoraggio**. Contiene i widget che forniscono informazioni di riepilogo sugli incidenti, le risorse e le reazioni attivi.
- **Incidenti**. Contiene informazioni dettagliate sugli incidenti e gli strumenti per gestirli.
- **Risorse**. Contiene informazioni dettagliate sulle risorse e gli strumenti per gestirle.
- **Impostazioni**. Contiene le schede per gestire gli account utente, le notifiche, le impostazioni degli incidenti, i rapporti di riepilogo, l'API, i tenant e le impostazioni generali.
- **Informazioni**. Contiene le informazioni sulla soluzione, nonché i collegamenti al Contratto di MDR, all'Accordo di elaborazione dei dati, a questa guida online e al sito Web dell'Assistenza tecnica.

Nella parte inferiore del riquadro sinistro è presente il controllo **Impostazioni account** che consente di accedere alla *guida introduttiva* (Getting Started), modificare la lingua dell'interfaccia, accedere alla pagina del profilo utente e disconnettersi da Web Console MDR.

Area di lavoro

L'area di lavoro mostra le informazioni che si sceglie di visualizzare in Web Console MDR. L'area di lavoro contiene inoltre elementi di controllo che è possibile utilizzare per configurare la modalità di visualizzazione delle informazioni.

Modifica della lingua dell'interfaccia in Kaspersky Security Center

L'interfaccia di MDR in Kaspersky Security Center è disponibile nelle seguenti lingue:

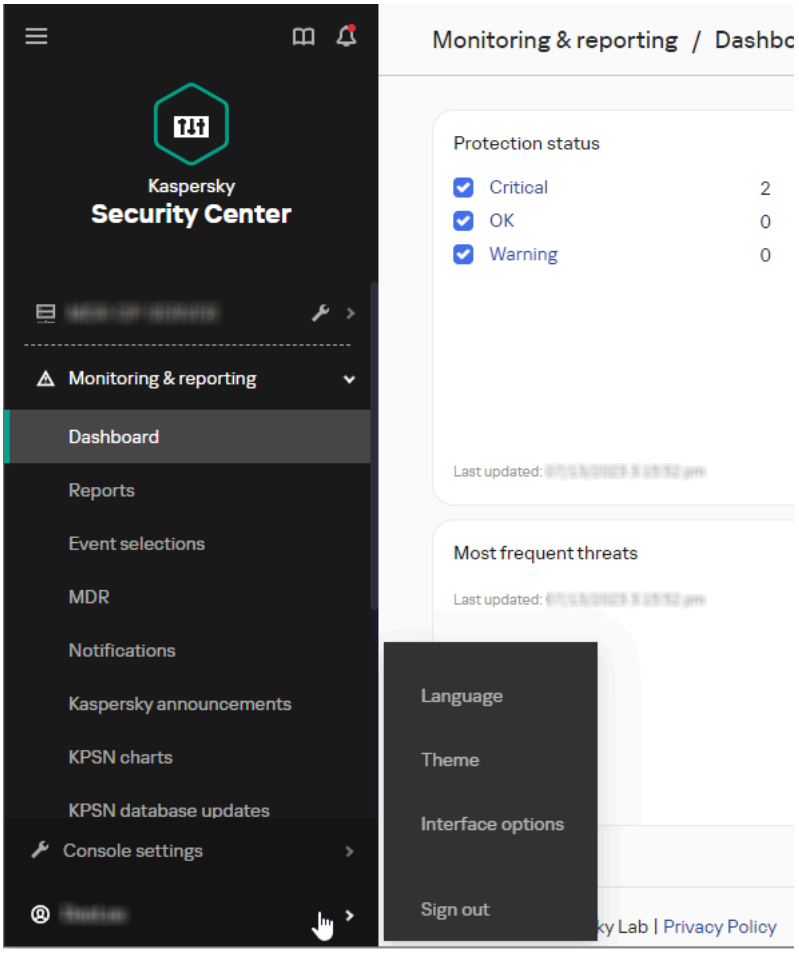
- Inglese
- Russo

- Tedesco
- Spagnolo
- Francese
- Italiano

Per modificare la lingua dell'interfaccia in Kaspersky Security Center:

1. In Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console passare il cursore del mouse sul nome utente situato nel riquadro sinistro in fondo.

   Viene visualizzato il menu delle impostazioni dell'interfaccia.



Modifica della lingua dell'interfaccia in Kaspersky Security Center

2. Fare clic su **Lingua**.

   Verrà visualizzata la sezione **Impostazioni utente**.

3. Nella scheda **Lingua** selezionare la lingua da applicare all'interfaccia di MDR in Kaspersky Security Center.

La lingua verrà cambiata.

È possibile passare a un'altra lingua in qualsiasi momento.

Modifica della lingua per le notifiche e i rapporti in Kaspersky Security Center

In Kaspersky Security Center è possibile selezionare la lingua inglese o russa per visualizzare i dati sugli incidenti, le notifiche e i rapporti.

Per modificare la lingua per le notifiche e i rapporti in Kaspersky Security Center:

1. In Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console fare clic su **MDR** → **Impostazioni**.
2. Nell'area **Lingua** selezionare **russo** o **inglese**.
3. Fare clic sul pulsante **Salva**.

   La lingua verrà cambiata.

   È possibile passare a un'altra lingua in qualsiasi momento.

La modifica della lingua si applica solo alle nuove notifiche e ai nuovi rapporti. Le notifiche e i rapporti già generati mantengono la lingua esistente.

Modifica della lingua dell'interfaccia in Web Console MDR

L'interfaccia di Web Console MDR è disponibile nelle seguenti lingue:

- Inglese
- Russo

Per modificare la lingua dell'interfaccia di Web Console MDR:

1. In Web Console MDR passare alla sezione **Impostazioni account** nella parte inferiore del pannello di sinistra. Questa sezione contiene l'area **Lingua**.
2. Nell'area **Lingua** fare clic sulla lingua da applicare all'interfaccia della console MDR.

La lingua verrà cambiata. È possibile passare a un'altra lingua in qualsiasi momento.

Attivazione di Kaspersky Managed Detection and Response

È consigliabile attivare Kaspersky Managed Detection and Response in Kaspersky Security Center con il plug-in MDR installato, come descritto in questa sezione.

Attivazione di Kaspersky Managed Detection and Response in Kaspersky Security Center

L'attivazione di Kaspersky Managed Detection and Response non è disponibile nell'area di lavoro di prova di Kaspersky Security Center Cloud Console.

Per attivare Kaspersky Managed Detection and Response:

1. Assicurarsi che il plug-in MDR sia installato e configurato in Kaspersky Security Center.
2. In Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console, fare clic su **Monitoraggio e generazione dei rapporti** → **MDR**.
3. Fare clic sul pulsante **Attiva la soluzione**.
4. Kaspersky Managed Detection and Response verifica se la connessione in background tra Kaspersky Security Center Web Console e Administration Server è abilitata e richiede di abilitarla, se necessario.
5. Se non è stato precedentemente creato un Kaspersky Account, crearlo e assicurarsi di confermarlo utilizzando il collegamento di conferma inviato all'indirizzo e-mail.

   Se il Kaspersky Account creato in precedenza (ovvero l'e-mail) è stato utilizzato in precedenza per accedere a Kaspersky Managed Detection and Response, potrebbe essere associato ai dati MDR di un'altra organizzazione e non essere disponibile per l'applicazione di un nuovo codice di attivazione. Per utilizzare il Kaspersky Account esistente per la nuova attivazione, contattare l'Assistenza tecnica.
   Nota: quando il personale dell'Assistenza tecnica rimuove l'associazione del Kaspersky Account esistente con i dati di un'altra organizzazione in MDR, il Kaspersky Account esistente non può più essere utilizzato per accedere ai dati dell'altra organizzazione per cui è stato utilizzato in precedenza.

6. Quando il Kaspersky Account viene attivato, nella sezione **MDR** di Kaspersky Security Center accedere con il proprio Kaspersky Account.

7. Kaspersky Managed Detection and Response controlla se l'account dispone di una licenza corrente per Kaspersky Managed Detection and Response:

   - Se non viene rilevata una licenza corrente, immettere il codice di attivazione ricevuto da Kaspersky, selezionare la regione e fare clic sul pulsante **Attiva**.

     La regione selezionata influisce sulla scelta della lingua che verrà utilizzata per garantire il servizio (russo o inglese) e sulla posizione di archiviazione dei dati di telemetria. Se si selezionano le regioni **Europa** o **Canada**, i dati di telemetria vengono archiviati nel Nord Europa. Se si seleziona **Arabia Saudita**, i dati di telemetria vengono archiviati nel Regno dell'Arabia Saudita. Se si seleziona la **Russia** o altre regioni, i dati di telemetria vengono archiviati in Russia.

   - Se viene rilevata una licenza corrente e si dispone già di tenant, selezionare i tenant a cui avranno accesso gli utenti di questo Administration Server.

   L'abilitazione della connessione in background è necessaria per le prestazioni di Kaspersky Managed Detection and Response.

8. Leggere e accettare i contratti applicabili alla regione selezionata facendo clic sul pulsante **Accetta**.

   Se non si accettano i termini dei contratti applicabili, non sarà possibile utilizzare Kaspersky Managed Detection and Response.

L'attivazione è completa.

Per interrompere l'utilizzo di Kaspersky Managed Detection and Response, fare riferimento alla sezione Interruzione dell'utilizzo di Kaspersky Managed Detection and Response o contattare l'Assistenza tecnica.

Attivazione di Kaspersky Managed Detection and Response in Web Console MDR

Per attivare Kaspersky Managed Detection and Response:

1. Se non è stato precedentemente creato un Kaspersky Account, crearlo e assicurarsi di confermarlo utilizzando il collegamento di conferma inviato all'indirizzo e-mail.

   Se il Kaspersky Account creato in precedenza (ovvero l'e-mail) è stato utilizzato in precedenza per accedere a Kaspersky Managed Detection and Response, potrebbe essere associato ai dati MDR di un'altra organizzazione e non essere disponibile per l'applicazione di un nuovo codice di attivazione. Per utilizzare il Kaspersky Account esistente per la nuova attivazione, contattare l'Assistenza tecnica.
   Nota: quando il personale dell'Assistenza tecnica rimuove l'associazione del Kaspersky Account esistente con i dati di un'altra organizzazione in MDR, il Kaspersky Account esistente non può più essere utilizzato per accedere ai dati dell'altra organizzazione per cui è stato utilizzato in precedenza.

2. Quando il Kaspersky Account è attivato, in MDR Web Console accedere con il proprio Kaspersky Account.

3. Per utilizzare Web Console MDR, inserire il codice di attivazione ricevuto da Kaspersky nel campo corrispondente nella pagina.

4. Leggere e accettare i contratti applicabili nella propria regione facendo clic sul pulsante **Conferma**.

   Se non si accettano i contratti applicabili, non sarà possibile utilizzare Kaspersky Managed Detection and Response.

L'attivazione è completa.

Per interrompere l'utilizzo di Kaspersky Managed Detection and Response, fare riferimento a questo articolo o contattare l'Assistenza tecnica.

Attivazione della soluzione MDR nelle applicazioni Kaspersky

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Per attivare la soluzione MDR nelle applicazioni Kaspersky:

1. Fornire un nuovo codice di attivazione.

2. Attivare la soluzione MDR nelle proprie risorse.

   Per attivare la soluzione MDR per qualsiasi applicazione supportata, è possibile utilizzare un file di configurazione MDR (BLOB). Una volta generato, il file BLOB scade dopo 5 anni, anche se la licenza è perpetua o rilasciata per un periodo più lungo.

   È possibile utilizzare un codice di attivazione o un file chiave per attivare applicazioni e versioni specifiche in base alla licenza. Vedere l'elenco degli argomenti di seguito.

3. Connettere le risorse a Kaspersky Security Network.

   La soluzione MDR può funzionare senza i file di configurazione di KPSN solo con applicazioni e versioni specifiche.

Licenza MDR	Applicazioni supportate per i seguenti metodi: Codice di attivazione File BLOB	Applicazioni supportate per i seguenti metodi: File BLOB
Kaspersky Next Complete Security Kaspersky Symphony MDR Kaspersky Next MDR Optimum Fare riferimento alle: licenze Kaspersky Symphony MDR e NEXT Complete Security	• Kaspersky Endpoint Security for Windows versione 12.6 e successiva • Kaspersky Endpoint Security for Windows 12.8 e versioni successive in modalità Light Agent • Kaspersky Endpoint Security for Windows 12.6 e versioni successive nella modalità Endpoint Detection and Response Agent • Kaspersky Endpoint Security for Linux versione 12.3 e successiva • Kaspersky Endpoint Security for Linux 12.3 e versioni successive in modalità Light Agent • Kaspersky Endpoint Security for Mac 12.2 e versioni successive L'installazione del file BLOB è necessaria se l'organizzazione dispone di più tenant. L'attivazione con un file chiave ha un supporto limitato. È consigliabile utilizzare un codice di attivazione.	• Kaspersky Endpoint Security for Windows 12.5 e versioni precedenti • Kaspersky Endpoint Security for Windows versione 5.2–6.1 in modalità Light Agent • Kaspersky Endpoint Security for Windows versione 12.3–12.5 nella modalità Endpoint Detection and Response Agent • Kaspersky Endpoint Security for Linux 12.2 e versioni precedenti • Kaspersky Endpoint Security for Linux 12.2 e versioni precedenti in modalità Light Agent • Kaspersky Endpoint Security for Mac 12.1 e versioni precedenti Kaspersky Anti Targeted Attack Platform (incluso EDR) versione 4.0–7.1 supporta l'installazione del file di configurazione MDR, che include il file BLOB e il file di configurazione di KPSN. Kaspersky Anti Targeted Attack Platform (incluso EDR) versione 8.0 non richiede il file di configurazione di MDR.

Kaspersky MDR Kaspersky Managed Detection and Response Fare riferimento a: Licenze di Kaspersky MDR	• Kaspersky Endpoint Security for Windows versione 12.6 e successiva • Kaspersky Endpoint Security for Windows 12.8 e versioni successive in modalità Light Agent • Kaspersky Endpoint Security for Windows 12.6 e versioni successive nella modalità Endpoint Detection and Response Agent • Kaspersky Endpoint Security for Linux versione 12.3 e successiva • Kaspersky Endpoint Security for Linux 12.3 e versioni successive in modalità Light Agent • Kaspersky Endpoint Security for Mac 12.2 e versioni successive L'installazione del file BLOB è necessaria se l'organizzazione dispone di più tenant. L'attivazione con un file chiave ha un supporto limitato. È consigliabile utilizzare un codice di attivazione.	• Kaspersky Endpoint Security for Windows 12.5 e versioni precedenti • Kaspersky Endpoint Security for Windows versione 5.2–6.1 in modalità Light Agent • Kaspersky Endpoint Security for Windows versione 12.3–12.5 nella modalità Endpoint Detection and Response Agent • Kaspersky Endpoint Security for Linux 12.2 e versioni precedenti • Kaspersky Endpoint Security for Linux 12.2 e versioni precedenti in modalità Light Agent • Kaspersky Endpoint Security for Mac 12.1 e versioni precedenti Kaspersky Anti Targeted Attack Platform (incluso EDR) versione 4.0–7.1 supporta l'installazione del file di configurazione MDR, che include il file BLOB e il file di configurazione di KPSN.
Componente aggiuntivo Kaspersky MDR Optimum Componente aggiuntivo Kaspersky MDR Expert Kaspersky Managed Detection and Response Basic Add-on Kaspersky Managed Detection and Response Advanced Add-on Kaspersky Managed Detection and Response Prime Add-on Fare riferimento a: Licenze del componente aggiuntivo Kaspersky MDR.	• Kaspersky Endpoint Security for Windows versione 12.6 e successiva • Kaspersky Endpoint Security for Windows 12.8 e versioni successive in modalità Light Agent • Kaspersky Endpoint Security for Windows 12.6 e versioni successive nella modalità Endpoint Detection and Response Agent L'installazione del file BLOB è necessaria se l'organizzazione dispone di più tenant. L'attivazione con un file chiave ha un supporto limitato. È consigliabile utilizzare un codice di attivazione.	• Kaspersky Endpoint Security for Windows 12.5 e versioni precedenti • Kaspersky Endpoint Security for Windows versione 5.2–6.1 in modalità Light Agent • Kaspersky Endpoint Security for Windows versione 12.3–12.5 nella modalità Endpoint Detection and Response Agent Kaspersky Anti Targeted Attack Platform (incluso EDR) versione 4.0–7.1 supporta l'installazione del file di configurazione MDR, che include il file BLOB e il file di configurazione di KPSN.
Kaspersky Managed Detection And Response for Industrial CyberSecurity Fare riferimento a: Licenza dei componenti aggiuntivi di Kaspersky MDR for Industrial CyberSecurity	Kaspersky Industrial CyberSecurity for Nodes Windows 4.0 e versioni successive. L'installazione del file BLOB è necessaria se l'organizzazione dispone di più tenant.	L'installazione del file BLOB è necessaria se l'organizzazione dispone di più tenant. In questo scenario è ancora necessario un codice di attivazione o un file chiave.
Componente aggiuntivo Kaspersky Managed Detection and Response for Embedded Systems Security Fare riferimento a: Licenza del componente aggiuntivo Kaspersky MDR for Embedded Systems Security	Kaspersky Embedded Systems Security for Windows 4.0 e versioni successive. È possibile applicare questa licenza solo se si dispone della licenza MDR Expert. Il file BLOB non viene utilizzato per questa licenza. Per attivare MDR nelle risorse in cui è installato Kaspersky for Embedded Systems Security for Windows, utilizzare la funzionalità di Administration Server per distribuire una chiave di licenza ai dispositivi client automaticamente o tramite l'attività **Attivazione dell'applicazione**.	L'opzione Multi-tenancy non è supportata. Le risorse in cui è installato Kaspersky for Embedded Systems Security Windows vengono assegnate al tenant radice.

Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenze del componente aggiuntivo Kaspersky MDR

Le tabelle seguenti descrivono i metodi di attivazione della soluzione MDR nelle applicazioni Kaspersky per le seguenti licenze:

- Componente aggiuntivo Kaspersky MDR Expert
- Componente aggiuntivo Kaspersky MDR Optimum
- Kaspersky Managed Detection and Response Basic Add-on
- Kaspersky Managed Detection and Response Advanced Add-on
- Kaspersky Managed Detection and Response Prime Add-on

Kaspersky Endpoint Security for Windows

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.10	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Per attivare sia la soluzione Endpoint Detection and Response Optimum sia la soluzione MDR, applicare il codice di attivazione per Endpoint Detection and Response Optimum e un file di configurazione di MDR (BLOB) per la soluzione MDR.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.9	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Per attivare sia la soluzione Endpoint Detection and Response Optimum sia la soluzione MDR, applicare il codice di attivazione per Endpoint Detection and Response Optimum e un file di configurazione di MDR (BLOB) per la soluzione MDR.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.

12.6–12.8	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Per attivare sia la soluzione Endpoint Detection and Response Optimum sia la soluzione MDR, applicare il codice di attivazione per Endpoint Detection and Response Optimum e un file di configurazione di MDR (BLOB) per la soluzione MDR.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.5 e versioni precedenti	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Endpoint Security for Windows nella modalità Endpoint Detection and Response Agent

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.10	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Per attivare sia la soluzione Endpoint Detection and Response Optimum sia la soluzione MDR, applicare il codice di attivazione per Endpoint Detection and Response Optimum e un file di configurazione di MDR (BLOB) per la soluzione MDR.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.9	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB).
12.6–12.8	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB).
12.3–12.5	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Security for Virtualization Light Agent

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
6.3 Kaspersky Endpoint Security for Windows 12.10 o versione successiva in modalità Light Agent	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Per attivare sia la soluzione Endpoint Detection and Response Optimum sia la soluzione MDR, applicare il codice di attivazione per Endpoint Detection and Response Optimum e un file di configurazione di MDR (BLOB) per la soluzione MDR.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
6.2 Kaspersky Endpoint Security for Windows 12.8-12.9 in modalità Light Agent	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Per attivare sia la soluzione Endpoint Detection and Response Optimum sia la soluzione MDR, applicare il codice di attivazione per Endpoint Detection and Response Optimum e un file di configurazione di MDR (BLOB) per la soluzione MDR.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
6.0–6.1 Kaspersky Security for Virtualization Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.
5.2 Kaspersky Security for Virtualization Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.
6.3 Kaspersky Endpoint Security for Linux 12.3 o versione successiva in modalità Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
6.2 Kaspersky Endpoint Security for Linux 12.2 in modalità Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Endpoint Security for Linux

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.3	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.2 e versioni precedenti	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Endpoint Security for Mac

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.2	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.1 e versioni precedenti	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenze Kaspersky MDR

Le tabelle seguenti descrivono i metodi di attivazione della soluzione MDR nelle applicazioni Kaspersky per le seguenti licenze:

- Kaspersky MDR
- Kaspersky Managed Detection and Response

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.10	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.9	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.6–12.8	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Per attivare sia la soluzione Endpoint Detection and Response Optimum sia la soluzione MDR, applicare il codice di attivazione per Endpoint Detection and Response Optimum e un file di configurazione di MDR (BLOB) per la soluzione MDR.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.5 e versioni precedenti	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Endpoint Security for Windows nella modalità Endpoint Detection and Response Agent

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.10	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.9	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB).
12.6–12.8	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB).
12.3–12.5	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Security for Virtualization Light Agent

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
6.3 Kaspersky Endpoint Security for Windows 12.10 o versione successiva in modalità Light Agent	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.

6.2 Kaspersky Endpoint Security for Windows 12.8-12.9 in modalità Light Agent	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Per attivare sia la soluzione Endpoint Detection and Response Optimum sia la soluzione MDR, applicare il codice di attivazione per Endpoint Detection and Response Optimum e un file di configurazione di MDR (BLOB) per la soluzione MDR.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
6.0–6.1 Kaspersky Security for Virtualization Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.
5.2 Kaspersky Security for Virtualization Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.
6.3 Kaspersky Endpoint Security for Linux 12.3 o versione successiva in modalità Light Agent	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
6.2 Kaspersky Endpoint Security for Linux 12.2 in modalità Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Endpoint Security for Linux

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.3	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.2 e versioni precedenti	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Endpoint Security for Mac

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.2	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.1 e versioni precedenti	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenze Kaspersky Symphony MDR e NEXT Complete Security

Le tabelle seguenti descrivono i metodi di attivazione della soluzione MDR nelle applicazioni Kaspersky per le seguenti licenze:

- Kaspersky Symphony MDR
- Kaspersky NEXT Complete Security

Kaspersky Endpoint Security for Windows

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.10	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.9	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.

12.6–12.8	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.5 e versioni precedenti	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Security for Virtualization Light Agent

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
6.0–6.1 Kaspersky Security for Virtualization Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.
5.2 Kaspersky Security for Virtualization Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.
6.3 Kaspersky Endpoint Security for Windows 12.10 o versione successiva in modalità Light Agent	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Light Agent non può essere attivato con la licenza NEXT Complete Security.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
6.2 Kaspersky Endpoint Security for Windows 12.8-12.9 in modalità Light Agent	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione. Light Agent non può essere attivato con la licenza NEXT Complete Security.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.

6.3 Kaspersky Endpoint Security for Linux 12.3 o versione successiva in modalità Light Agent	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
6.2 Kaspersky Endpoint Security for Linux 12.2 in modalità Light Agent	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Endpoint Security for Linux

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.3	È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione o un file chiave nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.2 e versioni precedenti	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Kaspersky Endpoint Security for Mac

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
12.2	L'attivazione della soluzione MDR con un file chiave non è supportata. È necessario disporre di un file di configurazione MDR (BLOB) installato prima di applicare un codice di attivazione nei seguenti casi: • Al momento si utilizzano tenant MDR. • Sono stati creati tenant MDR, anche se sono stati eliminati ulteriori tenant. Non è necessario modificare la configurazione MDR scaduta (BLOB) installata prima quando si applica un codice di attivazione.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN. Per utilizzare la soluzione MDR senza un file di configurazione di KPSN, specificare il codice di attivazione anche se è stato distribuito un file di configurazione di MDR (BLOB). Se i file di configurazione MDR (BLOB) sono già installati nelle risorse e la soluzione MDR è stata attivata prima di gennaio 2024, è necessario scaricare nuovamente e reinstallare i file BLOB: 1. Scaricare il file di configurazione di MDR (BLOB) per il tenant richiesto in Web Console MDR. 2. Configurare i criteri per installare il file BLOB nelle risorse.
12.1 e versioni precedenti	La soluzione MDR può essere attivata con un file di configurazione di MDR (BLOB).	La soluzione MDR può funzionare solo se il file di configurazione di KPSN è installato in Kaspersky Security Center.

Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenza del componente aggiuntivo Kaspersky Managed Detection and Response for Industrial CyberSecurity

La tabella seguente descrive i metodi di attivazione della soluzione MDR nelle applicazioni Kaspersky per la licenza del componente aggiuntivo Kaspersky Managed Detection and Response for Industrial CyberSecurity.

Kaspersky Industrial CyberSecurity for Nodes Windows

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
4.5	Applicare un codice di attivazione o un file chiave per attivare la soluzione MDR. • Se non si utilizzano e non si sono mai creati tenant MDR, non è necessario utilizzare un file di configurazione di MDR (BLOB). Se si utilizzano tenant MDR, è necessario installare un file di configurazione di MDR (BLOB), anche se è scaduto. L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN.	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN.

Attivazione della soluzione MDR nelle applicazioni Kaspersky. Licenza del componente aggiuntivo Kaspersky Managed Detection and Response for Embedded Systems Security

La tabella seguente descrive i metodi per attivare la soluzione MDR nelle applicazioni Kaspersky per la licenza del componente aggiuntivo Kaspersky Managed Detection and Response for Embedded Systems Security.

Kaspersky Embedded Systems Security

Versione applicazione	Metodo di attivazione	Requisito del file di configurazione di KPSN
4.0	Applicare un codice di attivazione o un file chiave per attivare la soluzione MDR. Non è necessario l'utilizzo di un file di configurazione di MDR (BLOB).	L'applicazione supporta l'utilizzo di MDR con e senza file di configurazione di KPSN.

Disattivazione di Kaspersky Managed Detection and Response

Se si desidera smettere di utilizzare Kaspersky Managed Detection and Response, è possibile terminare in modo permanente il relativo utilizzo o sospenderlo in una risorsa particolare.

Interruzione dell'utilizzo di Kaspersky Managed Detection and Response

È possibile terminare manualmente l'utilizzo di Kaspersky Managed Detection and Response se si desidera interromperne l'utilizzo.

Quando si termina l'utilizzo di Kaspersky Managed Detection and Response, Kaspersky Managed Detection and Response interrompe l'invio dei dati di telemetria dalle risorse. Per eliminare i dati sull'organizzazione dall'infrastruttura di Kaspersky Managed Detection and Response, contattare il Servizio di assistenza tecnica.

Per interrompere l'utilizzo di Kaspersky Managed Detection and Response:

1. In Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console passare alla sezione **Dispositivi** → **Criteri e profili**, se si utilizzano le applicazioni EPP che supportano i criteri.

   Se si utilizza un'applicazione EPP che non supporta i criteri, passare alla sezione **Dispositivi** → **Attività**.

   Viene aperto l'elenco dei criteri (o l'elenco delle attività).

2. Fare clic su un criterio o un'attività creati durante la distribuzione di Kaspersky Managed Detection and Response per configurare l'integrazione tra un'applicazione EPP e Kaspersky Managed Detection and Response.

   Verrà visualizzata la finestra delle impostazioni dei criteri (o la finestra delle impostazioni delle attività).

3. Nella scheda **Impostazioni dell'applicazione**, nel riquadro a sinistra, selezionare **Detection and Response**, quindi nel riquadro a destra selezionare **Managed Detection and Response**.

   Verrà visualizzato il riquadro delle impostazioni di **Managed Detection and Response**.

4. Disabilitare l'opzione **Managed Detection and Response abilitato**.

   Il nome dell'opzione diventa **Managed Detection and Response disabilitato**.

5. Salvare le modifiche al criterio o all'attività.

6. Revocare il consenso alle condizioni per l'utilizzo della soluzione MDR.

7. Se si utilizza Kaspersky Security Center Web Console on-premises insieme a Kaspersky MDR, si consiglia inoltre di rimuovere il file di configurazione di KPSN da Kaspersky Security Center Administration Server.

L'utilizzo di Kaspersky Managed Detection and Response viene interrotto.

Sospensione temporanea dell'utilizzo di Kaspersky Managed Detection and Response

Al fine di ottemperare ai termini di utilizzo della soluzione MDR è necessario sospendere l'utilizzo della soluzione sulle risorse se si trovano temporaneamente nel territorio degli Stati Uniti (ad esempio, durante una trasferta di lavoro).

Per sospendere temporaneamente l'utilizzo della soluzione MDR su risorse particolari:

1. In Kaspersky Security Center creare un nuovo gruppo di amministrazione per gestire le risorse per le quali si desidera sospendere l'utilizzo della soluzione MDR. Sarà possibile modificare l'elenco delle risorse in questo gruppo in un secondo momento.

2. Per questo gruppo di amministrazione, creare nuovi criteri delle applicazioni EPP utilizzate per fornire la telemetria MDR dalle risorse, quindi disabilitare l'utilizzo della soluzione MDR e Kaspersky Security Network nelle impostazioni del criterio.

   Per dettagli sulla configurazione dei criteri, fare riferimento agli articoli della guida per una particolare applicazione EPP. Ad esempio, Kaspersky Endpoint Security for Windows aiuta a contenere le istruzioni sulla gestione dei criteri e sulla configurazione dell'integrazione con la soluzione MDR.

3. Spostare le risorse su cui si desidera sospendere l'utilizzo della soluzione MDR per il gruppo di amministrazione creato.

   Il nuovo criterio in cui l'utilizzo della soluzione MDR e Kaspersky Security Network sono disabilitati verrà applicato alle risorse dopo la sincronizzazione. È inoltre possibile forzare manualmente la sincronizzazione.

Per riprendere l'utilizzo di Kaspersky Managed Detection and Response dopo la sospensione:

1. Escludere la risorsa dal gruppo di amministrazione utilizzato per la sospensione.

2. Applicare un criterio regolare in cui l'utilizzo della soluzione MDR sia abilitato e configurato su questa risorsa.

   Le risorse non verranno monitorate dalla soluzione MDR fino a quando non viene applicato un criterio in cui l'utilizzo della soluzione MDR sia abilitato e configurato.

Revoca del consenso alle condizioni per l'utilizzo della soluzione MDR

Se si decide di interrompere l'utilizzo di Kaspersky Managed Detection and Response, revocare il proprio consenso alle condizioni per l'utilizzo della soluzione MDR, quindi disabilitare l'utilizzo di Kaspersky Managed Detection and Response nelle risorse.

Questa funzionalità è disponibile solo se il diritto di accesso **Integrazione applicazioni** è impostato in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console.

Per revocare il consenso alle condizioni per l'utilizzo della soluzione MDR:

1. Nella sezione MDR della finestra di Kaspersky Security Center fare clic sulla scheda **Utilizzo di MDR**.
2. Espandere le **Condizioni per l'utilizzo della soluzione MDR** facendo clic sul relativo nome.
3. Fare clic sul collegamento **Revoca la conferma dell'accettazione delle condizioni per l'utilizzo della soluzione MDR**.
4. Confermare di voler revocare il consenso alle condizioni per l'utilizzo della soluzione MDR.

   Il consenso alle condizioni per l'utilizzo della soluzione MDR è stato revocato.

Se si desidera rimuovere le informazioni sull'organizzazione dall'infrastruttura MDR, contattare il Servizio di assistenza tecnica.

Distribuzione di Kaspersky Managed Detection and Response

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Questa sezione contiene informazioni sulla distribuzione di Kaspersky Managed Detection and Response. Gli scenari di distribuzione variano a seconda delle applicazioni Kaspersky utilizzate nell'infrastruttura.

È innanzitutto necessario eseguire i prerequisiti, che variano a seconda dell'applicazione che si utilizza per la gestione centralizzata della sicurezza di rete:

- Le applicazioni *on-premise* sono Kaspersky Security Center (Administration Console basata su Microsoft Management Console) e Kaspersky Security Center Web Console.
- La soluzione *basata sul cloud* è Kaspersky Security Center Cloud Console.

Ulteriori passaggi di distribuzione di Kaspersky Managed Detection and Response dipendono dalle specifiche applicazioni EPP installate nelle risorse.

Fino all'accettazione dell'Informativa di Kaspersky Security Network, KSN è disabilitato. Inoltre, gli stati delle risorse possono essere di tipo *Critico* in Kaspersky Security Center e si riceverà l'evento *I server KSN non sono disponibili*. L'utilizzo di KSN viene abilitato dopo l'applicazione del criterio in cui l'amministratore accetta i termini di utilizzo di KSN.

Distribuzione on-premise

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Questa sezione contiene gli scenari di distribuzione di Kaspersky Managed Detection and Response che utilizzano applicazioni on-premise Kaspersky Security Center (Administration Console basata su Microsoft Management Console) e Kaspersky Security Center Web Console.

Distribuzione tramite Kaspersky Security Center

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Prerequisiti

- L'infrastruttura IT deve soddisfare i requisiti hardware e software di Kaspersky Managed Detection and Response.

- Per le porte 443 e 1443 in ciascuna risorsa che si desidera proteggere, tutto il traffico non SSL in uscita è consentito e l'ispezione del traffico è disabilitata. Queste porte vengono utilizzate per trasferire i dati di telemetria dalle risorse ai server Kaspersky.

  In caso contrario, se nella rete è presente un server proxy, è necessario specificare le impostazioni del server proxy nelle variabili di ambiente. Fare riferimento al seguente articolo: Utilizzo delle funzioni MDR in Kaspersky Security Center tramite un server proxy. È tuttavia consigliabile inviare la telemetria dalle risorse direttamente senza un server proxy, per garantire un invio più tempestivo dei dati di telemetria e, di conseguenza, una reazione più tempestiva da parte della soluzione MDR alle minacce emergenti.

La distribuzione di Kaspersky Managed Detection and Response utilizzando Kaspersky Security Center procede in più fasi:

1. **Attivazione della soluzione**

   Attivare la soluzione Kaspersky Managed Detection and Response con la propria licenza.

2. **Installazione delle applicazioni EPP**

   Assicurarsi di avere installato le applicazioni EPP che supportano la funzionalità Kaspersky Managed Detection and Response nelle risorse.

3. **Download del file di configurazione MDR**

   Scaricare il file di configurazione MDR per l'organizzazione o scaricare archivi separati per ogni tenant dalla sezione **Tenant** di Web Console MDR.

   A partire da Kaspersky Endpoint Security for Windows 12.6, se si dispone solo del tenant principale e se non si utilizza la soluzione MDR insieme a Kaspersky Endpoint Detection and Response Optimum non è necessario scaricare il file di configurazione MDR. Fare riferimento alle istruzioni fornite per Kaspersky Endpoint Security for Windows nella fase 5.

4. **Configurazione di Kaspersky Private Security Network (KPSN).**

   L'articolo Passaggio della soluzione MDR al funzionamento senza file di configurazione di KPSN descrive come utilizzare la soluzione MDR senza KPSN.

   Se la configurazione non soddisfa i requisiti per il funzionamento senza file di configurazione di KPSN, è necessario configurare KPSN sulle risorse utilizzando il file di configurazione di KPSN dal file di configurazione di MDR.

5. **Integrazione con le applicazioni EPP**

   Eseguire gli scenari di distribuzione specifici dell'applicazione per tutte le applicazioni Kaspersky installate nelle risorse:

   - **Kaspersky Endpoint Security for Windows**

La distribuzione dipende dalla versione di Kaspersky Endpoint Security for Windows installata nelle risorse. Se nell'infrastruttura è installata più di una versione di Kaspersky Endpoint Security for Windows, è possibile eseguire gli scenari per queste versioni in qualsiasi ordine:

Kaspersky Endpoint Security for Windows 12.6 e versioni successive con solo il tenant principale e senza Kaspersky Endpoint Detection and Response Optimum

Se si dispone solo del tenant principale, è possibile saltare il download del file di configurazione MDR e aggiungere e distribuire la chiave di licenza direttamente in Kaspersky Security Center.

Per distribuire Kaspersky Managed Detection and Response in Kaspersky Endpoint Security for Windows 12.6 e versioni successive:

1. Assicurarsi che tutte le risorse appartengano al tenant principale.
2. Verificare se Kaspersky Endpoint Security for Windows in tutte le risorse è stato aggiornato alla versione 12.6 o a una versione successiva.
3. Verificare che il componente Kaspersky Managed Detection and Response sia abilitato in Kaspersky Endpoint Security for Windows su tutte le risorse.
4. Aggiungere una chiave di licenza nell'archivio delle chiavi di licenza in Kaspersky Security Center.
5. Distribuire automaticamente la chiave di licenza alle risorse o utilizzando l'attività *Aggiungi chiave di licenza*.

Per dettagli sull'utilizzo simultaneo delle soluzioni MDR ed EDR Optimum, fare riferimento alla guida di Kaspersky Endpoint Security for Windows.

Kaspersky Endpoint Security for Windows 12.5 e versioni successive con diversi tenant

Se si passa alla funzionalità MDR integrata in Kaspersky Endpoint Security for Windows dopo aver utilizzato la funzionalità di Kaspersky Endpoint Agent, assicurarsi di disabilitare Kaspersky Managed Detection and Response nel criterio di Kaspersky Endpoint Agent dopo aver configurato l'integrazione con Kaspersky Managed Detection and Response nel criterio di Kaspersky Endpoint Security for Windows per tutte le risorse con Kaspersky Endpoint Security for Windows 11.6 e versioni successive.

Se lo stesso criterio viene applicato anche alle risorse con Kaspersky Endpoint Security for Windows 11.5 e versioni precedenti, è necessario creare e configurare un criterio separato per queste risorse prima di mantenerne l'integrazione con Kaspersky Managed Detection and Response tramite il criterio di Kaspersky Endpoint Agent.

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- **Kaspersky Security for Virtualization 5.2 Light Agent**

1. Assicurarsi di avere installato Kaspersky Endpoint Agent nell'ambito di Kaspersky Endpoint Security for Windows.

   Kaspersky Endpoint Agent può essere installato:

   - Durante l'installazione di Kaspersky Endpoint Security for Windows.
   - Dopo l'installazione di Kaspersky Endpoint Security for Windows.

2. Verificare se la versione di Kaspersky Endpoint Agent for Windows è aggiornata e, se necessario, aggiornarla.

   Per Kaspersky Endpoint Security for Windows 11.5 è necessario Kaspersky Endpoint Agent 3.10 o versione successiva.

3. Configurare la soluzione Kaspersky Endpoint Detection and Response Optimum.

4. Creare un criterio per Kaspersky Endpoint Agent.

5. Configurare l'integrazione tra Kaspersky Endpoint Agent for Windows e Kaspersky Managed Detection and Response caricando il file BLOB dal file di configurazione MDR nel criterio di Kaspersky Endpoint Agent.

6. Configurare Kaspersky Endpoint Security for Windows nelle risorse.

   Devono essere abilitati i seguenti componenti:

   - Kaspersky Security Network

     Nelle impostazioni di Kaspersky Security Network selezionare la casella di controllo **Abilita modalità KSN estesa**.

   - Rilevamento del Comportamento

     > L'abilitazione di questi componenti è obbligatoria. In caso contrario, Kaspersky Managed Detection and Response non è utilizzabile, poiché non è possibile inviare i dati di telemetria.

   Kaspersky Managed Detection and Response può inoltre utilizzare i dati dei seguenti componenti:

   - Protezione Minacce Web
   - Protezione Minacce di Posta
   - Firewall

     > L'abilitazione di questi componenti è facoltativa. Se sono disabilitati, Kaspersky Managed Detection and Response continua a inviare i dati di telemetria, ma limitati.

7. Se è stato abilitato Firewall in Kaspersky Endpoint Security for Windows, creare una regola Firewall con le seguenti proprietà:

- Nell'elenco a discesa **Azione** selezionare il valore **Consenti**.
- Nell'elenco a discesa **Direzione** selezionare il valore **In entrata/In uscita**.
- Negli elenchi a discesa **Indirizzi remoti** e **Indirizzi locali** selezionare il valore **Qualsiasi indirizzo**.

  Una volta creata la regola, spostarla in cima all'elenco delle regole.

- Kaspersky Security for Virtualization 5.2 Light Agent
- **Se si utilizza Kaspersky Endpoint Detection and Response Optimum (per Kaspersky Endpoint Security for Windows 11.6 e versioni precedenti)**

1. Assicurarsi di avere installato Kaspersky Endpoint Agent nell'ambito di Kaspersky Endpoint Security for Windows.

   Kaspersky Endpoint Agent può essere installato:

   - Durante l'installazione di Kaspersky Endpoint Security for Windows.
   - Dopo l'installazione di Kaspersky Endpoint Security for Windows.

2. Verificare se la versione di Kaspersky Endpoint Agent for Windows è aggiornata e, se necessario, aggiornarla.

   Per Kaspersky Endpoint Security for Windows 11.5 è necessario Kaspersky Endpoint Agent 3.10 o versione successiva.

3. Configurare la soluzione Kaspersky Endpoint Detection and Response Optimum.

4. Creare un criterio per Kaspersky Endpoint Agent.

5. Configurare l'integrazione tra Kaspersky Endpoint Agent for Windows e Kaspersky Managed Detection and Response caricando il file BLOB dal file di configurazione MDR nel criterio di Kaspersky Endpoint Agent.

6. Configurare Kaspersky Endpoint Security for Windows nelle risorse.

   Devono essere abilitati i seguenti componenti:

   - Kaspersky Security Network

     Nelle impostazioni di Kaspersky Security Network selezionare la casella di controllo **Abilita modalità KSN estesa**.

   - Rilevamento del Comportamento

     > L'abilitazione di questi componenti è obbligatoria. In caso contrario, Kaspersky Managed Detection and Response non è utilizzabile, poiché non è possibile inviare i dati di telemetria.

   Kaspersky Managed Detection and Response può inoltre utilizzare i dati dei seguenti componenti:

   - Protezione Minacce Web
   - Protezione Minacce di Posta
   - Firewall

     > L'abilitazione di questi componenti è facoltativa. Se sono disabilitati, Kaspersky Managed Detection and Response continua a inviare i dati di telemetria, ma limitati.

7. Se è stato abilitato Firewall in Kaspersky Endpoint Security for Windows, creare una regola Firewall con le seguenti proprietà:

- Nell'elenco a discesa **Azione** selezionare il valore **Consenti**.
- Nell'elenco a discesa **Direzione** selezionare il valore **In entrata/In uscita**.
- Negli elenchi a discesa **Indirizzi remoti** e **Indirizzi locali** selezionare il valore **Qualsiasi indirizzo**.

  Una volta creata la regola, spostarla in cima all'elenco delle regole.

- **Piattaforma Kaspersky Anti Targeted Attack**

  Kaspersky Managed Detection and Response consente di analizzare e monitorare i dati ottenuti dalla piattaforma Kaspersky Anti Targeted Attack (KATA).

  L'integrazione con Kaspersky Anti Targeted Attack Platform non è disponibile quando si utilizza una chiave di licenza per l'Arabia Saudita.

  Per configurare l'integrazione tra Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform, è prima necessario ricevere un file di configurazione MDR. È possibile scaricare il file di configurazione MDR dalla pagina **Licensing**. Per informazioni dettagliate su come configurare l'integrazione, fare riferimento alla Guida in linea della piattaforma Kaspersky Anti-Targeted Attack.

  La piattaforma Kaspersky Anti-Targeted Attack non fa parte di Kaspersky Managed Detection and Response. Se si desidera utilizzare la piattaforma Kaspersky Anti Targeted Attack Platform, è necessario acquistarla separatamente.

Se nell'infrastruttura sono installate più applicazioni Kaspersky, è possibile eseguire gli scenari specifici dell'applicazione in qualsiasi ordine.

Attivare la soluzione MDR nelle applicazioni EPP.

L'articolo Componenti necessari per il funzionamento di MDR elenca i componenti EPP che garantiscono l'invio di telemetria dalle risorse

È possibile controllare lo stato delle risorse utilizzando la funzionalità relativa agli stati delle risorse MDR.

Distribuzione tramite Kaspersky Security Center Web Console

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Prerequisiti

- L'infrastruttura IT soddisfa i requisiti hardware e software di Kaspersky Managed Detection and Response.
- Per le porte 443 e 1443 in ciascuna risorsa che si desidera proteggere, il traffico non SSL in uscita è consentito e l'ispezione del traffico è disabilitata. Queste porte vengono utilizzate per il trasferimento dei dati di telemetria dalle risorse ai server KSN elencati nel seguente articolo: Impostazioni di rete per l'interazione con i servizi esterni.

La distribuzione di Kaspersky Managed Detection and Response con l'utilizzo di Kaspersky Security Center Web Console procede per fasi:

1. **Installazione del plug-in MDR**

   Scaricare e configurare il plug-in MDR per la gestione della soluzione in Kaspersky Security Center Web Console.

2. **Attivazione della soluzione**

   Attivare la soluzione Kaspersky Managed Detection and Response con la propria licenza.

3. **Download del file di configurazione MDR**

   Scaricare il file di configurazione MDR per l'organizzazione o scaricare archivi separati per ogni tenant dalla **sezione** Tenant di Web Console MDR o utilizzando il plug-in MDR in Kaspersky Security Center Web Console.

   A partire da Kaspersky Endpoint Security for Windows 12.6, se si dispone solo del tenant principale e se non si utilizza la soluzione MDR insieme a Kaspersky Endpoint Detection and Response Optimum non è necessario scaricare il file di configurazione MDR. Fare riferimento alle istruzioni fornite per Kaspersky Endpoint Security for Windows nella fase 5.

4. **Installazione delle applicazioni EPP**

   Assicurarsi di avere installato le applicazioni EPP che supportano la funzionalità Kaspersky Managed Detection and Response nelle risorse.

5. **Integrazione con le applicazioni EPP**

   Eseguire gli scenari di distribuzione specifici dell'applicazione per tutte le applicazioni Kaspersky installate nelle risorse:

   - **Kaspersky Endpoint Security for Windows**

La distribuzione dipende dalla versione di Kaspersky Endpoint Security for Windows installata nelle risorse. Se nell'infrastruttura è installata più di una versione di Kaspersky Endpoint Security for Windows, è possibile eseguire gli scenari per queste versioni in qualsiasi ordine:

Kaspersky Endpoint Security for Windows 12.6 e versioni successive con solo il tenant principale e senza Kaspersky Endpoint Detection and Response Optimum

Se si dispone solo del tenant principale, è possibile saltare il download del file di configurazione MDR e aggiungere e distribuire la chiave di licenza direttamente in Kaspersky Security Center.

Per distribuire Kaspersky Managed Detection and Response in Kaspersky Endpoint Security for Windows 12.6 e versioni successive:

1. Assicurarsi che tutte le risorse appartengano al tenant principale.
2. Verificare se Kaspersky Endpoint Security for Windows in tutte le risorse è stato aggiornato alla versione 12.6 o a una versione successiva.
3. Verificare che il componente Kaspersky Managed Detection and Response sia abilitato in Kaspersky Endpoint Security for Windows su tutte le risorse.
4. Aggiungere una chiave di licenza nell'archivio delle chiavi di licenza in Kaspersky Security Center.
5. Distribuire automaticamente la chiave di licenza alle risorse o utilizzando l'attività *Aggiungi chiave di licenza*.

Se si dispone solo del tenant principale, è possibile saltare il download del file di configurazione MDR e aggiungere e distribuire la chiave di licenza direttamente in Kaspersky Security Center Web Console.

Per distribuire Kaspersky Managed Detection and Response in Kaspersky Endpoint Security for Windows 12.6 e versioni successive:

1. Assicurarsi che tutte le risorse appartengano al tenant principale.
2. Verificare se Kaspersky Endpoint Security for Windows in tutte le risorse è stato aggiornato alla versione 12.6 o a una versione successiva.
3. Verificare che il componente Kaspersky Managed Detection and Response sia abilitato in Kaspersky Endpoint Security for Windows su tutte le risorse.
4. Aggiungere una chiave di licenza all'archivio delle chiavi di licenza in Kaspersky Security Center Web Console.
5. Distribuire automaticamente la chiave di licenza alle risorse o utilizzando l'attività *Aggiungi chiave di licenza*.

Per dettagli sull'utilizzo simultaneo delle soluzioni MDR ed EDR Optimum, fare riferimento alla guida di Kaspersky Endpoint Security for Windows.

Kaspersky Endpoint Security for Windows 11.6–12.5 e versioni successive con diversi tenant

Se si passa alla funzionalità MDR integrata in Kaspersky Endpoint Security for Windows dopo aver utilizzato la funzionalità di Kaspersky Endpoint Agent, assicurarsi di disabilitare Kaspersky Managed Detection and Response nel criterio di Kaspersky Endpoint Agent dopo aver configurato l'integrazione con Kaspersky Managed Detection and Response nel criterio di Kaspersky Endpoint Security for Windows per tutte le risorse con Kaspersky Endpoint Security for Windows 11.6 e versioni successive.

Se lo stesso criterio viene applicato anche alle risorse con Kaspersky Endpoint Security for Windows 11.5 e versioni precedenti, è necessario creare e configurare un criterio separato per queste risorse prima di mantenerne l'integrazione con Kaspersky Managed Detection and Response tramite il criterio di Kaspersky Endpoint Agent.

Kaspersky Endpoint Security for Windows 11.0–11.5

1. Creare un'attività **Installa l'applicazione in remoto** in Kaspersky Security Center. Nella finestra **Selezione del pacchetto di distribuzione per l'installazione** scegliere il file BAT dal file di configurazione MDR.

2. Eseguire l'attività manualmente o attendere che venga avviata in base alla pianificazione specificata nelle impostazioni dell'attività.

   Assicurarsi che l'attività venga eseguita in tutte le risorse.

3. Configurare Kaspersky Endpoint Security for Windows nelle risorse.

   Devono essere abilitati i seguenti componenti:

   - Kaspersky Security Network

     Nelle impostazioni di Kaspersky Security Network selezionare la casella di controllo **Abilita modalità KSN estesa**.

   - Rilevamento del Comportamento

     > L'abilitazione di questi componenti è obbligatoria. In caso contrario, Kaspersky Managed Detection and Response non è utilizzabile, poiché non è possibile inviare i dati di telemetria.

   Kaspersky Managed Detection and Response può inoltre utilizzare i dati dei seguenti componenti:

   - Protezione Minacce Web
   - Protezione Minacce di Posta
   - Firewall

     > L'abilitazione di questi componenti è facoltativa. Se sono disabilitati, Kaspersky Managed Detection and Response continua a inviare i dati di telemetria, ma limitati.

4. Se è stato abilitato Firewall in Kaspersky Endpoint Security for Windows, creare una regola Firewall con le seguenti proprietà:

   - Nell'elenco a discesa **Azione** selezionare il valore **Consenti**.
   - Nell'elenco a discesa **Direzione** selezionare il valore **In entrata/In uscita**.
   - Negli elenchi a discesa **Indirizzi remoti** e **Indirizzi locali** selezionare il valore **Qualsiasi indirizzo**.

     Una volta creata la regola, spostarla in cima all'elenco delle regole.

Se si utilizza Kaspersky Endpoint Detection and Response Optimum

1. Assicurarsi di avere installato Kaspersky Endpoint Agent nell'ambito di Kaspersky Endpoint Security for Windows.

   Kaspersky Endpoint Agent può essere installato:

   - Durante l'installazione di Kaspersky Endpoint Security for Windows.
   - Dopo l'installazione di Kaspersky Endpoint Security for Windows.

2. Verificare se la versione di Kaspersky Endpoint Agent for Windows è aggiornata e, se necessario, aggiornarla.

   Per Kaspersky Endpoint Security for Windows 11.5 è necessario Kaspersky Endpoint Agent 3.10 o versione successiva.

3. Configurare la soluzione Kaspersky Endpoint Detection and Response Optimum.

4. Creare un criterio per Kaspersky Endpoint Agent.

5. Configurare l'integrazione tra Kaspersky Endpoint Agent for Windows e Kaspersky Managed Detection and Response caricando il file BLOB dal file di configurazione MDR nel criterio di Kaspersky Endpoint Agent.

6. Configurare Kaspersky Endpoint Security for Windows nelle risorse.

   Devono essere abilitati i seguenti componenti:

   - Kaspersky Security Network

     Nelle impostazioni di Kaspersky Security Network, la casella di controllo **Abilita modalità KSN estesa** deve essere selezionata.

   - Rilevamento del Comportamento

     > L'abilitazione di questi componenti è obbligatoria. In caso contrario, Kaspersky Managed Detection and Response non è utilizzabile, poiché non è possibile inviare i dati di telemetria.

   Kaspersky Managed Detection and Response può inoltre utilizzare i dati dei seguenti componenti:

   - Protezione Minacce Web
   - Protezione Minacce di Posta
   - Firewall

     > L'abilitazione di questi componenti è facoltativa. Se sono disabilitati, Kaspersky Managed Detection and Response continua a inviare i dati di telemetria, ma limitati.

7. Se è stato abilitato Firewall in Kaspersky Endpoint Security for Windows, creare una regola Firewall con le seguenti proprietà:

- Nell'elenco a discesa **Azione** selezionare il valore **Consenti**.
- Nell'elenco a discesa **Direzione** selezionare il valore **In entrata/In uscita**.
- Negli elenchi a discesa **Indirizzi remoti** e **Indirizzi locali** selezionare il valore **Qualsiasi indirizzo**.

  Una volta creata la regola, spostarla in cima all'elenco delle regole.

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac
- **Kaspersky Security for Virtualization 5.2 Light Agent**

1. Assicurarsi di avere installato Kaspersky Endpoint Agent nell'ambito di Kaspersky Endpoint Security for Windows.

   Kaspersky Endpoint Agent può essere installato:

   - Durante l'installazione di Kaspersky Endpoint Security for Windows.
   - Dopo l'installazione di Kaspersky Endpoint Security for Windows.

2. Verificare se la versione di Kaspersky Endpoint Agent for Windows è aggiornata e, se necessario, aggiornarla.

   Per Kaspersky Endpoint Security for Windows 11.5 è necessario Kaspersky Endpoint Agent 3.10 o versione successiva.

3. Configurare la soluzione Kaspersky Endpoint Detection and Response Optimum.

4. Creare un criterio per Kaspersky Endpoint Agent.

5. Configurare l'integrazione tra Kaspersky Endpoint Agent for Windows e Kaspersky Managed Detection and Response caricando il file BLOB dal file di configurazione MDR nel criterio di Kaspersky Endpoint Agent.

6. Configurare Kaspersky Endpoint Security for Windows nelle risorse.

   Devono essere abilitati i seguenti componenti:

   - Kaspersky Security Network

     Nelle impostazioni di Kaspersky Security Network selezionare la casella di controllo **Abilita modalità KSN estesa**.

   - Rilevamento del Comportamento

     > L'abilitazione di questi componenti è obbligatoria. In caso contrario, Kaspersky Managed Detection and Response non è utilizzabile, poiché non è possibile inviare i dati di telemetria.

   Kaspersky Managed Detection and Response può inoltre utilizzare i dati dei seguenti componenti:

   - Protezione Minacce Web
   - Protezione Minacce di Posta
   - Firewall

     > L'abilitazione di questi componenti è facoltativa. Se sono disabilitati, Kaspersky Managed Detection and Response continua a inviare i dati di telemetria, ma limitati.

7. Se è stato abilitato Firewall in Kaspersky Endpoint Security for Windows, creare una regola Firewall con le seguenti proprietà:

- Nell'elenco a discesa **Azione** selezionare il valore **Consenti**.
- Nell'elenco a discesa **Direzione** selezionare il valore **In entrata/In uscita**.
- Negli elenchi a discesa **Indirizzi remoti** e **Indirizzi locali** selezionare il valore **Qualsiasi indirizzo**.

  Una volta creata la regola, spostarla in cima all'elenco delle regole.

- Kaspersky Security for Virtualization 5.2 Light Agent
- **Se si utilizza Kaspersky Endpoint Detection and Response Optimum (per Kaspersky Endpoint Security for Windows 11.6 e versioni precedenti)**

1. Assicurarsi di avere installato Kaspersky Endpoint Agent nell'ambito di Kaspersky Endpoint Security for Windows.

   Kaspersky Endpoint Agent può essere installato:

   - Durante l'installazione di Kaspersky Endpoint Security for Windows.
   - Dopo l'installazione di Kaspersky Endpoint Security for Windows.

2. Verificare se la versione di Kaspersky Endpoint Agent for Windows è aggiornata e, se necessario, aggiornarla.

   Per Kaspersky Endpoint Security for Windows 11.5 è necessario Kaspersky Endpoint Agent 3.10 o versione successiva.

3. Configurare la soluzione Kaspersky Endpoint Detection and Response Optimum.

4. Creare un criterio per Kaspersky Endpoint Agent.

5. Configurare l'integrazione tra Kaspersky Endpoint Agent for Windows e Kaspersky Managed Detection and Response caricando il file BLOB dal file di configurazione MDR nel criterio di Kaspersky Endpoint Agent.

6. Configurare Kaspersky Endpoint Security for Windows nelle risorse.

   Devono essere abilitati i seguenti componenti:

   - Kaspersky Security Network

     Nelle impostazioni di Kaspersky Security Network selezionare la casella di controllo **Abilita modalità KSN estesa**.

   - Rilevamento del Comportamento

     > L'abilitazione di questi componenti è obbligatoria. In caso contrario, Kaspersky Managed Detection and Response non è utilizzabile, poiché non è possibile inviare i dati di telemetria.

   Kaspersky Managed Detection and Response può inoltre utilizzare i dati dei seguenti componenti:

   - Protezione Minacce Web
   - Protezione Minacce di Posta
   - Firewall

     > L'abilitazione di questi componenti è facoltativa. Se sono disabilitati, Kaspersky Managed Detection and Response continua a inviare i dati di telemetria, ma limitati.

7. Se è stato abilitato Firewall in Kaspersky Endpoint Security for Windows, creare una regola Firewall con le seguenti proprietà:

- Nell'elenco a discesa **Azione** selezionare il valore **Consenti**.
- Nell'elenco a discesa **Direzione** selezionare il valore **In entrata/In uscita**.
- Negli elenchi a discesa **Indirizzi remoti** e **Indirizzi locali** selezionare il valore **Qualsiasi indirizzo**.

  Una volta creata la regola, spostarla in cima all'elenco delle regole.

- **Piattaforma Kaspersky Anti Targeted Attack**

  Kaspersky Managed Detection and Response consente di analizzare e monitorare i dati ottenuti dalla piattaforma Kaspersky Anti Targeted Attack (KATA).

  L'integrazione con Kaspersky Anti Targeted Attack Platform non è disponibile quando si utilizza una chiave di licenza per l'Arabia Saudita.

  Per configurare l'integrazione tra Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform, è prima necessario ricevere un file di configurazione MDR. È possibile scaricare il file di configurazione MDR dalla pagina **Licensing**. Per informazioni dettagliate su come configurare l'integrazione, fare riferimento alla Guida in linea della piattaforma Kaspersky Anti-Targeted Attack.

  La piattaforma Kaspersky Anti-Targeted Attack non fa parte di Kaspersky Managed Detection and Response. Se si desidera utilizzare la piattaforma Kaspersky Anti Targeted Attack Platform, è necessario acquistarla separatamente.

Se nell'infrastruttura sono installate più applicazioni Kaspersky, è possibile eseguire gli scenari specifici dell'applicazione in qualsiasi ordine.

Attivare la soluzione MDR nelle applicazioni EPP.

L'articolo Componenti necessari per il funzionamento di MDR elenca i componenti EPP che garantiscono l'invio di telemetria dalle risorse.

È possibile controllare lo stato delle risorse utilizzando la funzionalità relativa agli stati delle risorse MDR.

Distribuzione basata su cloud

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

La distribuzione di Kaspersky Managed Detection and Response con l'utilizzo di Kaspersky Security Center Cloud Console procede per fasi:

1. **Attivazione della soluzione**

   Attivare la soluzione Kaspersky Managed Detection and Response con la propria licenza.

2. **Installazione delle applicazioni EPP**

Assicurarsi di avere installato le applicazioni EPP che supportano la funzionalità Kaspersky Managed Detection and Response nelle risorse.

3. **Download del file di configurazione MDR**

   Scaricare il file di configurazione MDR per l'organizzazione o scaricare archivi separati per ogni tenant dalla **sezione** Tenant di Web Console MDR o utilizzando il plug-in MDR in Kaspersky Security Center Cloud Console.

   A partire da Kaspersky Endpoint Security for Windows 12.6, se si dispone solo del tenant principale e se non si utilizza la soluzione MDR insieme a Kaspersky Endpoint Detection and Response Optimum non è necessario scaricare il file di configurazione MDR. Fare riferimento alle istruzioni fornite per Kaspersky Endpoint Security for Windows nella fase 4.

4. **Integrazione con le applicazioni EPP**

   Eseguire gli scenari di distribuzione specifici dell'applicazione per tutte le applicazioni Kaspersky installate nelle risorse:

   - **Kaspersky Endpoint Security for Windows**

La distribuzione dipende dalla versione di Kaspersky Endpoint Security for Windows installata nelle risorse. Se nell'infrastruttura è installata più di una versione di Kaspersky Endpoint Security for Windows, è possibile eseguire gli scenari per queste versioni in qualsiasi ordine:

Kaspersky Endpoint Security for Windows 12.6 e versioni successive con solo il tenant principale e senza Kaspersky Endpoint Detection and Response Optimum

Se si dispone solo del tenant principale, è possibile saltare il download del file di configurazione MDR e immettere il codice di attivazione direttamente in Kaspersky Security Center Cloud Console.

Per distribuire Kaspersky Managed Detection and Response in Kaspersky Endpoint Security for Windows 12.6 e versioni successive:

1. Assicurarsi che tutte le risorse appartengano al tenant principale.
2. Verificare se Kaspersky Endpoint Security for Windows in tutte le risorse è stato aggiornato alla versione 12.6 o a una versione successiva.
3. Verificare che il componente Kaspersky Managed Detection and Response sia abilitato in Kaspersky Endpoint Security for Windows su tutte le risorse.
4. Specificare un nuovo codice di attivazione nell'archivio delle chiavi di licenza in Kaspersky Security Center Cloud Console.
5. Attivare automaticamente Kaspersky Managed Detection and Response sulle risorse oppure utilizzando l'attività *Aggiungi chiave di licenza*.

Per dettagli sull'utilizzo simultaneo delle soluzioni MDR ed EDR Optimum, fare riferimento alla guida di Kaspersky Endpoint Security for Windows.

Kaspersky Endpoint Security for Windows 11.6–12.5 e versioni successive con diversi tenant

Se si passa alla funzionalità MDR integrata in Kaspersky Endpoint Security for Windows dopo aver utilizzato la funzionalità di Kaspersky Endpoint Agent, assicurarsi di disabilitare Kaspersky Managed Detection and Response nel criterio di Kaspersky Endpoint Agent dopo aver configurato l'integrazione con Kaspersky Managed Detection and Response nel criterio di Kaspersky Endpoint Security for Windows per tutte le risorse con Kaspersky Endpoint Security for Windows 11.6 e versioni successive.

Se lo stesso criterio viene applicato anche alle risorse con Kaspersky Endpoint Security for Windows 11.5 e versioni precedenti, è necessario creare e configurare un criterio separato per queste risorse prima di mantenerne l'integrazione con Kaspersky Managed Detection and Response tramite il criterio di Kaspersky Endpoint Agent.

Kaspersky Endpoint Security for Windows 11.3–11.5

1. Creare un'attività **Installa l'applicazione in remoto** https://support.kaspersky.com/KSC/CloudConsole/it-it/175982.htm in Kaspersky Security Center Cloud Console. Nella finestra **Selezione del pacchetto di distribuzione per l'installazione** scegliere il file BAT dal file di configurazione MDR.

2. Eseguire l'attività manualmente o attendere che venga avviata in base alla pianificazione specificata nelle impostazioni dell'attività.

   Assicurarsi che l'attività venga eseguita in tutte le risorse.

3. Configurare Kaspersky Endpoint Security for Windows nelle risorse.

   Devono essere abilitati i seguenti componenti:

   - Kaspersky Security Network

     Nelle impostazioni di Kaspersky Security Network selezionare la casella di controllo **Abilita modalità KSN estesa**.

   - Rilevamento del Comportamento

     > L'abilitazione di questi componenti è obbligatoria. In caso contrario, Kaspersky Managed Detection and Response non è utilizzabile, poiché non è possibile inviare i dati di telemetria.

   Kaspersky Managed Detection and Response può inoltre utilizzare i dati dei seguenti componenti:

   - Protezione Minacce Web
   - Protezione Minacce di Posta
   - Firewall

     > L'abilitazione di questi componenti è facoltativa. Se sono disabilitati, Kaspersky Managed Detection and Response continua a inviare i dati di telemetria, ma limitati.

4. Se è stato abilitato Firewall in Kaspersky Endpoint Security for Windows, creare una regola Firewall con le seguenti proprietà:

   - Nell'elenco a discesa **Azione** selezionare il valore **Consenti**.
   - Nell'elenco a discesa **Direzione** selezionare il valore **In entrata/In uscita**.
   - Negli elenchi a discesa **Indirizzi remoti** e **Indirizzi locali** selezionare il valore **Qualsiasi indirizzo**.

     Una volta creata la regola, spostarla in cima all'elenco delle regole.

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac

- Kaspersky Security for Windows Server

1. Assicurarsi di avere installato Kaspersky Endpoint Agent for Windows nell'ambito di Kaspersky Security for Windows Server.

   Kaspersky Endpoint Agent for Windows può essere installato:

   - Durante l'installazione di Kaspersky Security for Windows Server
   - Dopo l'installazione di Kaspersky Security for Windows Server

2. Verificare se la versione di Kaspersky Endpoint Agent for Windows è aggiornata e, se necessario, aggiornarla.

   Per utilizzare Kaspersky Security Center Cloud Console è necessario Kaspersky Endpoint Agent 3.11.

3. Creare un criterio per Kaspersky Endpoint Agent for Windows tramite Kaspersky Security Center Cloud Console.

4. Per configurare l'integrazione tra Kaspersky Endpoint Agent for Windows e Kaspersky Managed Detection and Response, caricare il file BLOB dal file di configurazione MDR nel criterio.

5. Configurare Kaspersky Security for Windows Server nelle risorse. È possibile eseguire ogni passaggio in locale, in Kaspersky Security for Windows Server su ciascuna delle risorse, oppure globalmente, in Kaspersky Security Center.

   1. Avviare l'attività Utilizzo di KSN.

      L'avvio dell'attività Utilizzo di KSN consente di utilizzare Kaspersky Security Network in Kaspersky Security for Windows Server.

      Nella finestra **Elaborazione dei dati** dell'attività Utilizzo di KSN selezionare tutte le caselle di controllo in tutte le schede.

      Nella finestra **Impostazioni** dell'attività Utilizzo di KSN, nella scheda **Gestione attività**, selezionare la casella di controllo **Esegui in base alla pianificazione**. Nell'elenco a discesa **Frequenza** selezionare il valore **All'avvio dell'applicazione**.

      Nella sottosezione **Utilizzo di KSN** verificare che sia visualizzato un lucchetto chiuso. Il lucchetto chiuso indica che il criterio definisce le impostazioni specificate per le risorse.

   2. Avviare l'attività Sicurezza del traffico.

      L'avvio dell'attività Sicurezza del traffico consente l'elaborazione del traffico Web (incluso il traffico ricevuto tramite e-mail), nonché l'intercettazione e la scansione degli oggetti trasferiti attraverso il traffico Web, allo scopo di rilevare computer noti e altre minacce sul dispositivo protetto.

      Nella finestra **Impostazioni** dell'attività Sicurezza del traffico, nella scheda **Generale**, selezionare il valore **Intercettore driver** dall'elenco a discesa **Modalità attività**.

      Nella finestra **Impostazioni** dell'attività Sicurezza del traffico, nella scheda **Gestione attività**, selezionare la casella di controllo **Esegui in base alla pianificazione**. Nell'elenco a discesa **Frequenza** selezionare il valore **All'avvio dell'applicazione**.

      Nella sottosezione **Sicurezza del traffico** verificare che sia visualizzato un lucchetto chiuso. Il lucchetto chiuso indica che il criterio definisce le impostazioni specificate per le risorse.

   3. Avviare l'attività Controllo avvio applicazioni

L'avvio dell'attività Controllo avvio applicazioni permette il monitoraggio dei tentativi degli utenti di avviare le applicazioni e consente o nega l'avvio di tali applicazioni.

Nella finestra **Impostazioni** dell'attività Controllo avvio applicazioni, nella scheda **Generale**, selezionare le caselle di controllo **Monitora il caricamento dei moduli DLL** e **Consenti le applicazioni considerate attendibili da KSN**.

Nella finestra **Impostazioni** dell'attività Controllo avvio applicazioni, nella scheda **Gestione attività**, selezionare la casella di controllo **Esegui in base alla pianificazione**. Nell'elenco a discesa **Frequenza** selezionare il valore **All'avvio dell'applicazione**.

Nella sottosezione **Controllo avvio applicazioni** verificare che sia visualizzato un lucchetto chiuso. Il lucchetto chiuso indica che il criterio definisce le impostazioni specificate per le risorse.

- **Piattaforma Kaspersky Anti Targeted Attack**

  Kaspersky Managed Detection and Response consente di analizzare e monitorare i dati ottenuti dalla piattaforma Kaspersky Anti Targeted Attack (KATA).

  L'integrazione con Kaspersky Anti Targeted Attack Platform non è disponibile quando si utilizza una chiave di licenza per l'Arabia Saudita.

  Per configurare l'integrazione tra Kaspersky Managed Detection and Response e Kaspersky Anti Targeted Attack Platform, è prima necessario ricevere un file di configurazione MDR. È possibile scaricare il file di configurazione MDR dalla pagina **Licensing**. Per informazioni dettagliate su come configurare l'integrazione, fare riferimento alla Guida in linea della piattaforma Kaspersky Anti-Targeted Attack.

  La piattaforma Kaspersky Anti-Targeted Attack non fa parte di Kaspersky Managed Detection and Response. Se si desidera utilizzare la piattaforma Kaspersky Anti Targeted Attack Platform, è necessario acquistarla separatamente.

Se nell'infrastruttura sono installate più applicazioni Kaspersky, è possibile eseguire gli scenari specifici dell'applicazione in qualsiasi ordine.

5. **Creazione del punto di distribuzione**

   Eseguire le seguenti azioni:

   1. Verificare di disporre di almeno un punto di distribuzione nella rete o configurare un dispositivo nella rete dell'organizzazione come punto di distribuzione. Il punto di distribuzione fungerà da server proxy per i dispositivi che partecipano a Kaspersky Security Network.
   2. **Abilitare il proxy KSN nel punto di distribuzione** nella sezione **Proxy KSN (punti di distribuzione)** delle impostazioni del punto di distribuzione.
   3. Configurare l'**ambito** del punto di distribuzione selezionando il gruppo di amministrazione e/o il percorso di rete.

È possibile controllare lo stato delle risorse utilizzando la funzionalità relativa agli stati delle risorse MDR.

Componenti necessari per il funzionamento di MDR

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Nella tabella seguente sono elencati i componenti necessari per l'invio dei dati di telemetria dalle risorse. Se uno di questi componenti è disabilitato o mancante, Kaspersky Managed Detection and Response interrompe l'invio dei dati di telemetria dalla risorsa.

La modalità Light Agent è supportata dalle seguenti versioni:

- Kaspersky Endpoint Security for Windows versione 12.8 e successiva
- Kaspersky Endpoint Security for Linux versione 12.1 e successiva

Componente	Documentazione
Rilevamento del Comportamento	Kaspersky Endpoint Security for Windows Kaspersky Endpoint Security for Linux Kaspersky Embedded Systems Security for Windows
Protezione Minacce File	Kaspersky Endpoint Security for Windows Kaspersky Endpoint Security for Linux Kaspersky Endpoint Security for Mac Kaspersky Security for Virtualization Light Agent Kaspersky Embedded Systems Security for Windows
System Watcher	Kaspersky Security for Virtualization Light Agent

Nella tabella seguente sono elencati i componenti che influiscono sulla completezza dei dati di telemetria inviati.

Componente	Documentazione
Firewall	Kaspersky Endpoint Security for Windows Kaspersky Endpoint Security for Linux Kaspersky Security for Virtualization Light Agent Kaspersky Embedded Systems Security for Windows
Protezione Minacce di Rete	Kaspersky Endpoint Security for Windows Kaspersky Endpoint Security for Linux Kaspersky Endpoint Security for Mac Kaspersky Embedded Systems Security for Windows
Protezione minacce di posta ed estensione aggiuntiva di Microsoft Office Outlook	Kaspersky Endpoint Security for Windows
Protezione Minacce Web	Kaspersky Endpoint Security for Windows Kaspersky Endpoint Security for Linux Kaspersky Endpoint Security for Mac Kaspersky Security for Virtualization Light Agent
Auto-Difesa del prodotto	Kaspersky Endpoint Security for Windows Kaspersky Security for Virtualization Light Agent Kaspersky Embedded Systems Security for Windows

Informazioni sul file di configurazione MDR

Kaspersky Managed Detection and Response utilizza un file di configurazione MDR per abilitare la soluzione nelle applicazioni EPP Kaspersky per workstation (come Kaspersky Endpoint Security for Windows) installate sulle risorse.

Il file di configurazione MDR viene generato automaticamente da Kaspersky Managed Detection and Response quando si attiva la soluzione tramite un codice di attivazione. Il file di configurazione MDR è un archivio ZIP contenente i seguenti file:

- File di configurazione di KPSN.
- File BLOB (P7) per la distribuzione delle applicazioni EPP che supportano l'integrazione con MDR tramite i criteri di Kaspersky Security Center.

Una volta generato, il file BLOB scade dopo 5 anni, anche se la licenza è perpetua o rilasciata per un periodo più lungo.

Potrebbe non essere necessario il file BLOB (P7) nelle seguenti condizioni:

> Anche se non si utilizza il file di configurazione MDR, è necessario attivare la soluzione tramite Web Console MDR o tramite il Plug-in MDR in Kaspersky Security Center.

- Si stanno utilizzando solo le seguenti applicazioni EPP:
  - Kaspersky Endpoint Security for Windows 12.6 o versione successiva
  - Kaspersky Endpoint Security for Windows 12.8 o versione successiva in modalità Light Agent
  - Kaspersky Endpoint Security for Linux 12.3 o versione successiva
  - Kaspersky Endpoint Security for Linux 12.3 o versione successiva
  - Kaspersky Endpoint Security for Mac 12.2 o versione successiva
- L'organizzazione utilizza solo il tenant radice e non ha mai creato tenant aggiuntivi.
- Non si utilizza la soluzione Kaspersky Endpoint Detection and Response Optimum contemporaneamente alla soluzione Kaspersky MDR. Per i dettagli, fare riferimento alla sezione Attivazione della soluzione MDR nelle applicazioni Kaspersky.

In questo caso Kaspersky Endpoint Security for Windows applica la licenza di Kaspersky Security Center. Se si utilizzano tenant diversi dal tenant radice, è necessario scaricare il file di configurazione MDR per ogni tenant.

Scaricare il file di configurazione MDR e utilizzarlo in base alle istruzioni per le applicazioni EPP installate nelle risorse:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Mac

Download del file di configurazione MDR in Kaspersky Security Center

Per scaricare il file di configurazione MDR in Kaspersky Security Center:

1. In Kaspersky Security Center Web Console o in Kaspersky Security Center Cloud Console fare clic su **MDR** nel riquadro di sinistra, quindi fare clic sulla scheda **Licenze**.
2. Selezionare la colonna **Archivio per la configurazione delle risorse** e fare clic su **Scarica** per scaricare il file di configurazione MDR per una licenza corrente.

Download del file di configurazione MDR in Web Console MDR

Per scaricare il file di configurazione di MDR per il tenant radice in Web Console MDR:

1. In Web Console MDR passare alla voce di menu **Impostazioni**.
2. Fare clic sulla scheda **Licensing**.
3. Nella colonna **Archivio configurazioni**, fare clic su **Scarica** per la licenza.

Per scaricare il file di configurazione di MDR per qualsiasi tenant in Web Console MDR:

1. In Web Console MDR passare alla voce di menu **Impostazioni**.
2. Fare clic sulla scheda **Tenant**.
3. Fare clic sulla riga con il tenant per il quale si desidera scaricare il file di configurazione di MDR.

   Verrà visualizzata la sezione **Impostazioni tenant**.
4. Fare clic sul pulsante **Scarica**.

Gestione delle licenze

Questa sezione tratta gli aspetti principali delle licenze della soluzione Kaspersky Managed Detection and Response.

Confronto dei livelli delle licenze commerciali

Il set di funzionalità disponibili in Kaspersky Managed Detection and Response dipende dal livello della licenza commerciale (vedere la tabella seguente).

Confronto dei livelli della licenza commerciale Kaspersky Managed Detection and Response

Funzionalità	MDR / MDR Expert	MDR Optimum*	MDR Basic*	MDR Advanced*	MDR Prime*
Monitoraggio, rilevamento e gestione degli incidenti 24 ore su 24, 7 giorni su 7	✓	✓	✓	✓	✓
Ricerca automatica delle minacce	✓	✓	✓	✓	✓
Playbook di reazione e reazione automatica agli incidenti	✓	✓	✓	✓	✓
Controllo dell'integrità della sicurezza e visibilità delle risorse	✓	✓	✓	✓	✓
Web Console MDR Kaspersky con dashboard e report	✓	✓	✓	✓	✓
Possibilità di ricevere informazioni avanzate sugli incidenti	✓	✓	✓	✓	✓
Periodo di conservazione della cronologia degli incidenti	1 anno	1 anno	1 anno	1 anno	1 anno
Periodo di conservazione dei dati non elaborati	3 mesi	1 mese	1 mese	3 mesi	3 mesi
Ricerca delle minacce gestite e indagine sugli incidenti	✓	—	—	✓	✓
Assistenza completa da parte di esperti per la gestione degli incidenti	✓	—	—	✓	✓
Accesso a Kaspersky Threat Intelligence Portal	✓	—	—	✓	✓
API per l'esportazione dei dati Kaspersky MDR	✓	—	—	✓	✓
I clienti possono creare un incidente personalizzato per l'elaborazione da parte della soluzione MDR**	✓	—	—	✓	✓
Archiviazione localizzata dei dati e gruppi di lavoro	—	—	✓	✓	✓
Multi-tenancy	✓	✓	✓	✓	✓
Aggiunta e modifica di commenti agli incidenti	✓	✓	✓	✓	✓

Funzionalità	MDR / MDR Expert	MDR Optimum*	MDR Basic*	MDR Advanced*	MDR Prime*
Aggiunta e modifica di allegati agli incidenti	✓	✓	✓	✓	✓
Indagine avanzata sugli incidenti: analisi per stabilire il background, le circostanze e il meccanismo di attacco dettagliato	—	—	—	✓ I clienti non possono scegliere gli incidenti per l'indagine avanzata, non c'è alcun tempo di risposta agli incidenti garantito	✓ I clienti possono scegliere gli incidenti per l'indagine avanzata (entro il limite di tempo acquistato), c'è un tempo di risposta agli incidenti garantito

*Questo livello è disponibile solo per alcune aree geografiche e potrebbe non essere disponibile per l'acquisto da parte di nuovi clienti. Contattare il provider della soluzione Kaspersky Managed Detection and Response per informazioni dettagliate sui livelli di licenza commerciale disponibili.

**La soluzione Kaspersky Managed Detection and Response garantisce l'elaborazione di tre richieste a settimana in linea con gli obiettivi di prestazione della soluzione. Il numero di richieste elaborate in linea con gli obiettivi di prestazione della soluzione aumenta proporzionalmente: ogni 10.000 endpoint connessi, il numero delle richieste aumenta di 1.

Informazioni sulla licenza

Una *licenza* concede per un determinato periodo di tempo il diritto di utilizzare l'applicazione, in conformità con il documento Termini e condizioni.

È possibile utilizzare una sola licenza in Web Console MDR e nel plug-in MDR versione 2.4.1 e precedenti. Quando si inserisce un nuovo codice di attivazione, questo sostituisce quello precedente.

A partire dalla versione 2.4.2 del plug-in MDR, è possibile utilizzare più licenze MDR contemporaneamente.

Una licenza consente di usufruire dei seguenti tipi di servizi:

- Utilizzo dell'applicazione in conformità con il documento Termini e condizioni
- Come ottenere assistenza tecnica

L'ambito dei servizi e il periodo di validità dipendono dal tipo di licenza con cui è stata attivata l'applicazione.

Sono disponibili i seguenti tipi di licenza:

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

  Una licenza di prova in genere è utilizzabile per un periodo di tempo limitato. Alla scadenza della licenza di prova, tutte le funzionalità di Kaspersky Managed Detection and Response vengono disabilitate. Per continuare a utilizzare l'applicazione, è necessario acquistare una licenza commerciale.

  È possibile attivare l'applicazione con la licenza di prova solo una volta.

- *Commerciale* - Una licenza a pagamento fornita con l'acquisto dell'applicazione.

  Alla scadenza della licenza commerciale, l'applicazione continua a essere eseguita con funzionalità limitate (non viene fornita la telemetria). Per continuare a utilizzare tutte le funzionalità di Kaspersky Managed Detection and Response, è necessario rinnovare la licenza commerciale.

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

- *Abbonamento* - Una licenza a pagamento che consente l'utilizzo dell'applicazione per un periodo di fatturazione mensile o annuale, con rinnovo automatico, fino all'annullamento o alla scadenza.

  La licenza in abbonamento può essere di due tipi:

  - *Limitata* - Rinnovata automaticamente alla fine di ogni periodo di fatturazione fino alla data di scadenza definita.

  - *A tempo indeterminato* - Rinnovata automaticamente alla fine di ogni periodo di fatturazione fino alla cancellazione da parte del cliente.

  È possibile gestire la licenza in abbonamento tramite Kaspersky License Management Portal (LMP).

  Se si modifica l'ambito della licenza, ad esempio il numero di risorse, i dettagli della licenza vengono aggiornati in Web Console MDR entro 24 ore.

  Alla scadenza o in caso di annullamento della licenza in abbonamento, l'applicazione continua a essere eseguita con funzionalità limitate (non viene fornita la telemetria). Per continuare a utilizzare tutte le funzionalità di Kaspersky Managed Detection and Response, è necessario rinnovare la licenza in abbonamento.

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

La licenza di Kaspersky Managed Detection and Response consente anche l'utilizzo della soluzione Kaspersky Endpoint Detection and Response Optimum. La soluzione diventa disponibile in una risorsa dopo aver configurato l'integrazione tra Kaspersky Managed Detection and Response e Kaspersky Endpoint Agent.

Informazioni sul codice di attivazione

Il *codice di attivazione* è una sequenza univoca di 20 lettere e numeri. È necessario immettere un codice di attivazione per attivare Kaspersky Managed Detection and Response. Si riceverà il codice di attivazione all'indirizzo e-mail fornito al momento dell'acquisto di Kaspersky Managed Detection and Response.

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

Se è stato smarrito il codice di attivazione, contattare il partner Kaspersky da cui è stata acquistata la licenza.

Fornire un nuovo codice di attivazione

Attivazione iniziale di Kaspersky Managed Detection and Response

Fare riferimento a questi articoli:

- Attivazione di Kaspersky Managed Detection and Response in Kaspersky Security Center (consigliato)
- Attivazione di Kaspersky Managed Detection and Response in Web Console MDR

Inserimento di un nuovo codice di attivazione

È necessario fornire un nuovo codice di attivazione per Kaspersky Managed Detection and Response, ad esempio quando si desidera aggiornare la soluzione o quando è necessario rinnovare la licenza in scadenza.

Questa funzionalità è disponibile solo se il diritto di accesso **Integrazione applicazioni** è impostato in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console.

Per informazioni dettagliate su come gestire più licenze in Kaspersky Managed Detection and Response in Kaspersky Security Center con il plug-in MDR 2.4.2 e versioni successive, fare riferimento a questo articolo: Gestione delle licenze in Kaspersky Security Center.

È possibile rinnovare la licenza corrente in Web Console MDR se scade a breve. Il ruolo **Amministratore MDR** è obbligatorio.

Se la soluzione MDR è stata attivata con un codice di attivazione, è necessario utilizzare il plug-in MDR per Kaspersky Security Center per rinnovare la licenza. L'utilizzo di Web Console MDR per il rinnovo della licenza in questo scenario interrompe l'invio della telemetria dalle risorse.

È consigliabile utilizzare il plug-in MDR per Kaspersky Security Center per immettere un nuovo codice di attivazione.

Per immettere un nuovo codice di attivazione per Kaspersky Managed Detection and Response in Kaspersky Security Center con il plug-in MDR:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Licensing**.
2. Fare clic sul pulsante **Immettere un nuovo codice di attivazone** e immettere il codice di attivazione nel pannello visualizzato.
3. Selezionare i tenant a cui avranno accesso gli utenti di questo Administration Server.

   Verrà applicato il nuovo codice di attivazione. Kaspersky Managed Detection and Response funziona con la licenza fornita.

Per sostituire il codice di attivazione corrente con uno nuovo in Web Console MDR:

1. Fare clic sulla scheda **Licensing**.
2. Fare clic sul collegamento **Immettere un nuovo codice di attivazione**.
3. Immettere un nuovo codice di attivazione e fare clic su **Continua**.
4. Selezionare l'area geografica e fare clic su **Conferma e attiva**.

Gestione delle licenze in Kaspersky Security Center

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Se l'organizzazione dispone di licenze correnti, è possibile gestirle solo in Kaspersky Security Center.

Per la gestione delle licenze, è necessario il ruolo **Amministratore MDR**.

Per visualizzare le licenze:

Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Licensing**.

Viene visualizzato l'elenco **Licenze nell'organizzazione**. Nel pannello superiore sono elencate le informazioni generali sulle licenze:

- Regione
- Livello Licenza commerciale
- Numero totale e limite delle risorse connesse

La scheda **Attiva** mostra solo le licenze correnti. Fare clic sulla scheda **Tutto** per visualizzare tutte le licenze nella propria organizzazione.

Nella tabella sono riportate le seguenti informazioni sulle licenze:

- **Nome licenza**

  Nome della licenza che include dettagli come il livello della licenza e il limite delle risorse.

- **Limite/risorse connesse**

  Numero di risorse che utilizzano questa licenza e limite.

  Quando viene superato, il limite di risorse per la licenza viene evidenziato in rosso.

  Questo numero non include gli host con file di configurazione BLOB creati prima del 1° gennaio 2024. Per risolvere questo problema, aggiornare il file BLOB nelle impostazioni del tenant e applicarlo alle risorse del tenant. Per maggiori dettagli, fare riferimento al seguente argomento: Informazioni sul file di configurazione MDR.

- **ID**

  Identificativo della licenza.

- **Data di attivazione**

- **Data di scadenza**

  La data di scadenza della licenza è evidenziata in rosso se la licenza è scaduta o scade entro 14 giorni o prima.

- **Stato**

  Uno dei seguenti stati:
  - Attuale
  - Scaduto
  - Rifiutato
  - Non utilizzato
  - Sostituito

- **Nome del cliente**

  Nascosto per impostazione predefinita. È possibile abilitare questa colonna nel menu della tabella.

Per scaricare un file CSV che mostra le licenze in base ai tenant (plug-in MDR versione 2.4.2):

Nella scheda **Corrente**, fare clic su **Esporta in base ai tenant in CSV**.

Il file CSV include la distribuzione delle risorse in base al tenant per ciascuna licenza.

Per visualizzare le licenze in base ai tenant (plug-in MDR versione 2.5.0 o successiva),

Nella scheda **Corrente** fare clic su **Visualizza l'utilizzo delle licenze in base al tenant**.

La tabella mostra la distribuzione delle risorse in base al tenant per ogni licenza.

Per scaricare il file di configurazione MDR per una licenza:

Selezionare la colonna **Archivio per la configurazione delle risorse** e fare clic su **Scarica**.

Per immettere un nuovo codice di attivazione:

Fare clic sul pulsante **Immettere un nuovo codice di attivazone** e immettere il codice di attivazione nel pannello visualizzato.

Il livello di licenza e l'area geografica della nuova licenza devono corrispondere al livello di licenza e all'area geografica degli altri codici di attivazione nell'organizzazione.

Per rimuovere un codice di attivazione:

1. Individuare la colonna **Azioni** e fare clic sull'icona .
2. Nella finestra che si apre, confermare l'eliminazione del codice di attivazione.

   Lo stato della licenza cambia in **Non utilizzato**. È possibile reimmettere il codice di attivazione eliminato.

Risoluzione dei problemi di licensing

Se è stata attivata la soluzione MDR nelle risorse e la sezione Licensing in Web Console MDR mostra meno risorse connesse alla soluzione MDR, fare riferimento al seguente elenco di possibili cause e alle relative soluzioni.

Sono in uso più licenze MDR

Soluzione:

Attivare tutte le licenze MDR nel plug-in MDR. Web Console MDR non supporta l'attivazione di più licenze MDR.

La soluzione MDR è stata attivata nelle risorse prima dell'1 gennaio 2024 utilizzando il file di configurazione MDR (BLOB)

Soluzione 1:

1. Scaricare un nuovo file di configurazione MDR (BLOB):
2. Applicare il nuovo file di configurazione MDR (BLOB) alle risorse.

Soluzione 2:

Applicare un codice di attivazione per attivare la soluzione MDR nelle risorse.

Alcune risorse utilizzano Kaspersky Endpoint Security for Windows 12.9 o versioni precedenti e la soluzione MDR in tali risorse viene attivata con un file chiave

Soluzione:

Applicare un codice di attivazione per attivare la soluzione MDR nelle risorse. L'attivazione con un file chiave in tali risorse ha un supporto limitato e non è consigliata.

Trasmissione dei dati

Per il corretto funzionamento di componenti di Kaspersky Managed Detection and Response, è necessario che Kaspersky elabori i dati dell'utente. I componenti non inviano dati senza l'autorizzazione dell'amministratore di Kaspersky Managed Detection and Response.

L'elenco dei dati dell'utente dipende dalla regione in cui viene utilizzata la soluzione. Per la regione dell'utente, l'elenco dei dati degli utenti potrebbe differire da quello elencato in questa sezione.

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

Elenco dei dati sugli eventi che si verificano sui dispositivi dell'Utente

Al fine di facilitare il rilevamento di nuove e complesse minacce per la sicurezza dei dati e le loro fonti, ridurre il rischio di accessi non autorizzati e adottare misure tempestive per aumentare la protezione dei dati archiviati ed elaborati dal Cliente sul suo computer, il Cliente accetta di fornire automaticamente le seguenti informazioni allo scopo di ricevere il Servizio:

- Data di installazione e attivazione del software; nome completo e versione del software, incluse le informazioni sugli aggiornamenti installati e sulla lingua di localizzazione del software.
- Informazioni sul software installato sul computer, inclusi la versione del sistema operativo e la data del download e degli aggiornamenti installati, gli oggetti kernel, i driver, i servizi, le voci di avvio automatico, i programmi che vengono automaticamente avviati in concomitanza a vari eventi di sistema (ad esempio, avvio del sistema operativo, accesso utente e così via), oltre che le configurazioni, le estensioni browser, le estensioni di Microsoft Internet Explorer, le estensioni del sistema di stampa, le estensioni di Esplora risorse, le estensioni della shell del sistema operativo, le checksum degli oggetti caricati (MD5), gli elementi di gestione installazione, le applicazioni del pannello di controllo, le versioni del browser e del client di posta elettronica.
- Informazioni sulle autorizzazioni del file system, il bit effettivo per le autorizzazioni del file system, le versioni delle autorizzazioni del file system, le variabili di ambiente e i nomi delle chiamate di sistema.
- Informazioni sulle autorizzazioni ereditate per un file di sistema.
- Informazioni sul nome del computer, gli indirizzi IP, i gateway predefiniti, gli indirizzi MAC e l'hardware, tra cui un checksum del numero di serie del disco rigido, gli ultimi 12 byte dell'ID di protezione del computer (SID) e l'identificatore di zona di protezione contenuto nello stream di dati NTFS.
- Informazioni sugli strumenti software utilizzati per risolvere i problemi del software installato sul computer dell'Utente, o per modificarne la funzionalità, inoltre i codici restituiti ricevuti dopo l'installazione di ogni parte del software.
- Informazioni sullo stato della protezione anti-virus del computer, comprese le versioni, le date di rilascio e le volte in cui sono stati utilizzati i database anti-virus, le statistiche sugli aggiornamenti e i collegamenti con i servizi di Kaspersky Lab, gli identificatori processo, gli identificatori e le versioni dei componenti software che eseguono la scansione, i contrassegni che denotano l'ambiente di test interno Kaspersky, i codici di errore primari per un evento specifico, i codici di errore secondari per un evento specifico e i numeri ordinali degli eventi.
- Licenza corrente e numero di serie dei prodotti AO Kaspersky Lab, nomi e versioni di questi prodotti. Identificatori delle installazioni dei prodotti AO Kaspersky Lab e descrizione del client dal file di informazioni sulla licenza.

- Informazioni sugli account utente del Cliente: nome dell'account utente, nome dell'utente, identificatore del sistema operativo, informazioni di accesso, privilegi, appartenenze a gruppi, tipi di sessioni di accesso al sistema, nome del pacchetto di autenticazione, nomi di dominio, nomi DNS utilizzati per le sessioni di accesso al sistema di autenticazione, nome server utilizzato per l'autenticazione, nome principale utente (UPN) per l'account e SID.

- Contenuto completo dei log del sistema operativo.

- Informazioni sui sistemi di chiamata.

- Informazioni sui rilevamenti dai programmi AO Kaspersky Lab che supportano Kaspersky Managed Detection and Response.

- Informazioni sulle e-mail ricevute, inclusi: indirizzi e-mail del mittente e del destinatario, oggetto, informazioni sugli allegati: nome del file allegato, dimensione, hash (MD5), risultati dell'analisi del formato del file.

- Informazioni sulle coordinate dell'area di schermo in cui è stato eseguito lo screenshot.

- Informazioni sulle connessioni di rete, inclusi: indirizzi IP e le porte del mittente e del destinatario, indici di zona IPv6, informazioni sulla direzione della connessione di rete (in entrata/in uscita), tipi e maschere delle query DNS effettuate, codici di errore per un'operazione di query DNS, risposta a una query DNS e informazioni sul server DNS richiesto.

- Dati e metodi di connessione HTTP, inclusi: indirizzi Web visitati, URL di riferimento, agenti utente e dati del protocollo di autenticazione di rete: hash MD5 dei dati per l'autenticazione Kerberos, nome account o computer, nome dell'area di autenticazione Kerberos a cui appartiene il nome server, dominio a cui appartiene il nome client, UPN per l'account, pacchetto di crittografia utilizzato per il ticket Kerberos, maschera di contrassegno per il ticket Kerberos in formato esadecimale, ora di emissione del ticket Kerberos, ora di scadenza del ticket Kerberos, data di scadenza del ticket (dopo la quale il ticket non può essere rinnovato) e nome del controller di dominio utilizzato per emettere il ticket Kerberos.

- Informazioni sui protocolli a livello di applicazione: dimensione richiesta di ricerca LDAP, filtro richiesta di ricerca LDAP, nome univoco della richiesta di ricerca LDAP, elenco di attributi per la richiesta di ricerca LDAP.

- Informazioni su .NET: nome completo della build .NET scaricata, flag dell'assembly della build .NET scaricata, flag del modulo .NET scaricato, nome del dominio della build .NET scaricata, moduli per lo stub MSIL generato, informazioni sul metodo gestito: spazio dei nomi, nome e firma del metodo gestito di interoperabilità, firma del metodo nativo, firma dello stub del metodo.

- Le informazioni sui file vengono elaborate all'interno del sistema operativo: nome e percorso del file, dimensioni, attributi, tipi di file e oggetti, risultati dell'analisi del formato del file, checksum (MD5), indirizzo Web di download del file, indirizzo e-mail e oggetto dell'e-mail del mittente del file, contenuto del file system della struttura VERSIONINFO dei metadati del file, informazioni sul publisher (se il file è firmato), ID utente del proprietario del file, ID del gruppo dei proprietari del file, marca temporale dell'ultimo accesso al file e dell'ultima modifica dei metadati del file, creazione del file, maschere dei flag di verifica della firma digitale, marche temporali e codici delle operazioni su file e oggetti, numero di avvii dei file eseguibili, identificatore del formato del file, percorso completo dell'oggetto e del relativo container, contenuto del file di esecuzione automatica, nome e percorso del file della risorsa di rete remota a cui si sta eseguendo l'accesso.

- Contenuto della directory \etc\.

- Dati di output del comando.

- Dati audit: risultato dell'operazione, descrizione dell'operazione, tipo di evento e utente dell'operazione.

- Informazioni sul processo: identificatore del processo (PID), tracciamento delle chiamate del processo, informazioni sul file eseguibile del processo e sulla sua riga di comando, informazioni sul processo principale, hash MD5 del codice di errore di calcolo del file eseguibile, codici di errore primari, informazioni di integrità del processo, informazioni di accesso alla sessione, riga di comando, argomenti della riga di comando per il processo, variabili d'ambiente per il processo di destinazione, identificatore unico del log di attività del processo, nome e/o indirizzo del sito di inserimento del codice, informazioni sui diritti di accesso per il processo, codici di errore per il calcolo dell'hash MD5 per un oggetto dalla riga di comando del processo, elenco di wrapper di file che incapsulano l'oggetto, directory di lavoro iniziale per il processo di destinazione, serie di identificatori (PID) per i processi completati.

- Informazioni sul Registro di sistema: nomi, sezioni e valori.

- Informazioni sulle operazioni da remoto: nome del computer remoto e nome completo (FQDN) del computer remoto su cui è stata eseguita l'operazione da remoto, nome dell'account utente che ha avviato l'operazione da remoto, identificatore fornito dal sistema del processo remoto che ha avviato l'operazione da remoto, ora di inizio del processo remoto che ha avviato l'operazione da remoto, nome dello spazio dei nomi per l'utente degli eventi WMI, nome del filtro eventi WMI dell'utente, nome dell'utente creato per gli eventi WMI e il codice sorgente dell'utente degli eventi WMI.

- Informazioni sull'errore: codice di errore per il calcolo MD5, codice di errore di accesso al file, codici di errore primari e codici di errore secondari.

- Informazioni sulle attività degli eventi di risposta creati dagli specialisti di AO Kaspersky Lab e dell'Utente: nome e tipo di evento, data e ora in cui si è verificato l'evento; impostazioni e risultati dell'attività di risposta (informazioni sull'oggetto [percorso all'oggetto, nome e dimensioni dell'oggetto, checksum MD5 e SHA256], informazioni sulla quarantena dell'oggetto, informazioni sull'eliminazione dell'oggetto, informazioni sulla terminazione del processo, informazioni sull'eliminazione di una chiave di registro/ramo, informazioni sull'avvio del processo, informazioni sugli oggetti richiesti dagli specialisti di AO Kaspersky Lab per un'analisi dettagliata con il consenso dell'Utente [nome, percorso, dimensione e tipo dell'oggetto, checksum MD5 e SHA256, descrizione dell'oggetto, data e ora dell'elaborazione della richiesta di file, contenuti dei file], informazioni sull'installazione e la rimozione dell'isolamento della rete del dispositivo, informazioni sugli errori derivanti dall'attività di risposta).

- Dati sugli script in esecuzione sul computer: argomenti della riga di comando, contenuto dello script o di una parte dello stesso in esecuzione sul computer e contenuto dell'oggetto o di una parte dello stesso ricevuto da AMSI.

- Dati sui comandi ricevuti dall'applicazione della console, inclusi gli interpreti della riga di comando, che utilizzano il reindirizzamento dell'input tramite una pipe o un file, nonché i comandi eseguiti dall'utente nelle applicazioni della console, inclusi gli interpreti della riga di comando.

Elenco dei dati sugli eventi rilevati a seguito dell'analisi del traffico di rete

Al fine di facilitare il rilevamento di nuovi e complessi eventi per la sicurezza dei dati e le loro fonti, ridurre il rischio di accessi non autorizzati e adottare misure tempestive per aumentare la protezione dei dati archiviati ed elaborati dal Cliente sul suo computer, il Cliente accetta di fornire automaticamente le seguenti informazioni allo scopo di ricevere il Servizio:

- Informazioni su identificatore, versione, tipo e timestamp del record nel database anti-virus utilizzato per rilevare un evento relativo alla sicurezza delle informazioni, il nome della minaccia in base alla classificazione di AO Kaspersky Lab, timestamp dei database anti-virus utilizzati, codice tipo di file, identificatore formato file, ID di operazione del software che ha rilevato l'evento, il contrassegno di verifica della reputazione o la verifica della firma del file.

- Informazioni per determinare la reputazione dei file e delle risorse Web, inclusi indirizzo IP e nome dominio dell'indirizzo URL al quale si richiede la reputazione, nome del file eseguito al momento del rilevamento dell'evento, percorso del file e checksum (MD5) del file e suo percorso.

- Informazioni sull'emulazione del file eseguibile, inclusi, dimensioni del file e relative checksum (MD5, SHA256, SHA1), versione del componente di emulazione, profondità di emulazione, serie di proprietà e funzioni dei blocchi logici ottenute durante l'emulazione, dati estratti dalle intestazioni PE del file eseguibile.

- Informazioni su tutti gli oggetti rilevati, inclusi nome e dimensioni dell'oggetto, percorso completo dell'oggetto sul computer, checksum (MD5, SHA256) dei file elaborati, nome dell'evento associato all'oggetto, data e ora del rilevamento, contrassegno della presenza della firma digitale del file, nome dell'organizzazione che ha firmato il file, stato di attendibilità e livello della minaccia del file, identificatore e priorità della regola impiegata per il rilevamento, infine, tipo di tecnologia di rilevamento.

- Tipo di origine da cui è stato scaricato l'oggetto, indirizzo IP dell'origine, o checksum (MD5) dell'indirizzo IP quando è locale, indirizzo URL dell'origine, nonché indirizzo URL del referrer, nome, nome di dominio e checksum (MD5) dell'host che ha inviato la richiesta di download e informazioni di servizio sul browser Web che ha inviato la richiesta di download.

- Le checksum (MD5) delle parti di dominio e locali degli indirizzi e-mail del mittente e del destinatario, oltre che la checksum (MD5) dell'oggetto dell'e-mail.

- Gli indirizzi IP locali e remoti della connessione di rete, i numeri delle porte locali e remote e l'identificatore protocollo della connessione.

- Indirizzo URL e nome dell'host di destinazione e indirizzi IP dell'host.

- Identificatore del sistema operativo, installato in una macchina virtuale, utilizzato dal software per analizzare gli oggetti.

- Informazioni aggiuntive sugli eventi, inclusi, l'indice di frequenza del file nella rete locale dell'Utente, la data di intrusione del file nella rete locale e sul computer dell'Utente, gli identificatori degli account dai quali ha avuto inizio il processo, le checksum dei loro nomi utente, i nomi dei loro domini o gruppi di lavoro, le informazioni sui privilegi degli account utente.

- Informazioni sull'attività di rete del processo, inclusi i nomi dominio delle risorse di rete utilizzate per stabilire una connessione, oltre che gli indirizzi IP dei domini, la frequenza della connessione alla risorsa di rete selezionata, le dimensioni e il tipo dei dati trasferiti.

- Informazioni sull'utilizzo del dominio della risorsa di rete, inclusi indice di frequenza delle richieste al dominio dalla rete locale, timestamp della prima richiesta al dominio dalla rete locale, durata delle richieste da diversi utenti e checksum dei relativi nomi, nomi dei computer che hanno avviato le richieste al dominio, ulteriori informazioni sui motivi del rilevamento.

- Informazioni di servizio sul componente di elaborazione delle statistiche, inclusi data e ora di inizio e di fine del periodo di tempo utilizzato per analizzare i dati delle statistiche, volume della memoria del disco libera e in uso, ora dell'ultima elaborazione dell'evento, tempo di funzionamento di diversi algoritmi di rilevamento, messaggi sugli errori del componente, messaggi sul corretto avvio di diversi algoritmi di rilevamento.

- Dati inviati all'assistenza tecnica.

Trasmissione dei dati durante l'utilizzo di Kaspersky Endpoint Agent

Per informazioni dettagliate sulla trasmissione dei dati durante l'utilizzo di Kaspersky Endpoint Agent, fare riferimento a Kaspersky Endpoint Agent for Windows.

Aree geografiche del trattamento dei dati

Nella tabella seguente sono elencate le aree geografiche in cui i dati degli utenti vengono trattati in conformità all'Accordo sul trattamento dei dati DI Kaspersky Managed Detection and Response.

Aree geografiche del trattamento dei dati

Area geografica di utilizzo della licenza	Area geografica del trattamento dei dati
Europe, Canada	Europa
Regno dell'Arabia Saudita	Regno dell'Arabia Saudita
Russia e altre aree geografiche eccetto quelle elencate sopra	Russia

L'area geografica del trattamento dei dati dipende dall'area geografica selezionata durante l'attivazione di Kaspersky Managed Detection and Response per garantire la conformità ai requisiti legali relativi al trattamento dei dati degli utenti.

Informazioni su Kaspersky Security Network

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

La soluzione MDR utilizza Kaspersky Security Network (KSN) per inviare dati di telemetria dalle risorse.

Kaspersky Private Security Network (KPSN) è una soluzione che consente agli utenti dei dispositivi in cui sono installate applicazioni Kaspersky di ottenere l'accesso ai database di reputazione di Kaspersky Security Network e ad altri dati statistici senza inviare dati a KSN globale dai propri dispositivi.

La soluzione MDR supporta due modalità operative sulle risorse:

- A partire dall'aggiornamento di luglio 2025, la soluzione MDR può funzionare senza il file di configurazione di KPSN.
- Se la configurazione non soddisfa i requisiti per il funzionamento senza file di configurazione di KPSN, è necessario installare il file di configurazione di KPSN su Kaspersky Security Center Administration Server.

  Il file di configurazione di MDR include il file di configurazione di KPSN. Per informazioni dettagliate sulla configurazione di KPSN, fare riferimento alla documentazione di Kaspersky Security Center.

  Per garantire la trasmissione sicura dei dati di telemetria del cliente a Kaspersky Managed Detection and Response, Kaspersky aggiorna periodicamente le chiavi di criptaggio per i dati di telemetria MDR. Per maggiori dettagli, fare riferimento al seguente articolo: Aggiornamento periodico dei file di configurazione di KPSN.

  Se si installa il file di configurazione di KPSN su Kaspersky Security Center Administration Server, KPSN viene automaticamente disabilitato quando si revoca il consenso alle Condizioni per l'utilizzo della soluzione MDR.

Aggiornamento periodico dei file di configurazione KPSN

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Si consiglia di impostare la soluzione MDR su un funzionamento senza file di configurazione di KPSN. Per maggiori dettagli, fare riferimento a questo articolo: Passaggio della soluzione MDR al funzionamento senza file di configurazione di KPSN. Se si dispone di risorse che utilizzano file di configurazione di KPSN, è necessario aggiornare tali file una volta all'anno. In caso contrario, i dati di telemetria provenienti da queste risorse non verranno più inviati a Kaspersky Managed Detection and Response.

Per garantire la trasmissione sicura dei dati di telemetria del cliente a Kaspersky Managed Detection and Response, Kaspersky aggiorna periodicamente le chiavi di criptaggio per i dati di telemetria MDR. La chiave pubblica viene trasmessa come parte del file di configurazione di KPSN.

Se si utilizza il plug-in MDR per Kaspersky Security Center Cloud Console o Kaspersky Security Center on-premises, in alcuni casi (controllare i dettagli nella tabella seguente) il file di configurazione di KPSN verrà aggiornato automaticamente. Tuttavia, in molti casi è necessario sostituire manualmente il file di configurazione di KPSN installato.

Al massimo un mese prima della scadenza del file di configurazione di KSN corrente, Kaspersky invierà una notifica relativa all'imminente scadenza del file di configurazione di KPSN. Sono disponibili due opzioni di notifica:

- Verrà creato un incidente che avviserà dell'imminente scadenza del file di configurazione di KPSN corrente.
- Verrà pubblicata una notifica sull'imminente scadenza del file di configurazione di KPSN corrente in Web Console MDR. Tutti gli utenti che accedono a Web Console MDR visualizzeranno questa notifica.

Azioni richieste per aggiornare il file di configurazione di KPSN

La soluzione utilizzata per gestire le risorse	L'interfaccia utilizzata dagli analisti SOC	Azioni necessarie
Kaspersky Security Center Cloud Console	Il plug-in MDR installato in Kaspersky Security Center Cloud Console	Accedere a Kaspersky Security Center Cloud Console. Quando si esegue l'accesso, il plug-in MDR tenta di installare il nuovo file di configurazione di KPSN in Kaspersky Security Center Cloud Console. Se il plug-in MDR riesce ad aggiornare il file, si riceverà una notifica sulla modifica del file di configurazione di KPSN. Se il plug-in MDR non riesce ad aggiornare il file di configurazione di KPSN, si riceverà una notifica sulla causa del problema: • L'account non dispone dei diritti di accesso sufficienti per aggiornare il file. • Si è verificato un errore imprevisto durante l'aggiornamento del file di configurazione di KPSN. Se non vengono visualizzate notifiche, è probabile che il file di configurazione di KPSN sia stato aggiornato correttamente quando un altro specialista si è connesso a Kaspersky Security Center Cloud Console. Se viene visualizzata una notifica relativa ai diritti di accesso insufficienti per aggiornare il file di configurazione si KPSN, contattare l'amministratore di Kaspersky Security Center Cloud Console (ruolo **Amministratore principale**) per ricevere assistenza: Chiedere all'amministratore di connettersi a Kaspersky Security Center Cloud Console. Quando l'amministratore si connette, il file di configurazione di KPSN verrà aggiornato. È possibile verificare in qualsiasi momento se il file di configurazione di KPSN è aggiornato. A tale scopo, nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Utilizzo MDR**. Verranno visualizzate le informazioni sulla versione corrente del file di configurazione di KPSN. Se è disponibile una nuova versione del file di configurazione di KPSN, è possibile utilizzare un pulsante per aggiornare il file di configurazione di KPSN. Se si verifica un errore imprevisto durante l'aggiornamento, contattare l'Assistenza tecnica di Kaspersky.
Kaspersky Security Center Cloud Console	Web Console MDR O Si utilizza l'API per scaricare gli incidenti al fine di elaborarli nel proprio sistema	Accedere a Kaspersky Security Center Cloud Console. Avviare la Configurazione iniziale guidata per attivare il plug-in MDR. Se l'account non dispone di diritti di accesso sufficienti per attivare il plug-in MDR, contattare l'amministratore del server Kaspersky Security Center Cloud Console per ricevere assistenza. Quindi seguire le istruzioni per il server Kaspersky Security Center Cloud Console e il plug-in MDR riportate sopra. Se si verifica un errore imprevisto durante l'aggiornamento, contattare l'Assistenza tecnica di Kaspersky.

La soluzione utilizzata per gestire le risorse	L'interfaccia utilizzata dagli analisti SOC	Azioni necessarie
Kaspersky Security Center in locale versione 14 e successive	Plug-in MDR installato in Kaspersky Security Center on-premises	Accedere a Kaspersky Security Center. Quando si esegue l'accesso, il plug-in MDR tenta di installare il nuovo file di configurazione di KPSN nel server Kaspersky Security Center. Se il plug-in MDR riesce ad aggiornare il file, si riceverà una notifica sulla modifica del file di configurazione KPSN. Se il plug-in MDR non riesce ad aggiornare il file di configurazione di KPSN, si riceverà una notifica sulla causa del problema: • L'account non dispone dei diritti di accesso sufficienti per aggiornare il file. • Si è verificato un errore imprevisto durante l'aggiornamento del file di configurazione KPSN. Se non vengono visualizzate notifiche, è probabile che il file di configurazione di KPSN sia stato aggiornato correttamente quando un altro specialista si è connesso a Kaspersky Security Center Cloud Console. Se viene visualizzata una notifica relativa ai diritti di accesso mancanti per aggiornare il file di configurazione di KPSN, contattare l'amministratore del server di Kaspersky Security Center per ricevere assistenza. Chiedere all'amministratore di connettersi al server Kaspersky Security Center. Quando l'amministratore si connette, il file di configurazione KPSN verrà aggiornato. Se non riceve la notifica relativa alla modifica del file di configurazione di KPSN, l'amministratore deve controllare la versione del plug-in MDR installato e aggiornarlo alla versione corrente, se necessario (plug-in MDR 2.1.17 o versione successiva). È possibile verificare in qualsiasi momento se il file di configurazione KPSN è aggiornato. A tale scopo, nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Utilizzo MDR**. Verranno visualizzate le informazioni sulla versione corrente del file di configurazione di KPSN. Se è disponibile una nuova versione del file di configurazione di KPSN, è possibile utilizzare un pulsante per aggiornare il file di configurazione di KPSN. Se si verifica un errore imprevisto durante l'aggiornamento, contattare l'Assistenza tecnica di Kaspersky.
Kaspersky Security Center in locale versione 14 e successive	Web Console MDR (plug-in MDR non installato in Kaspersky Security Center in locale O È necessario utilizzare l'API per scaricare gli incidenti al fine di elaborarli nel sistema	Chiedere all'amministratore di Web Console MDR di: 1. Scaricare l'archivio ZIP MDR dalla pagina **Licensing**. 2. Estrarre il file di configurazione di KPSN dall'archivio ZIP. 3. Inviare questo file all'amministratore di Kaspersky Security Center Administration Server.
Kaspersky Security Center in locale 13.* o versione precedente	Plug-in MDR installato in Kaspersky Security Center in locale O È necessario utilizzare l'API per scaricare gli incidenti al fine di elaborarli nel sistema	Chiedere all'amministratore del server Kaspersky Security Center di caricare il file di configurazione di KPSN facendo clic su **Proprietà di Administration Server → Impostazioni del server proxy KSN → File delle impostazioni del server proxy KSN**. Se si verifica un errore imprevisto durante l'aggiornamento, contattare l'Assistenza tecnica di Kaspersky.

Se nella rete sono installati più server Kaspersky Security Center, è necessario aggiornare il file di configurazione di KPSN in ciascun server.

Aggiornamento del file di configurazione di KPSN nei server KATA

Se sono presenti server KATA connessi a Kaspersky Managed Detection and Response nella rete, è necessario aggiornare il file di configurazione MDR in questi server KATA.

Chiedere all'amministratore di Web Console MDR di scaricare l'archivio ZIP di configurazione MDR nella pagina **Per iniziare** (Getting Started): https://mdr.kaspersky.com/guide.

La pagina **introduttiva** (Getting Started) di Web Console MDR è disponibile solo per gli utenti che hanno effettuato l'accesso.

Quando si ottiene l'archivio ZIP di configurazione MDR, chiedere all'amministratore del server KATA di caricare il file di configurazione MDR nei server KATA. In caso di problemi durante l'aggiornamento del file di configurazione MDR, l'amministratore del server KATA deve contattare l'Assistenza tecnica di Kaspersky per istruzioni su come aggiornare il file di configurazione MDR nel server KATA.

Passaggio della soluzione MDR al funzionamento senza file di configurazione di KPSN

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

La soluzione MDR deve utilizzare la configurazione KPSN nei seguenti scenari:

- Per garantire che i dati statistici e di query KSN non vengano mai inviati a un'altra area geografica. Senza la configurazione di KPSN, Kaspersky garantisce solo che i dati vengano instradati verso l'area geografica specificata. Per maggiori dettagli, fare riferimento a questo articolo: Aggiornamento periodico dei file di configurazione di KPSN.

- Per garantire il funzionamento della soluzione MDR quando su uno qualsiasi dei dispositivi è installato un programma di installazione di un'applicazione EPP obsoleta.

È possibile commutare la soluzione MDR in modo che funzioni senza file di configurazione di KPSN se si soddisfano i seguenti requisiti:

1. Le versioni dell'applicazione EPP che supportano il funzionamento senza KPSN sono installate su tutte le risorse:

   - Kaspersky Endpoint Security for Windows versione 12.6 o successiva
   - Kaspersky Endpoint Security for Windows versione 12.6 o successiva nella configurazione di Endpoint Detection and Response Agent
   - Kaspersky Endpoint Security for Windows Light Agent versione 12.8 o successiva
   - Kaspersky Endpoint Security for Linux 12.3 o versione successiva
   - Kaspersky Endpoint Security for Mac 12.2 o versione successiva
   - Kaspersky Embedded Systems Security for Windows 4.0
   - Kaspersky Industrial CyberSecurity for Nodes 4.5

2. La soluzione MDR viene attivata su tutte le risorse tramite un codice di attivazione o un file BLOB creato non prima del 1° gennaio 2024.

   > I file BLOB creati a partire dal 1° gennaio 2024 contengono dati necessari per il funzionamento senza KPSN.

   Si consiglia di applicare un codice di attivazione per attivare la soluzione MDR per le applicazioni EPP che la supportano. Alcune versioni delle applicazioni EPP non supportano il funzionamento senza KPSN se si utilizza un file chiave per attivare la soluzione MDR. Per i dettagli, fare riferimento al seguente articolo: Requisiti hardware e software.

Per passare dalla soluzione MDR al funzionamento senza KPSN:

1. Generare e rivedere un rapporto sulle versioni del software Kaspersky in Kaspersky Security Center.
2. Aggiornare le applicazioni EPP in base ai requisiti:

   - Kaspersky Endpoint Security for Windows versione 12.6 o successiva
   - Kaspersky Endpoint Security for Windows versione 12.6 o successiva, modalità Endpoint Detection and Response Agent (richiede l'installazione di un file BLOB)
   - Kaspersky Endpoint Security for Windows Light Agent versione 12.8 o successiva
   - Kaspersky Endpoint Security for Linux 12.3 o versione successiva
   - Kaspersky Endpoint Security for Mac 12.2 o versione successiva
   - Kaspersky Embedded Systems Security for Windows 4.0
   - Kaspersky Industrial CyberSecurity for Nodes 4.5

3. Disabilitare l'utilizzo di KPSN nell'Administration Server.

   - In Kaspersky Security Center che utilizza il plug-in MDR:

   1. Assicurarsi che il plug-in MDR sia aggiornato alla versione 2.5.1.

   2. Nella sezione MDR della finestra di Kaspersky Security Center fare clic sulla scheda **Utilizzo di MDR**.

   3. Espandere il blocco **KPSN** e fare clic su **Disabilita KPSN**.

   - In Kaspersky Security Center che non utilizza il plug-in MDR:

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

   2. Si apre la finestra delle proprietà dell'Administration Server.

   3. Nella scheda **Generale**, selezionare la sezione Impostazioni proxy KSN.

   4. Disabilitare l'opzione **Utilizza Kaspersky Private Security Network**.

   5. Abilitare l'opzione **Abilita proxy KSN sull'Administration Server**.

4. Se si distribuiscono risorse da un'immagine del sistema operativo, aggiornare l'immagine in modo che l'applicazione EPP non utilizzi la configurazione di KPSN.

5. Modificare i criteri per le applicazioni EPP (necessari sia per l'utilizzo del codice di attivazione che per gli scenari di utilizzo del file BLOB).

   1. Disabilitare l'utilizzo di Kaspersky Security Network e salvare il criterio. Per ulteriori informazioni, consultare l'articolo: Configurazione di Kaspersky Security Network.

   2. Se l'applicazione EPP può essere attivata solo con un file BLOB, scaricare il file di configurazione MDR e caricare il file BLOB nel criterio.

   3. Riabilitare l'utilizzo di Kaspersky Security Network e accettare il contratto di KSN. Assicurarsi che l'opzione Applica sia abilitata nelle impostazioni dei criteri.

Monitoraggio dei dashboard in Web Console MDR

MDR Web Console fornisce dashboard di monitoraggio per visualizzare informazioni di riepilogo.

Per visualizzare i dashboard:

1. In Web Console MDR passare alla voce di menu **Monitoraggio**.

   Verrà visualizzata la pagina **Riepilogo**.

2. Nella pagina **Riepilogo** sono presenti i seguenti dashboard:

   - **Risorse massime per la licenza**

     Questo grafico a torta mostra il numero di risorse connesse rispetto al numero massimo di risorse disponibili per la licenza.

   - **Risorse in base allo stato**

     Questo grafico a torta mostra la distribuzione delle risorse in base al relativo stato.

   - **Incidenti attivi**

     Questo grafico a torta mostra la distribuzione degli incidenti attivi in base al relativo stato.

   - **Reazioni**

     Questo grafico a torta mostra la distribuzione delle reazioni in base al relativo stato.

     Il numero di risorse connesse rappresenta le risorse visualizzate in Web Console MDR negli ultimi 7 giorni. Se si desidera ottenere il numero di risorse connesse per lo specifico periodo di tempo, passare alla voce di menu **Risorse** di Web Console MDR.

   - **Statistiche di telemetria**

     Si tratta di una dashboard che mostra le statistiche di telemetria della soluzione MDR per un client, incluse le statistiche da tenant specifici. È possibile visualizzare i dati per 1 giorno, 7, 30, 90, 180 giorni, per 1 anno o per l'intero periodo in cui un client utilizza continuativamente la soluzione MDR.

     Questa dashboard visualizza il numero di ciascuno dei seguenti oggetti:

     - Gli *eventi di telemetria* sono tutti gli eventi inviati dalle risorse di un client a Kaspersky Managed Detection and Response.
     - Gli *eventi sospetti* sono eventi di telemetria che Kaspersky Managed Detection and Response definisce eventi che richiedono un controllo aggiuntivo.
     - Gli *eventi di sicurezza* sono eventi di telemetria che le regole di rilevamento definiscono come potenziali incidenti.
     - Gli *incidenti* sono azioni che la tecnologia di rilevamento definisce come critici. Gli incidenti richiedono una reazione immediata (azione di risposta) da parte di Kaspersky Managed Detection and Response.
     - Le *regole di rilevamento attivate* rappresentano il numero di regole di rilevamento univoche attivate su eventi di telemetria specificati per un dato periodo di tempo.

I dashboard vengono aggiornati a ogni aggiornamento della pagina **Riepilogo**.

Per passare dalle dashboard alle statistiche specifiche del tenant:

1. Nella parte superiore della pagina **Riepilogo**, fare clic su **Filtra per tenant**.
2. Nel menu richiamato, selezionare uno o più tenant.
3. Fare clic su **Salva**.

Le statistiche specifiche per tenant sono disponibili per i seguenti widget:

- **Limite di risorse per questa licenza**
- **Risorse in base allo stato**
- **Incidenti attivi**
- **Incidenti**
- **Reazioni**
- **Statistiche di telemetria**

Ricezione di informazioni di riepilogo

Kaspersky Managed Detection and Response fornisce diversi tipi di informazioni di riepilogo che è possibile ricevere tramite e-mail. In questa sezione viene descritto come configurare la ricezione delle informazioni di riepilogo.

Ricezione di un riepilogo di tutte le risorse in un file CSV (Web Console MDR)

È possibile ricevere un riepilogo come file CSV che contiene tutte le risorse dell'account. Nessun filtro viene applicato al riepilogo, quindi il numero delle risorse in questo riepilogo rappresenta tutte le risorse visualizzate in Web Console MDR.

È possibile nascondere le risorse con stato **Assente** nel riepilogo selezionando la casella di controllo corrispondente nelle **Impostazioni**.

Per ricevere un riepilogo CSV:

1. In Web Console MDR passare alla voce di menu **Risorse**.

   Verrà visualizzato l'elenco delle risorse.

2. Fare clic sul pulsante **Ricevi riepilogo CSV tramite e-mail** nella parte superiore della finestra.

Il riepilogo viene inviato all'indirizzo e-mail specificato durante l'attivazione di Kaspersky Managed Detection and Response.

Ricezione delle informazioni sull'incidente in formato PDF (Web Console MDR)

È possibile ricevere informazioni di riepilogo su un particolare incidente in formato PDF.

Per ricevere un riepilogo PDF:

1. In Web Console MDR passare alla voce di menu **Incidenti**.

   Verrà visualizzato l'elenco degli incidenti.

2. Fare clic sull'incidente di cui si desidera ricevere il riepilogo.

   Verrà visualizzata la scheda dell'incidente.

3. Fare clic sul collegamento **Ricevi riepilogo PDF tramite e-mail** nella parte superiore della finestra.

Il riepilogo viene inviato all'indirizzo e-mail specificato durante l'attivazione di Kaspersky Managed Detection and Response.

Impostazione dell'invio di rapporti periodici in Web Console MDR

Questa funzionalità è disponibile solo in MDR Web Console.

È possibile pianificare la ricezione di un rapporto di riepilogo contenente i dati sugli incidenti aperti. Ogni set di impostazioni per l'invio viene salvato come pianificazione. Non è possibile creare più di 50 pianificazioni per un'organizzazione e più di 10 pianificazioni per ogni tenant.

Per creare o modificare le pianificazioni di invio dei rapporti, è necessario disporre del ruolo utente di amministratore MDR.

Il rapporto viene inviato tramite e-mail in formato PDF aperto e non crittografato agli indirizzi specificati e secondo la pianificazione definita.

Il rapporto contiene sempre i dati degli ultimi sette giorni e il giorno di generazione del rapporto non è incluso. In altre parole, se la configurazione prevede che il rapporto di riepilogo venga ricevuto ogni giorno, il rapporto giornaliero conterrà i dati dei sette giorni precedenti, escluso il giorno corrente. Se la configurazione prevede che il rapporto di riepilogo venga inviato ogni mercoledì, il rapporto conterrà i dati dal mercoledì precedente al martedì seguente.

Per impostare la ricezione del rapporto di riepilogo come file PDF:

1. Nella sezione **Impostazioni** di Web Console MDR fare clic sulla scheda **Pianificazioni**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Aggiungi nuova pianificazione**.
3. Spostare l'interruttore sulla posizione **Abilitato**.
4. Leggere attentamente la notifica di seguito relativa ai termini e alle condizioni di invio dei rapporti di sintesi. Quindi selezionare la casella di controllo per confermare di aver letto e compreso i termini e le condizioni. Se la casella di controllo non è selezionata, non è possibile salvare le modifiche apportate.

5. Specificare le seguenti impostazioni:

- Nel campo **Nome pianificazione** specificare un nome leggibile arbitrario del rapporto di riepilogo. Il nome deve contenere lettere dell'alfabeto latino, cifre e caratteri speciali. Non può avere una lunghezza superiore a 1000 caratteri.

- Nel campo **Tenant** selezionare il tenant per cui si desidera ricevere un rapporto di riepilogo. Il rapporto conterrà solo i dati del tenant selezionato. In alternativa, se si desidera ricevere un rapporto di riepilogo su tutti i tenant, selezionare **Tutti i tenant**.

- Nel campo **A e-mail**, specificare un indirizzo e-mail o un elenco separato da virgole di indirizzi e-mail degli utenti che riceveranno il riepilogo.

  > Ricontrollare gli indirizzi e-mail inseriti, poiché verranno aggiunti senza ulteriori conferme. I rapporti di riepilogo possono contenere dati sensibili e verranno inviati in formato PDF aperto e non criptato.

- Nel campo **Giorno di invio** selezionare i giorni della settimana in cui il riepilogo deve essere inviato agli indirizzi e-mail specificati. È possibile scegliere un giorno o **Tutti i giorni**.

- Nel campo **Ora, UTC** specificare l'ora nel formato 24 ore UTC. Ad esempio, 15:00.

  La pianificazione influisce solo sull'ora di ricezione del rapporto, ma non sul periodo dei dati nel rapporto.

  Il rapporto contiene sempre i dati degli ultimi sette giorni e il giorno di generazione del rapporto non è incluso. In altre parole, se la configurazione prevede che il rapporto di riepilogo venga ricevuto ogni giorno, il rapporto giornaliero conterrà i dati dei sette giorni precedenti, escluso il giorno corrente. Se la configurazione prevede che il rapporto di riepilogo venga inviato ogni mercoledì, il rapporto conterrà i dati dal mercoledì precedente al martedì seguente.

6. Fare clic sul pulsante **Salva**.

Il riepilogo verrà inviato ogni settimana o ogni giorno agli indirizzi e-mail specificati.

Ricezione di notifiche

È possibile configurare l'invio di notifiche sugli eventi che si verificano in relazione agli incidenti e alle reazioni durante l'elaborazione in Kaspersky Managed Detection and Response.

Kaspersky Managed Detection and Response invia notifiche ai clienti tramite Telegram o via e-mail, a seconda delle impostazioni specificate. Il corpo della notifica contiene una descrizione dell'evento e un collegamento all'oggetto in cui si è verificato l'evento.

È possibile configurare le notifiche in Web Console MDR e nella sezione **MDR** di Kaspersky Security Center.

Impostazione delle notifiche in Web Console MDR

Per configurare l'invio delle notifiche in Web Console MDR:

1. Nella sezione **Impostazioni** di Web Console MDR fare clic sulla scheda **Impostazioni di notifica**.
2. Selezionare le caselle di controllo corrispondenti agli eventi per cui si desidera ricevere notifiche tramite e-mail o Telegram.

   Le caselle di controllo disponibili sono:

   - **Tutti** - Tutti gli eventi per cui Kaspersky Managed Detection and Response invia notifiche.
   - **Incidenti** - Notifiche sulla creazione, l'aggiornamento, la risoluzione e la chiusura degli incidenti.
     - **Notifiche estese** - Una descrizione dell'attacco rilevato come incidente e i suggerimenti per la reazione. Questa casella di controllo è disponibile se la funzionalità delle notifiche estese è abilitata nella scheda **Impostazioni generali**. È possibile abilitare queste notifiche solo in Web Console MDR, ma non nel plug-in MDR.
   - **Commenti**: Notifiche sulla creazione, l'aggiornamento e l'eliminazione dei commenti negli incidenti.
   - **Reazioni**: Notifiche sulla creazione, l'accettazione e il rifiuto delle risposte.
   - **Informazioni sulla scadenza della licenza** - Notifiche sui seguenti eventi: meno di 30 giorni mancanti alla scadenza della licenza, licenza scaduta. Kaspersky Managed Detection and Response invia queste notifiche ogni giorno, ma non dopo la scadenza della licenza o dopo il rinnovo della licenza.

3. Fare clic sul pulsante **Sottoscrivi** sopra le caselle di controllo per eseguire la sottoscrizione alle notifiche della chatbot di Telegram. Facendo clic sul pulsante **Sottoscrivi**, l'applicazione genera e visualizza un collegamento univoco per attivare la chatbot in Telegram. È possibile utilizzare questo collegamento per un solo account Telegram.

   > Utilizzare questo collegamento solo su un dispositivo (desktop o mobile) in cui è installata l'app Telegram. Il collegamento non può attivare la chatbot nella versione Web di Telegram.

   Se si desidera ricevere le notifiche su un altro account Telegram, fare clic sul pulsante **Annulla sottoscrizione**, quindi ripetere la procedura di sottoscrizione per generare un nuovo collegamento e utilizzarlo per attivare il bot della chat per un altro account.

4. Fare clic sul pulsante **Salva** nella parte inferiore della finestra per salvare le impostazioni. Il pulsante **Salva** diventa attivo solo se sono state modificate le impostazioni.

L'invio delle notifiche è configurato.

Impostazione delle notifiche in Kaspersky Security Center

*Per configurare l'invio delle notifiche nella sezione **MDR** di Kaspersky Security Center:*

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Notifiche**.

   Verrà visualizzata la scheda **Notifiche**.

2. Se si desidera ricevere notifiche tramite e-mail, abilitare l'opzione **Notifica tramite e-mail**, specificare l'indirizzo e-mail e le seguenti impostazioni di notifica.

   - Specificare un indirizzo e-mail nel campo **E-mail** e selezionare almeno una delle caselle di controllo. In caso contrario, le impostazioni non possono essere salvate.
   - **Incidenti**: Notifiche sulla creazione, la risoluzione e la chiusura degli incidenti.
     - **Notifiche estese** - Notifiche che contengono una descrizione dell'attacco rilevato come incidente e i suggerimenti per la reazione. Questa casella di controllo è disponibile se la funzionalità di notifica estesa è abilitata nella **scheda** Impostazioni.
   - **Commenti**: Notifiche sulla creazione, l'aggiornamento e l'eliminazione di commenti all'interno degli incidenti.
   - **Reazioni**: Notifiche sulla creazione, l'accettazione e il rifiuto delle risposte.

3. Se si desidera ricevere notifiche tramite Telegram, abilitare l'opzione **Notifica tramite Telegram**, quindi selezionare almeno una delle seguenti caselle di controllo:

   - **Incidenti** - Notifiche sulla creazione, la risoluzione e la chiusura degli incidenti.
   - **Commenti**: Notifiche sulla creazione, l'aggiornamento e l'eliminazione di commenti all'interno degli incidenti.
   - **Reazioni**: Notifiche sulla creazione, l'accettazione e il rifiuto delle risposte.

   Fare clic sul pulsante **Sottoscrivi** sopra le caselle di controllo per eseguire la sottoscrizione alle notifiche della chatbot di Telegram. Facendo clic sul pulsante **Sottoscrivi**, l'applicazione genera e visualizza un collegamento univoco per attivare la chatbot in Telegram. È possibile utilizzare questo collegamento per un solo account Telegram.

4. Fare clic sul pulsante **Salva** nella parte inferiore della finestra per salvare le impostazioni. Il pulsante **Salva** diventa attivo solo se sono state modificate le impostazioni.

   Se si seleziona la notifica tramite e-mail, il codice di verifica univoco viene inviato all'indirizzo e-mail specificato. Il codice di verifica ha una durata di 10 minuti.

   Verrà visualizzata la sezione di verifica.

   Nella sezione di verifica visualizzata incollare il codice di conferma per l'indirizzo e-mail specificato.

   Se si incolla un codice errato tre volte di seguito o si incolla un codice scaduto, viene visualizzato il pulsante **Invia di nuovo**. Fare clic su questo pulsante per ricevere un nuovo codice di verifica.

5. Una volta verificato l'indirizzo e-mail, viene visualizzata la sezione con il messaggio corrispondente.

6. Fare clic sul pulsante **Chiudi** nella parte inferiore della sezione.

L'invio delle notifiche è configurato.

Ricezione delle notifiche estese

È possibile configurare l'invio delle notifiche estese sugli incidenti tramite e-mail o Telegram agli utenti MDR. Le notifiche estese contengono una descrizione dell'attacco rilevato come incidente e i suggerimenti per la reazione. La descrizione dell'attacco include alcuni dati che la soluzione MDR riceve come telemetria dai dispositivi connessi alla soluzione MDR, quindi la descrizione può includere le seguenti informazioni sensibili:

- Nomi host
- Indirizzi IP dell'host
- Nomi degli account
- Password degli account (se in un dispositivo è stato eseguito uno script contenente una password)
- URL di servizio
- Nomi file
- Indirizzi e-mail
- Nomi di reparti e tenant

L'elenco completo dei dati ricevuti dalla soluzione MDR è contenuto nella sezione Trasmissione dei dati.

Abilitazione delle notifiche estese in Web Console MDR

Per abilitare l'invio delle notifiche estese:

1. Nella sezione **Impostazioni** di Web Console MDR fare clic sulla scheda **Impostazioni generali**.
2. Attivare una o entrambe le opzioni:
   - **Abilita la notifica estesa tramite e-mail**
   - **Abilita la notifica estesa tramite Telegram**
3. Selezionare la casella di controllo in fondo al riquadro per confermare di aver letto e compreso i termini per l'invio delle notifiche estese.
4. Fare clic sul pulsante **Salva**.

Ora è possibile iscriversi alle notifiche estese nelle **Impostazioni di notifica** di Web Console MDR.

Abilitazione delle notifiche estese in Kaspersky Security Center

Per abilitare l'invio delle notifiche estese:

1. Nella sezione **MDR** di Kaspersky Security Center selezionare la scheda **Impostazioni**.
2. Attivare una o entrambe le opzioni:
   - **Abilita la notifica estesa tramite e-mail**
   - **Abilita la notifica estesa tramite Telegram**
3. Selezionare la casella di controllo in fondo al riquadro per confermare di aver letto e compreso i termini per l'invio delle notifiche estese.
4. Fare clic sul pulsante **Salva**.

Ora è possibile iscriversi alle notifiche estese nella scheda **Notifiche**.

Gestione degli utenti

Gli utenti di Kaspersky Managed Detection and Response possono avere ruoli diversi, con differenti funzionalità disponibili per ogni ruolo. Il *modello di ruolo* è un set di regole che specificano i ruoli utente.

In Kaspersky Managed Detection and Response sono presenti i seguenti ruoli:

- **Amministratore MDR**

  L'utente con privilegi avanzati che ha accesso a tutte le funzioni di Kaspersky Managed Detection and Response concesse dalla licenza. L'amministratore MDR può concedere l'accesso alle origini dati client ad altri utenti. L'utente che attiva Kaspersky Managed Detection and Response diventa automaticamente l'amministratore MDR. Pertanto, è consigliabile utilizzare un indirizzo e-mail aziendale per il processo di attivazione invece di un indirizzo e-mail personale. La creazione dell'amministratore MDR con un indirizzo e-mail personale può comportare rischi per la sicurezza, come il furto dell'account dell'amministratore MDR.

  In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	✓	—
Gestione delle reazioni	✓	—
Gestione dei tenant	✓	—
Pianificazione per il riepilogo incidenti	✓	—
Accesso all'API REST	✓	—

- **Senior Security Officer**

  Un dipendente che ha accesso alle funzioni di Kaspersky Managed Detection and Response concesse dalla licenza, ma non ha accesso all'API REST. Il Senior Security Officer ha il diritto di accettare e rifiutare le reazioni.

  In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	✓	—
Gestione delle reazioni	✓	—
Gestione dei tenant	—	✓
Pianificazione per il riepilogo incidenti	—	✓
Accesso all'API REST	—	✓

- **Security Officer**

Un dipendente che ha accesso alle funzioni di Kaspersky Managed Detection and Response concesse dalla licenza, ma non ha accesso all'API REST. Il Security Officer non può accettare e rifiutare le reazioni.

In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	—	✓
Gestione delle reazioni	—	✓
Gestione dei tenant	—	✓
Pianificazione per il riepilogo incidenti	—	✓
Accesso all'API REST	—	✓

Invito di nuovi utenti in Web Console MDR

Per invitare un nuovo utente in Kaspersky Managed Detection and Response:

Se il Kaspersky Account creato in precedenza (ovvero l'e-mail) è stato utilizzato in precedenza per accedere a Kaspersky Managed Detection and Response, potrebbe essere associato ai dati MDR di un'altra organizzazione e non essere disponibile per l'applicazione di un nuovo codice di attivazione. Per utilizzare il Kaspersky Account esistente per la nuova attivazione, contattare l'Assistenza tecnica.
Nota: quando il personale dell'Assistenza tecnica rimuove l'associazione del Kaspersky Account esistente con i dati di un'altra organizzazione in MDR, il Kaspersky Account esistente non può più essere utilizzato per accedere ai dati dell'altra organizzazione per cui è stato utilizzato in precedenza.

1. Nella finestra di Web Console MDR passare alla voce di menu **Impostazioni**.

   Verrà visualizzato l'elenco degli utenti.

2. Fare clic sul pulsante **Aggiungi** sopra l'elenco degli utenti.

   Verrà visualizzata la scheda dell'invito.

3. Nel campo **E-mail** specificare un indirizzo e-mail.

4. Nel campo **Ruolo utente** specificare un ruolo per il nuovo utente.

   Sono disponibili i seguenti ruoli utente:

- **Amministratore MDR**

  L'utente con privilegi avanzati che ha accesso a tutte le funzioni di Kaspersky Managed Detection and Response concesse dalla licenza. L'amministratore MDR può concedere l'accesso alle origini dati client ad altri utenti. L'utente che attiva Kaspersky Managed Detection and Response diventa automaticamente l'amministratore MDR. Pertanto, è consigliabile utilizzare un indirizzo e-mail aziendale per il processo di attivazione invece di un indirizzo e-mail personale. La creazione dell'amministratore MDR con un indirizzo e-mail personale può comportare rischi per la sicurezza, come il furto dell'account dell'amministratore MDR.

  In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	✓	—
Gestione delle reazioni	✓	—
Gestione dei tenant	✓	—
Pianificazione per il riepilogo incidenti	✓	—
Accesso all'API REST	✓	—

  Solo un utente a cui è stato assegnato il ruolo di amministratore MDR può assegnare il ruolo di **Amministratore MDR** a un nuovo utente.

- **Senior Security Officer**

  Un dipendente che ha accesso alle funzioni di Kaspersky Managed Detection and Response concesse dalla licenza, ma non ha accesso all'API REST. Il Senior Security Officer ha il diritto di accettare e rifiutare le reazioni.

  In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	✓	—
Gestione delle reazioni	✓	—
Gestione dei tenant	—	✓
Pianificazione per il riepilogo incidenti	—	✓
Accesso all'API REST	—	✓

- **Security Officer**

Un dipendente che ha accesso alle funzioni di Kaspersky Managed Detection and Response concesse dalla licenza, ma non ha accesso all'API REST. Il Security Officer non può accettare e rifiutare le reazioni.

In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	—	✓
Gestione delle reazioni	—	✓
Gestione dei tenant	—	✓
Pianificazione per il riepilogo incidenti	—	✓
Accesso all'API REST	—	✓

5. Se necessario, selezionare il valore (o i valori) nell'elenco a discesa **Tenant**.

   Vengono suggeriti i tenant già esistenti nella Console e il valore **Tenant radice**.

   L'utente può visualizzare solo le risorse e gli incidenti relativi ai tenant specificati. Se sono presenti risorse e incidenti non assegnati ad alcun tenant, l'utente può visualizzarli se si seleziona il valore **Tenant radice**.

   È possibile selezionare il valore **Tenant radice** oltre a specificare i nomi dei tenant.

6. Fare clic su **Invita**.

   La scheda dell'invito verrà nascosta.

   Inserire l'indirizzo e-mail. L'indirizzo e-mail deve essere prima registrato e verificato sul portale web auth.hq.uis.kaspersky.com.

Un messaggio con il collegamento di invito viene inviato da noreply@mail.account.uis.kaspersky.com all'indirizzo e-mail specificato.

L'utente invitato deve verificare il proprio indirizzo e-mail visitando il collegamento nel messaggio. L'utente non può accedere e utilizzare Kaspersky Managed Detection and Response finché l'e-mail non viene verificata. Le autorizzazioni corrispondenti al ruolo utente verranno concesse dopo il primo accesso dell'utente.

Modifica dei ruoli utente in Web Console MDR

È possibile modificare il ruolo per un utente esistente. Ad esempio, un dipendente a cui è stato assegnato il ruolo Security Officer riceve responsabilità aggiuntive che richiedono l'assegnazione del ruolo Senior Security Officer.

Per modificare un ruolo per un utente esistente:

1. Nella finestra di Web Console MDR passare alla voce di menu **Impostazioni**.

   Verrà visualizzato l'elenco degli utenti.

2. Fare clic sulla stringa contenente l'utente di cui si desidera modificare il ruolo.

   Verrà visualizzata la scheda dell'utente.

3. Nella scheda dell'utente modificare il ruolo per l'utente esistente selezionando un altro ruolo dall'elenco a discesa dei ruoli.

Il ruolo dell'utente esistente verrà modificato.

Modifica dei metodi di notifica all'utente in Web Console MDR

La modifica dei metodi di notifica all'utente è disponibile solo per l'utente a cui è assegnato il ruolo Amministratore MDR. L'utente con tale ruolo può modificare le impostazioni di notifica per tutti gli utenti attivi, incluso se stesso.

Gli utenti con lo stato attivo possono ricevere notifiche da Kaspersky Managed Detection and Response tramite e-mail e/o Telegram.

Per modificare i metodi di notifica all'utente per un utente esistente:

1. Nella finestra di Web Console MDR passare alla voce di menu **Impostazioni**.

   Verrà visualizzato l'elenco degli utenti.

2. Fare clic sulla stringa contenente l'utente di cui si desidera modificare il ruolo.

   Verrà visualizzata la scheda dell'utente.

3. Nella scheda dell'utente specificare le seguenti opzioni:

   - **Notifiche e-mail abilitate**

     L'utente riceve le notifiche all'indirizzo e-mail specificato quando l'utente è stato invitato.

   - **Notifiche di Telegram abilitate**

     L'utente riceve notifiche dalla chatbot di Telegram.

   Se un utente non dispone più dell'accesso all'account Telegram, selezionare la casella di controllo **Annulla sottoscrizione notifiche per l'account Telegram**. Successivamente chiedere all'utente di accedere a Web Console MDR, passare a **Impostazioni** → **Impostazioni di notifica** e ripetere la procedura di sottoscrizione per generare un nuovo collegamento al fine di attivare la sottoscrizione Telegram per un altro account Telegram.

4. Nella parte inferiore della scheda dell'utente fare clic sul pulsante **Salva** per chiudere la scheda.

I metodi di notifica all'utente verranno modificati e salvati.

Modifica dell'accesso degli utenti ai tenant in Web Console MDR

È possibile modificare l'accesso degli utenti ai tenant nel proprio account se ad esempio si aggiunge un nuovo tenant e si desidera che un utente esistente possa accedervi.

Per modificare l'accesso ai tenant:

1. Nella finestra di Web Console MDR passare alla voce di menu **Impostazioni**.
   Verrà visualizzato l'elenco degli utenti.
2. Fare clic sulla stringa contenente l'utente di cui si desidera modificare i diritti di accesso.
   Verrà visualizzata la scheda dell'utente.
3. Nella scheda dell'utente modificare il valore (o i valori) nell'elenco a discesa **Tenant**.
4. Nella parte inferiore della scheda dell'utente fare clic sul pulsante **Salva** per chiudere la scheda.

L'accesso dell'utente ai tenant è stato modificato.

Gestione delle risorse

Una *risorsa* è un dispositivo con un'applicazione EPP Kaspersky installata (ad esempio Kaspersky Endpoint Security for Windows). Questa sezione fornisce informazioni sulla visualizzazione, l'ordinamento e il filtro delle risorse.

Visualizzazione e ricerca delle risorse in Web Console MDR

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

È possibile visualizzare e cercare le risorse disponibili utilizzando l'elenco delle risorse.

Per visualizzare le risorse:

1. Nella finestra di Web Console MDR passare alla voce di menu **Risorse**.

   Verrà visualizzato l'elenco delle risorse. Ogni riga rappresenta una risorsa. È possibile fare clic in qualsiasi punto della riga per visualizzare le informazioni sulla risorsa.

   I seguenti attributi delle risorse sono disponibili per la visualizzazione sopra l'elenco:

   - **Nome risorsa**

     Il nome di rete di un computer.

     È possibile fare clic su **Nome risorsa** per visualizzare le informazioni sulla risorsa in Kaspersky Security Center Web Console.

   - **ID risorsa**

     Identificatore univoco di una risorsa. Un ID risorsa viene generato automaticamente da Kaspersky Managed Detection and Response prima che la risorsa invii la telemetria per la prima volta.

   - **Applicazioni**

     Un'applicazione EPP (Endpoint Protection Platform) installata nella risorsa e configurata per l'utilizzo con Kaspersky Managed Detection and Response.

   - **Interfacce**

     Numero di tutte le interfacce di rete disponibili del dispositivo.

   - **Sistema operativo**

     Sistema operativo installato nella risorsa.

   - **Dominio**

     Dominio di rete a cui appartiene la risorsa.

   - **Tenant**

     Nome del tenant, se la risorsa appartiene a uno dei tenant. Se la risorsa non appartiene a un tenant, il campo è vuoto.

   - **Ultima visibilità**

     Numero di giorni dall'ultima volta che la risorsa è stata vista nella Console.

     Le risorse sono ordinate in base a questo attributo, in ordine decrescente.

     Per impostazione predefinita, vengono mostrate le risorse che sono risultate visibili negli ultimi 30 giorni. È possibile estendere l'intervallo di tempo filtrando le risorse.

- **Stato**

  È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

  Lo stato riflette lo stato corrente della risorsa. Per le risorse negli stati *OK*, *Avviso* o *Critico*, l'applicazione elenca anche i problemi (se presenti) delle ultime 72 ore.

  Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), gli stati *Avviso* e *Critico* per i componenti di controllo e protezione possono essere visualizzati in modo errato.

Le risorse hanno uno dei seguenti stati:

- **OK** (verde)

  Invio telemetria in corso, protezione completamente operativa.

- **Avviso** (giallo)

  Possibili ragioni dello stato **Avviso**:

  - Piccole perdite di telemetria. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse

  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:

    - *Firewall*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.

    - *Protezione minacce di rete*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security for Mac.

    - *Protezione minacce di posta* e l'*Estensione aggiuntiva per Microsoft Office Outlook*: ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows.

    - *Protezione minacce Web*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.

    - *Auto-Difesa del prodotto*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows o Kaspersky Security for Virtualization Light Agent.

    - I database anti-virus sono obsoleti da più di 7 giorni.

    Questi componenti influiscono sulla completezza dei dati di telemetria inviati. Se un componente è disabilitato o mancante, Kaspersky Managed Detection and Response non invia gli eventi di telemetria relativi a questo componente. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.

  - Il file di configurazione di KPSN sta per scadere. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione di KPSN. Se si continua a lavorare con il file di configurazione corrente, lo stato cambia in **Critico** pochi giorni prima della data di scadenza.

  Lo stato **Avviso** è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization Light Agent 5.2 o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Critico** (rosso)

  Possibili motivi dello stato **Critico**:

  - Gravi perdite di telemetria, i dati di telemetria non sono sufficienti per l'analisi. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse

  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:

    - *System Watcher* o *Rilevamento del comportamento*: Ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.

    - *Protezione minacce file*: ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.

    Se uno di questi componenti è disabilitato o mancante, Kaspersky Managed Detection and Response interrompe l'invio dei dati di telemetria dalla risorsa. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.

  - Il file di configurazione di KPSN sta per scadere o è già scaduto. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione KPSN.

  Questo stato è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization 5.2 Light Agent o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Offline** (nero)

  Nessun dato di telemetria da più di 7 giorni (valore predefinito). È possibile modificare il numero di giorni di assenza della telemetria, dopo i quali viene visualizzato lo stato **Offline** per la risorsa, nella sezione **Impostazioni**. L'intervallo disponibile è 2–29 giorni.

  Se si visualizza lo stato **Offline** per le risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  Lo stato **Offline** non è applicabile alle risorse VDI (macchine virtuali temporanee).

- **Assente** (nero)

  Nessun dato di telemetria da più di 30 giorni per le risorse fisiche o da più di 24 ore per le risorse VDI (macchine virtuali temporanee).

  Se si visualizza lo stato **Assente** per le proprie risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  È possibile nascondere le risorse con stato **Assente** nell'elenco delle risorse, nei rapporti e nei dati ricevuti tramite l'interfaccia API.

2. Per modificare il numero di risorse visualizzate in ogni pagina dell'elenco, selezionare il numero facendo clic sull'opzione **Voci per pagina** nella parte inferiore della pagina.

   È possibile selezionare 10, 20 o 50 risorse per pagina.

È possibile nascondere le risorse con stato **Assente** nell'elenco delle risorse selezionando la casella di controllo nelle **Impostazioni**.

Per spostarsi nell'elenco delle risorse, selezionare la pagina sotto l'elenco. Le opzioni **Precedente** e **Successivo** consentono di passare da una pagina all'altra.

Per impostazione predefinita, l'elenco delle risorse contiene le risorse visualizzate nella console negli ultimi 30 giorni.

Per modificare questo periodo:

1. Fare clic sull'icona dell'imbuto sopra l'elenco.
2. Nel riquadro **Filtro** a destra selezionare il periodo nel campo **Ultimo accesso**.
3. Fare clic su **Salva**.

È possibile eseguire ricerche delle risorse facendo clic sull'icona della lente di ingrandimento accanto all'icona a forma di imbuto sopra l'elenco delle risorse.

Filtro delle risorse in Web Console MDR

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

È possibile creare e applicare filtri all'elenco delle risorse.

Per creare un filtro per l'elenco delle risorse:

1. In Web Console MDR passare alla voce di menu **Risorse**.

   Verrà visualizzato l'elenco delle risorse.

2. Fare clic sull'icona a forma di imbuto sopra l'elenco delle risorse.

   Verrà visualizzato il menu **Filtro**.

   I parametri disponibili per il filtro sono:

   - **Ultima visualizzazione**

     Il momento in cui la risorsa è stata visualizzata l'ultima volta nella Console.

   - **Nome risorsa**

     Nomi delle risorse disponibili.

     Il nome di una risorsa è il nome di rete di un computer.

   - **Tenant**

     Nomi dei tenant disponibili.

     È possibile selezionare il valore **Tenant radice** per visualizzare le risorse che non sono assegnate ad alcun tenant.

     È possibile selezionare il valore **Tenant radice** oltre a specificare i nomi dei tenant.

- **Stato**

  È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

  Lo stato riflette lo stato corrente della risorsa. Per le risorse negli stati *OK*, *Avviso* o *Critico*, l'applicazione elenca anche i problemi (se presenti) delle ultime 72 ore.

  Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), gli stati *Avviso* e *Critico* per i componenti di controllo e protezione possono essere visualizzati in modo errato.

Le risorse hanno uno dei seguenti stati:

- **OK** (verde)

  Invio telemetria in corso, protezione completamente operativa.

- **Avviso** (giallo)

  Possibili ragioni dello stato **Avviso**:

  - Piccole perdite di telemetria. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse

  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:

    - *Firewall*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.

    - *Protezione minacce di rete*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security for Mac.

    - *Protezione minacce di posta* e l'*Estensione aggiuntiva per Microsoft Office Outlook*: ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows.

    - *Protezione minacce Web*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.

    - *Auto-Difesa del prodotto*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows o Kaspersky Security for Virtualization Light Agent.

    - I database anti-virus sono obsoleti da più di 7 giorni.

    Questi componenti influiscono sulla completezza dei dati di telemetria inviati. Se un componente è disabilitato o mancante, Kaspersky Managed Detection and Response non invia gli eventi di telemetria relativi a questo componente. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.

  - Il file di configurazione di KPSN sta per scadere. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione di KPSN. Se si continua a lavorare con il file di configurazione corrente, lo stato cambia in **Critico** pochi giorni prima della data di scadenza.

  Lo stato **Avviso** è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization Light Agent 5.2 o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Critico** (rosso)

  Possibili motivi dello stato **Critico**:

  - Gravi perdite di telemetria, i dati di telemetria non sono sufficienti per l'analisi. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse
  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:
    - *System Watcher* o *Rilevamento del comportamento*: Ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.
    - *Protezione minacce file*: ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.

    Se uno di questi componenti è disabilitato o mancante, Kaspersky Managed Detection and Response interrompe l'invio dei dati di telemetria dalla risorsa. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.
  - Il file di configurazione di KPSN sta per scadere o è già scaduto. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione KPSN.

  Questo stato è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization 5.2 Light Agent o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Offline** (nero)

  Nessun dato di telemetria da più di 7 giorni (valore predefinito). È possibile modificare il numero di giorni di assenza della telemetria, dopo i quali viene visualizzato lo stato **Offline** per la risorsa, nella sezione **Impostazioni**. L'intervallo disponibile è 2–29 giorni.

  Se si visualizza lo stato **Offline** per le risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  Lo stato **Offline** non è applicabile alle risorse VDI (macchine virtuali temporanee).

- **Assente** (nero)

  Nessun dato di telemetria da più di 30 giorni per le risorse fisiche o da più di 24 ore per le risorse VDI (macchine virtuali temporanee).

  Se si visualizza lo stato **Assente** per le proprie risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  È possibile nascondere le risorse con stato **Assente** nell'elenco delle risorse, nei rapporti e nei dati ricevuti tramite l'interfaccia API.

- **Isolamento**

  Se l'isolamento della rete è abilitato o meno. I possibili valori di filtro sono:

  - **Isolato**

    L'isolamento della rete è abilitato.

  - **Non isolato**

    L'isolamento della rete è disabilitato.

3. Fare clic su **Salva** per applicare il filtro creato.

Solo le risorse che soddisfano i parametri selezionati del filtro vengono visualizzati nell'elenco delle risorse dopo l'applicazione del filtro.

È possibile nascondere le risorse con stato **Assente** nell'elenco delle risorse selezionando la casella di controllo nelle **Impostazioni**.

Visualizzazione di informazioni dettagliate sulle risorse in Web Console MDR

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Per visualizzare informazioni dettagliate sulle risorse:

1. Nella finestra di Web Console MDR passare alla voce di menu **Risorse**.

   Verrà visualizzato l'elenco delle risorse.

2. Fare clic sulla stringa con la risorsa di cui si desidera visualizzare i dettagli.

   Verrà visualizzata la scheda della risorsa. La scheda della risorsa contiene due schede:

   - **Proprietà** include le informazioni generali sulla risorsa
   - **Incidenti** include le informazioni sugli incidenti che si sono verificati con la risorsa

   Le informazioni generali nella scheda **Proprietà** contengono le seguenti informazioni:

   - Nome risorsa

     Il nome di rete di un computer.

     È possibile fare clic su **Nome risorsa** per visualizzare le informazioni sulla risorsa in Kaspersky Security Center Web Console.

- **Stato**

  È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

  Lo stato riflette lo stato corrente della risorsa. Per le risorse negli stati *OK*, *Avviso* o *Critico*, l'applicazione elenca anche i problemi (se presenti) delle ultime 72 ore.

  Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), gli stati *Avviso* e *Critico* per i componenti di controllo e protezione possono essere visualizzati in modo errato.

Le risorse hanno uno dei seguenti stati:

- **OK** (verde)

  Invio telemetria in corso, protezione completamente operativa.

- **Avviso** (giallo)

  Possibili ragioni dello stato **Avviso**:

  - Piccole perdite di telemetria. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse

  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:

    - *Firewall*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.

    - *Protezione minacce di rete*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security for Mac.

    - *Protezione minacce di posta* e l'*Estensione aggiuntiva per Microsoft Office Outlook*: ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows.

    - *Protezione minacce Web*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.

    - *Auto-Difesa del prodotto*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows o Kaspersky Security for Virtualization Light Agent.

    - I database anti-virus sono obsoleti da più di 7 giorni.

    Questi componenti influiscono sulla completezza dei dati di telemetria inviati. Se un componente è disabilitato o mancante, Kaspersky Managed Detection and Response non invia gli eventi di telemetria relativi a questo componente. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.

  - Il file di configurazione di KPSN sta per scadere. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione di KPSN. Se si continua a lavorare con il file di configurazione corrente, lo stato cambia in **Critico** pochi giorni prima della data di scadenza.

  Lo stato **Avviso** è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization Light Agent 5.2 o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Critico** (rosso)

  Possibili motivi dello stato **Critico**:

  - Gravi perdite di telemetria, i dati di telemetria non sono sufficienti per l'analisi. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse

  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:

    - *System Watcher* o *Rilevamento del comportamento*: Ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.

    - *Protezione minacce file*: ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.

    Se uno di questi componenti è disabilitato o mancante, Kaspersky Managed Detection and Response interrompe l'invio dei dati di telemetria dalla risorsa. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.

  - Il file di configurazione di KPSN sta per scadere o è già scaduto. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione KPSN.

  Questo stato è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization 5.2 Light Agent o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Offline** (nero)

  Nessun dato di telemetria da più di 7 giorni (valore predefinito). È possibile modificare il numero di giorni di assenza della telemetria, dopo i quali viene visualizzato lo stato **Offline** per la risorsa, nella sezione **Impostazioni**. L'intervallo disponibile è 2–29 giorni.

  Se si visualizza lo stato **Offline** per le risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  Lo stato **Offline** non è applicabile alle risorse VDI (macchine virtuali temporanee).

- **Assente** (nero)

  Nessun dato di telemetria da più di 30 giorni per le risorse fisiche o da più di 24 ore per le risorse VDI (macchine virtuali temporanee).

  Se si visualizza lo stato **Assente** per le proprie risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  È possibile nascondere le risorse con stato **Assente** nell'elenco delle risorse, nei rapporti e nei dati ricevuti tramite l'interfaccia API.

- **Indirizzo IP**

  L'indirizzo IP della risorsa.

- **Indirizzo fisico**
- **Tenant**

  Nome del tenant, se la risorsa appartiene a uno dei tenant. Se la risorsa non appartiene a un tenant, il campo è vuoto.

- Prima visualizzazione
- Ultima visualizzazione
- **Sistema operativo**

  Sistema operativo installato nella risorsa.

- **Applicazioni Kaspersky che funzionano con MDR**
- **Dominio**

La scheda **Incidenti** contiene l'elenco degli incidenti. La colonna **ID/Creato** dell'elenco contiene un identificatore dell'incidente e l'ora in cui è stato creato l'incidente. La colonna **Stato** dell'elenco contiene informazioni sullo stato dell'incidente.

Stati delle risorse

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Lo stato riflette lo stato corrente della risorsa. Per le risorse negli stati *OK*, *Avviso* o *Critico*, l'applicazione elenca anche i problemi (se presenti) delle ultime 72 ore.

Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), gli stati *Avviso* e *Critico* per i componenti di controllo e protezione possono essere visualizzati in modo errato.

Le risorse hanno uno dei seguenti stati:

- **OK** (verde)

  Invio telemetria in corso, protezione completamente operativa.

- **Avviso** (giallo)

  Possibili ragioni dello stato **Avviso**:

  - Piccole perdite di telemetria. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse
  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:
    - *Firewall*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.
    - *Protezione minacce di rete*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security for Mac.
    - *Protezione minacce di posta* e l'*Estensione aggiuntiva per Microsoft Office Outlook*: ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows.
    - *Protezione minacce Web*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.
    - *Auto-Difesa del prodotto*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows o Kaspersky Security for Virtualization Light Agent.
    - I database anti-virus sono obsoleti da più di 7 giorni.

    Questi componenti influiscono sulla completezza dei dati di telemetria inviati. Se un componente è disabilitato o mancante, Kaspersky Managed Detection and Response non invia gli eventi di telemetria relativi a questo componente. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.
  - Il file di configurazione di KPSN sta per scadere. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione di KPSN. Se si continua a lavorare con il file di configurazione corrente, lo stato cambia in **Critico** pochi giorni prima della data di scadenza.

  Lo stato **Avviso** è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization Light Agent 5.2 o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Critico** (rosso)

  Possibili motivi dello stato **Critico**:

  - Gravi perdite di telemetria, i dati di telemetria non sono sufficienti per l'analisi. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse
  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:
    - *System Watcher* o *Rilevamento del comportamento*: Ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.
    - *Protezione minacce file*: ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.

    Se uno di questi componenti è disabilitato o mancante, Kaspersky Managed Detection and Response interrompe l'invio dei dati di telemetria dalla risorsa. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.
  - Il file di configurazione di KPSN sta per scadere o è già scaduto. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione KPSN.

  Questo stato è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization 5.2 Light Agent o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Offline** (nero)

  Nessun dato di telemetria da più di 7 giorni (valore predefinito). È possibile modificare il numero di giorni di assenza della telemetria, dopo i quali viene visualizzato lo stato **Offline** per la risorsa, nella sezione **Impostazioni**. L'intervallo disponibile è 2–29 giorni.

  Se si visualizza lo stato **Offline** per le risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  Lo stato **Offline** non è applicabile alle risorse VDI (macchine virtuali temporanee).

- **Assente** (nero)

  Nessun dato di telemetria da più di 30 giorni per le risorse fisiche o da più di 24 ore per le risorse VDI (macchine virtuali temporanee).

  Se si visualizza lo stato **Assente** per le proprie risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  È possibile nascondere le risorse con stato **Assente** nell'elenco delle risorse, nei rapporti e nei dati ricevuti tramite l'interfaccia API.

Controllo dello stato delle risorse in Kaspersky Security Center

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

È possibile controllare lo stato delle risorse utilizzando la funzionalità relativa agli stati delle risorse MDR. Consente di verificare quali risorse sono attualmente protette da Kaspersky Managed Detection and Response e quali non hanno mai inviato la telemetria a Kaspersky Managed Detection and Response.

Per le risorse con Kaspersky Endpoint Security for Windows 12.3 e versioni successive che funzionano nella configurazione Endpoint Detection and Response Agent (EDR Agent), lo stato visualizzato in MDR non riflette lo stato effettivo.

Stati delle risorse per cui è stata inviata la telemetria almeno una volta

Per verificare lo stato delle risorse:

1. Nella sezione **MDR** di Kaspersky Security Center passare alla scheda **Stati delle risorse MDR**.
2. Selezionare la scheda **Tutte le risorse visualizzate**.

   Viene visualizzato l'elenco di tutte le risorse che hanno inviato telemetria a Kaspersky Managed Detection and Response almeno una volta.

   Per ogni risorsa vengono visualizzati i seguenti dettagli:

- **Stato**

  È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

  Lo stato riflette lo stato corrente della risorsa. Per le risorse negli stati *OK*, *Avviso* o *Critico*, l'applicazione elenca anche i problemi (se presenti) delle ultime 72 ore.

  Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), gli stati *Avviso* e *Critico* per i componenti di controllo e protezione possono essere visualizzati in modo errato.

Le risorse hanno uno dei seguenti stati:

- **OK** (verde)

  Invio telemetria in corso, protezione completamente operativa.

- **Avviso** (giallo)

  Possibili ragioni dello stato **Avviso**:

  - Piccole perdite di telemetria. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse

  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:

    - *Firewall*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.

    - *Protezione minacce di rete*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security for Mac.

    - *Protezione minacce di posta* e l'*Estensione aggiuntiva per Microsoft Office Outlook*: ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows.

    - *Protezione minacce Web*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.

    - *Auto-Difesa del prodotto*: Ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows o Kaspersky Security for Virtualization Light Agent.

    - I database anti-virus sono obsoleti da più di 7 giorni.

    Questi componenti influiscono sulla completezza dei dati di telemetria inviati. Se un componente è disabilitato o mancante, Kaspersky Managed Detection and Response non invia gli eventi di telemetria relativi a questo componente. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.

  - Il file di configurazione di KPSN sta per scadere. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione di KPSN. Se si continua a lavorare con il file di configurazione corrente, lo stato cambia in **Critico** pochi giorni prima della data di scadenza.

  Lo stato **Avviso** è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization Light Agent 5.2 o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Critico** (rosso)

  Possibili motivi dello stato **Critico**:

  - Gravi perdite di telemetria, i dati di telemetria non sono sufficienti per l'analisi. Leggere il seguente articolo: Come evitare la perdita dei dati di telemetria dalle risorse

  - Almeno uno dei seguenti componenti dell'applicazione EPP nella risorsa è disabilitato o non installato:

    - *System Watcher* o *Rilevamento del comportamento*: Ecco come abilitare o configurare questi componenti in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux o Kaspersky Security for Virtualization Light Agent.

    - *Protezione minacce file*: ecco come abilitare o configurare questo componente in Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Security for Mac, o Kaspersky Security for Virtualization Light Agent.

    Se uno di questi componenti è disabilitato o mancante, Kaspersky Managed Detection and Response interrompe l'invio dei dati di telemetria dalla risorsa. L'applicazione EPP installata potrebbe non includere tutti i componenti elencati.

  - Il file di configurazione di KPSN sta per scadere o è già scaduto. L'applicazione visualizza la data di scadenza. Prendere in considerazione l'aggiornamento del file di configurazione KPSN.

  Questo stato è applicabile alle risorse con Kaspersky Endpoint Security for Windows 11 o versione successiva, Kaspersky Endpoint Security for Linux 11.2 o versione successiva, Kaspersky Endpoint Security for Mac 11.2 o versione successiva o Kaspersky Security for Virtualization 5.2 Light Agent o versione successiva. Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), questo stato non viene visualizzato.

- **Offline** (nero)

  Nessun dato di telemetria da più di 7 giorni (valore predefinito). È possibile modificare il numero di giorni di assenza della telemetria, dopo i quali viene visualizzato lo stato **Offline** per la risorsa, nella sezione **Impostazioni**. L'intervallo disponibile è 2–29 giorni.

  Se si visualizza lo stato **Offline** per le risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  Lo stato **Offline** non è applicabile alle risorse VDI (macchine virtuali temporanee).

- **Assente** (nero)

  Nessun dato di telemetria da più di 30 giorni per le risorse fisiche o da più di 24 ore per le risorse VDI (macchine virtuali temporanee).

  Se si visualizza lo stato **Assente** per le proprie risorse:

  - Assicurarsi che i componenti dell'applicazione EPP elencati negli stati **Avviso** e **Critico** siano installati e abilitati nelle risorse.
  - Assicurarsi che Kaspersky Managed Detection and Response sia distribuito correttamente nell'infrastruttura.

  È possibile nascondere le risorse con stato **Assente** nell'elenco delle risorse, nei rapporti e nei dati ricevuti tramite l'interfaccia API.

- **Nome risorsa**

  Il nome di rete di un computer.

  È possibile fare clic su **Nome risorsa** per visualizzare le informazioni sulla risorsa in Kaspersky Security Center Web Console.

- **ID risorsa**

  Identificatore univoco di una risorsa. Un ID risorsa viene generato automaticamente da Kaspersky Managed Detection and Response prima che la risorsa invii la telemetria per la prima volta.

- **Dominio**

  Dominio di rete a cui appartiene la risorsa.

- **Versione sistema operativo**

  Sistema operativo installato nella risorsa.

- **Applicazioni EPP**

Un'applicazione EPP (Endpoint Protection Platform) installata nella risorsa e configurata per l'utilizzo con Kaspersky Managed Detection and Response.

- **Interfacce**

  Numero di tutte le interfacce di rete disponibili del dispositivo.

- **Tenant**

  Nome del tenant, se la risorsa appartiene a uno dei tenant. Se la risorsa non appartiene a un tenant, il campo è vuoto.

- **Ultima visibilità**

  Numero di giorni dall'ultima volta che la risorsa è stata vista nella Console.

  Le risorse sono ordinate in base a questo attributo, in ordine decrescente.

  Per impostazione predefinita, vengono mostrate le risorse che sono risultate visibili negli ultimi 30 giorni. È possibile estendere l'intervallo di tempo filtrando le risorse.

3. Utilizzare le seguenti opzioni di ordinamento e filtro per lavorare con questo elenco:

   - Fare clic su qualsiasi intestazione di colonna per ordinare l'elenco in base ai valori della colonna selezionata.
   - Fare clic sulla colonna **Stato**, quindi selezionare gli stati desiderati. L'elenco verrà filtrato per mostrare solo le risorse con gli stati selezionati.
   - Fare clic sull'icona del filtro ( ), quindi selezionare il periodo di tempo per visualizzare solo le ultime risorse visualizzate durante il periodo di tempo selezionato. È inoltre possibile specificare un periodo di tempo personalizzato.
   - Fare clic sull'icona di esportazione ( ) sopra l'elenco delle risorse per eseguire un'esportazione CSV.
   - Utilizzare il campo **Cerca** per cercare le risorse per nome.

Stati delle risorse che non hanno mai inviato la telemetria

Questa funzionalità funziona correttamente in Kaspersky Security Center 15.1 Windows e versioni successive, Kaspersky Security Center 15.1 Linux e versioni successive e Kaspersky Security Center Cloud Console.

Per visualizzare le risorse che non hanno mai inviato la telemetria:

1. Nella sezione **MDR** di Kaspersky Security Center passare alla scheda **Stati delle risorse MDR**.
2. Selezionare la scheda **Risorse malfunzionanti**.

   Web Console MDR mostra un elenco delle risorse che sono state aggiunte a Kaspersky Security Center, ma non hanno mai inviato la telemetria a Kaspersky Managed Detection and Response.

   Per ogni risorsa vengono visualizzati i seguenti dettagli:

   - **Nome risorsa**

     Il nome di rete di un computer.

     È possibile fare clic su **Nome risorsa** per visualizzare le informazioni sulla risorsa in Kaspersky Security Center Web Console.

   - **Applicazioni EPP**

     Un'applicazione EPP (Endpoint Protection Platform) installata nella risorsa e configurata per l'utilizzo con Kaspersky Managed Detection and Response.

   - **Stato MDR**

     Il componente MDR di un'applicazione EPP installata in una risorsa può avere uno dei seguenti stati:

     - *Sconosciuto*: a differenza degli altri stati, lo stato *Sconosciuto* non viene inviato dalle applicazioni. Questa opzione mostra che le applicazioni non dispongono di informazioni sullo stato del componente selezionato. Questo problema può ad esempio verificarsi quando il componente selezionato non appartiene a nessuna delle applicazioni installate nel dispositivo o quando il dispositivo è spento.
     - *Arrestato*: il componente è disabilitato e al momento non funziona.
     - *Sospeso*: Il componente è sospeso, ad esempio dopo che l'utente ha sospeso la protezione nell'applicazione gestita.
     - *Avvio*: il componente è attualmente in fase di inizializzazione.
     - *In esecuzione*: il componente è abilitato e funziona correttamente.
     - *Non riuscito*: si è verificato un errore durante il funzionamento del componente.
     - *Non installato*: l'utente non ha selezionato il componente per l'installazione durante la configurazione dell'installazione personalizzata dell'applicazione.
     - *Nessuna licenza*: la licenza che copre la funzionalità MDR è assente o scaduta.

   - **Server KSC**

     Nome del Kaspersky Security Center Administration Server che gestisce la risorsa selezionata.

   - **Stato dei componenti critici**

Elenco dei componenti dell'applicazione PPE critici per l'esecuzione di MDR. Ogni componente ha un'indicazione a colori a seconda dello stato del componente:

- L'indicazione gialla viene utilizzata quando il componente ha uno dei seguenti stati: **Sospeso**, **Avvio** o **Sconosciuto**.
- L'indicazione rossa viene utilizzata quando il componente ha uno dei seguenti stati: **Arrestato**, **Non riuscito**, **Nessuna licenza** o **Non installato**.

  Inoltre, la funzionalità Autodifesa è elencata insieme ai componenti dell'applicazione PPE. Se questa funzionalità è disabilitata, presenta anche un'indicazione rossa.
- I componenti con lo stato **In esecuzione** non sono elencati nella tabella e non hanno un'indicazione.

Per visualizzare l'elenco completo dei componenti, inclusi quelli non critici per il funzionamento di MDR, fare clic sul nome della risorsa. I componenti e i relativi stati verranno visualizzati nella finestra dei dettagli della risorsa.

3. Se necessario, è possibile filtrare le risorse in base allo stato MDR. A tale scopo, fare clic sull'icona del filtro (▽), quindi selezionare gli stati di MDR richiesti. Web Console MDR mostrerà solo le risorse in cui il componente MDR ha uno degli stati di MDR selezionati. In alternativa, selezionare una delle seguenti opzioni:

   - **Installato e attivato**: l'elenco verrà filtrato in modo da mostrare le risorse con uno dei seguenti stati di MDR: *Sconosciuto*, *Arrestato*, *Sospeso*, *Avvio*, *In esecuzione* o *Non riuscito*.
   - **Licenza mancante o scaduta**: l'elenco verrà filtrato per visualizzare le risorse con lo stato di MDR *Nessuna licenza*.
4. Se necessario, fare clic sul pulsante **Esporta** per esportare l'elenco delle risorse in un file CSV.

Come evitare la perdita dei dati di telemetria dalle risorse

È consigliabile utilizzare le versioni più recenti delle applicazioni e delle soluzioni Kaspersky per garantire la protezione migliore e ottenere l'accesso completo a nuove funzionalità e aggiornamenti.

Le risorse inviano i dati di telemetria a Kaspersky Managed Detection and Response per rilevare e analizzare gli incidenti di sicurezza nell'infrastruttura. Se si riscontrano perdite di telemetria nello stato della risorsa, assicurarsi di completare le seguenti istruzioni:

1. Le versioni consigliate delle applicazioni Kaspersky sono installate nelle risorse (vedere la colonna *Versioni consigliate e relative condizioni di supporto* nella sezione *Versioni delle applicazioni Kaspersky compatibili* di Requisiti hardware e software).
2. Il throughput del canale di rete soddisfa le specifiche fornite nella sezione *Canale di rete* di Requisiti hardware e software.

3. Il server proxy KSN fornisce una capacità di throughput sufficiente.

   In caso di problemi con la capacità di throughput del server proxy KSN, disabilitare il proxy KSN nel criterio KSC per forzare la connessione diretta delle risorse a KSN:

   a. Nel menu principale di Kaspersky Security Center, accedere a **Dispositivi** → **Criteri e profili**.

   b. Fare clic sul criterio per Kaspersky Endpoint Security for Windows, Linux o Mac. Viene aperta la finestra delle proprietà del criterio selezionato.

   c. Nelle proprietà del criterio, fare clic su **Impostazioni applicazione** → **Protezione minacce avanzata** → **Kaspersky Security Network**.

   d. Abilitare l'opzione **Usa server KSN quando il proxy KSN non è disponibile** (se applicabile per il criterio).

   e. Fare clic su **OK**.

4. Il proxy KSN è abilitato sul lato del punto di distribuzione in Kaspersky Security Center Cloud Console o Kaspersky Security Center Web Console per ottimizzare il carico di rete.

5. Il carico di lavoro Kaspersky Security Center Administration Server non supera i limiti.

6. Viene utilizzata la versione consigliata di Kaspersky Security Center specificata in Requisiti hardware e software e vengono installati gli ultimi hotfix e patch disponibili.

Gestione degli incidenti

Un *incidente* è un'attività valutata come critica dalla tecnologia di rilevamento e che richiede una reazione immediata da parte del servizio online. Questa sezione fornisce informazioni sulla gestione degli incidenti esistenti e sull'aggiunta di nuovi incidenti.

Con il rilascio della versione 2.3.1 del plug-in MDR, le funzioni di gestione degli incidenti sono state rimosse dalla sezione MDR di Kaspersky Security Center. È possibile gestire gli incidenti in Web Console MDR.

Se si utilizza il plug-in MDR versione 2.3.0 o precedente, è consigliabile gestire gli incidenti in Web Console MDR, poiché le funzioni di gestione degli incidenti in Kaspersky Security Center con il plug-in MDR non sono più in fase di sviluppo.

Per gestire gli incidenti in Web Console MDR, è necessario creare un Kaspersky Account e chiedere all'amministratore MDR (l'utente di Web Console MDR con il ruolo di **amministratore MDR**) di inviare un invito in Web Console MDR utilizzando l'indirizzo e-mail utilizzato per il Kaspersky Account.

Si riceverà l'e-mail di invito contenente il collegamento a Web Console MDR.

Informazioni sugli incidenti

Che cos'è un incidente

Nel contesto della sicurezza informatica, un incidente è qualsiasi evento imprevisto o indesiderato che potrebbe causare un'interruzione della normale attività o della sicurezza informatica.

Un evento è caratterizzato da indizi esterni identificati relativamente a uno stato particolare di un sistema, di un servizio o di una rete.

Nella struttura di questa soluzione Kaspersky MDR, il criterio principale per decidere se l'attività osservata sia un incidente è la capacità di implementare misure efficaci per contrastare, prevenire o ridurre i possibili danni risultanti da questa attività. Vedere la tabella seguente per esempi di possibili criteri di incidente e misure di reazione a seconda dell'origine dell'evento.

Esempi di criteri di rilevamento degli incidenti e misure di reazione

Origine dell'evento	Possibili criteri per l'incidente	Possibili reazioni per l'incidente
Dispositivo endpoint	• La fase attiva dell'attacco che non è stata impedita automaticamente • Evidenza di oggetti dannosi permanenti nel sistema • Indicatori di incidenti passati • Indicatori di attività di intrusione interna da parte del cliente (compresi i casi in cui l'attacco è stato evitato con successo)	• Rilevamento dei problemi tramite le soluzioni di AO Kaspersky Lab installate sui dispositivi endpoint e valutazione dell'efficienza della reazione automatica (se tecnicamente possibile) • Raccomandazione di azioni di reazione manuali • Richieste di azioni di risposta automatiche • Raccomandazioni per sensibilizzare gli utenti alla sicurezza informatica
Dispositivo endpoint + rete	Evento di sicurezza proveniente dalla tecnologia di rilevamento della rete supportata, confermato sul dispositivo endpoint	• Rilevamento dei problemi tramite le soluzioni di AO Kaspersky Lab installate sui dispositivi endpoint e le soluzioni di AO Kaspersky Lab per il monitoraggio del traffico di rete e la valutazione dell'efficienza della reazione automatica (se tecnicamente possibile) • Raccomandazione di azioni di reazione manuali • Richieste di azioni di risposta automatiche • Informare il cliente

Scenari di rilevamento incidente

Scenario 1. Rilevamento degli incidenti con la soluzione Kaspersky MDR

In questo scenario, viene rilevato un incidente di sicurezza informatica a seguito del funzionamento di Kaspersky MDR. L'incidente viene registrato automaticamente nel sistema di monitoraggio degli incidenti. Il livello di priorità dell'incidente predefinito può essere modificato in seguito, ma sarà necessario specificare il motivo della modifica in base alla tabella del livello di priorità dell'incidente (vedere di seguito). Kaspersky MDR elabora gli eventi registrati per ottenere tempestivamente informazioni sullo stato dell'infrastruttura informatica del cliente.

Se le cause principali dell'incidente vengono identificate come risultato dell'analisi, vengono fornite raccomandazioni di reazione al cliente. Se non sono disponibili informazioni sufficienti per identificare la causa principale dell'incidente, tutte le informazioni disponibili e i risultati dell'analisi vengono forniti al cliente per una ricerca indipendente.

Scenario 2. Rilevamento degli incidenti da parte del cliente (la creazione di incidenti personalizzati non è disponibile in alcuni livelli della licenza commerciale)

In questo scenario, il cliente rileva un incidente di sicurezza informatica, indipendentemente dal funzionamento di Kaspersky MDR. Se l'incidente deve essere elaborato da Kaspersky MDR, il cliente può registrarlo manualmente e fornire tutte le informazioni disponibili sull'incidente rilevato utilizzando le funzionalità di Kaspersky MDR. Per impostazione predefinita, il livello di priorità dell'incidente è impostato su **Basso**, se non diversamente specificato dal cliente durante la registrazione dell'incidente.

L'ulteriore elaborazione dell'incidente è simile allo Scenario 1.

Livelli di priorità degli incidenti

Livelli di priorità degli incidenti e relative descrizioni

Livelli di priorità degli incidenti	Descrizione
Alta	Incidenti che, secondo l'opinione degli esperti di AO Kaspersky Lab, possono causare gravi interruzioni o accesso non autorizzato alle risorse del cliente monitorate da Kaspersky MDR. Ad esempio, identificazione di tracce di un attacco mirato o di una minaccia sconosciuta che richiedono ulteriori ricerche utilizzando metodi di indagine scientifica digitale.
Media	Incidenti che, secondo l'opinione degli esperti di AO Kaspersky Lab, possono influire sull'efficienza o sulle prestazioni delle risorse del cliente monitorate da Kaspersky MDR o possono causare il danneggiamento dei dati monouso.
Bassa	Incidenti che, secondo l'opinione degli esperti di AO Kaspersky Lab, non influiscono in modo significativo sull'efficienza o sulle prestazioni delle risorse del cliente monitorate da Kaspersky MDR. Ad esempio, software potenzialmente indesiderato identificato come adware o riskware.

Il livello di priorità incidenti predefinito è **Basso**.

Obiettivi prestazionali della forniti dalla soluzione

Tempo di reazione di destinazione e valore della consegna di Kaspersky MDR a seconda della priorità dell'incidente

Livelli di priorità degli incidenti	Tempo di risposta	Valore target
Alta	1 ora	90%
Media	4 ore	90%
Bassa	24 ore	90%

L'incidente è considerato risolto se al cliente sono state fornite raccomandazioni sulle misure di reazione.

*Il tempo di reazione è il tempo che intercorre tra il rilevamento dell'incidente (ora di creazione) e la sua pubblicazione in Web Console MDR (ora di aggiornamento).

**Il valore target è la percentuale di incidenti nella quale il tempo di reazione soddisfa l'obiettivo indicato nella tabella.

Visualizzazione e ricerca degli incidenti in Web Console MDR

Per visualizzare gli incidenti:

1. In Web Console MDR passare alla voce di menu **Incidenti**.

   Verrà visualizzato l'elenco degli incidenti. Ogni riga rappresenta un incidente. È possibile fare clic in qualsiasi punto della riga per visualizzare le informazioni sull'incidente.

   I seguenti attributi dell'incidente sono presenti sopra l'elenco:

   - **ID/Creato** - Identificatore numerico dell'incidente nella console/data di creazione dell'incidente.
   - **Stato** - uno dei seguenti stati dell'incidente:
     - **Aperto** - L'incidente deve essere elaborato dal team di sicurezza.
     - **Risolto** - L'incidente ha ricevuto una reazione creata dal team di sicurezza.
     - **In attesa** - L'elaborazione dell'incidente è stata temporaneamente interrotta dal team di sicurezza.
     - **Chiuso** - L'incidente è stato elaborato dal team di sicurezza e non è necessario ulteriore lavoro su di esso.
   - **Riepilogo** - Un breve commento sull'incidente nel complesso.
   - **Tenant** - Tenant a cui è assegnato un incidente.
   - **Aggiornato** - Data e ora in cui è stato aggiornato l'incidente.

     Gli incidenti sono ordinati in base all'ora di aggiornamento in ordine decrescente.

     È possibile aggiungere o rimuovere attributi (colonne) e riordinarli facendo clic sull'icona a forma di ingranaggio sopra l'elenco.

2. Per modificare il numero di incidenti visualizzati in ogni pagina dell'elenco, selezionare un numero facendo clic sull'opzione **voci per pagina** nella parte inferiore della pagina. È possibile selezionare 10, 20 o 50 incidenti per pagina.

Per spostarsi nell'elenco degli incidenti, selezionare una pagina sotto l'elenco. Le opzioni **Precedente** e **Successivo** consentono di passare da una pagina all'altra.

Per filtrare gli incidenti, fare clic sull'icona a forma di imbuto sopra l'elenco.

È possibile eseguire ricerche degli incidenti facendo clic sull'icona della lente di ingrandimento accanto all'icona a forma di imbuto sopra l'elenco degli incidenti.

Filtro degli incidenti in Web Console MDR

Per visualizzare incidenti specifici, è possibile creare e applicare filtri all'elenco degli incidenti.

Per creare un filtro per l'elenco degli incidenti:

1. In Web Console MDR fare clic sulla voce del menu **Incidenti**.

   Verrà visualizzato l'elenco degli incidenti.

2. Fare clic sull'icona a forma di imbuto sopra l'elenco degli incidenti.

   Verrà visualizzata la sezione **Filtro**.

   I parametri disponibili per il filtro sono:

   - **Creato**

     Periodo di tempo per la creazione dell'incidente.

   - **Aggiornato**

     Periodo di tempo per l'aggiornamento dell'incidente.

   - **Priorità**

     Priorità dell'incidente. Le priorità disponibili sono Bassa, Normale e Alta.

   - **Stato**

     Stato dell'incidente.

   - **Risoluzione**

     Risoluzione dell'incidente.

   - **Risorse**

     Risorse disponibili.

   - **Tenant**

     Nomi dei tenant disponibili.

     È possibile selezionare il valore **Tenant radice** per visualizzare gli incidenti che non sono assegnate ad alcun tenant.

     È possibile selezionare il valore **Tenant radice** oltre a specificare i nomi dei tenant.

   - **Tattiche**

     Tattiche MITRE disponibili per la reazione agli incidenti.

   - **Stati delle reazioni**

     Mostra solo gli incidenti con gli stati selezionati delle reazioni corrispondenti.

3. Fare clic su **Salva** per applicare il filtro creato. Fare clic su **Cancella** per eliminare il filtro creato.

Solo gli incidenti che soddisfano i parametri selezionati del filtro vengono visualizzati nell'elenco degli incidenti dopo l'applicazione del filtro.

Creazione di incidenti personalizzati in Web Console MDR

La creazione di incidenti personalizzati non è disponibile in alcuni livelli di licenza commerciale.

Se si ritiene che alcune attività nella propria infrastruttura rappresentino una minaccia ma Kaspersky Managed Detection and Response non ha creato automaticamente un incidente, è possibile aggiungere manualmente un nuovo incidente.

In base ai termini del contratto di servizio (SLA), il numero di incidenti creati manualmente che possono essere elaborati dal team di sicurezza è limitato. Le informazioni sulle limitazioni sono disponibili nella scheda **Utilizzo di MDR** in Kaspersky Security Center. In questa scheda è possibile tenere traccia dell'utilizzo degli incidenti creati manualmente per il periodo corrente (ad esempio per la settimana corrente):

- Il numero totale di incidenti che è possibile creare per il periodo corrente. Questi incidenti devono essere elaborati dal team di sicurezza in base al contratto di servizio. È possibile creare più incidenti rispetto al numero specificato nel Contratto di MDR, ma non è garantita la conformità con le tempistiche SLA per l'elaborazione di tali incidenti.
- Il numero rimanente di incidenti che è possibile creare per il periodo corrente.

Per aggiungere un nuovo incidente:

1. Nella finestra di Web Console MDR passare alla voce di menu **Incidenti**.

   Verrà visualizzato l'elenco degli incidenti.

2. Nella parte superiore della finestra fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la sezione per il nuovo incidente.

3. Compilare i campi seguenti:

   - **Riepilogo**

     Un breve commento sull'incidente.

   - **Descrizione**

     Informazioni dettagliate in formato libero sull'incidente. Il markdown è supportato.

   - **Risorse**

     La risorsa compromessa nell'incidente. Per questo campo vengono suggerite le risorse già esistenti in Web Console MDR e Kaspersky Security Center.

4. Se necessario, compilare il campo **Tenant**.

   Per il campo **Tenant** vengono suggeriti i tenant già esistenti nella console e il valore **Radice senza tenant**.

5. Fare clic sul pulsante **Invia**.

   La sezione per il nuovo incidente verrà nascosta.

Il nuovo incidente verrà aggiunto all'elenco degli incidenti in Web Console MDR. È possibile visualizzare informazioni dettagliate su questo incidente e sull'elaborazione delle relative reazioni.

Visualizzazione di informazioni dettagliate sugli incidenti in Web Console MDR

Per visualizzare informazioni dettagliate sugli incidenti:

1. Nella finestra di Web Console MDR passare alla voce di menu **Incidenti**.

   Verrà visualizzato l'elenco degli incidenti.

2. Fare clic sulla stringa con l'incidente di cui si desidera visualizzare i dettagli.

   Verrà visualizzata la pagina dell'incidente.

   Il titolo della pagina contiene un identificatore dell'incidente. Sotto il titolo sono presenti quattro schede:

   - **Riepilogo**

     Contiene informazioni generali sull'incidente.

   - **Reazioni**

     Contiene informazioni sulle reazioni all'incidente.

   - **Comunicazione**

     Contiene informazioni sulle comunicazioni e sui file relativi all'incidente.

   - **Cronologia**

     Contiene informazioni sulle modifiche apportate all'incidente.

   Le informazioni generali nella scheda **Riepilogo** iniziano con un breve riepilogo dell'incidente. Le informazioni aggiuntive elencate in questa sezione includono:

   - Priorità dell'incidente
   - Stato dell'incidente
   - Risoluzione degli incidenti
   - Timestamp dell'ora di creazione e dell'ora di aggiornamento dell'incidente
   - Tattiche MITRE
   - Tecniche MITRE
   - Tecnologia di rilevamento

   Sotto il riepilogo dell'incidente sono elencate le seguenti informazioni:

   - Risorse interessate
   - IOC basati sulle risorse
   - IOC basati sulla rete

Le informazioni generali nella scheda **Riepilogo** si concludono con una descrizione del cliente e un pulsante **Chiudi incidente**.

3. Se si sa che l'incidente è un duplicato o che non verrà risolto, fare clic sul pulsante **Chiudi incidente**.

4. Fare riferimento alla scheda **Reazioni** per visualizzare le informazioni sulle richieste di reazione.

   Le informazioni nella scheda **Reazioni** sono presentate in un elenco. Le colonne dell'elenco sono:

   - **Stato**
   - **ID risorsa**
   - **Tipo**
   - **Dettagli**
   - **Commento**
   - **Modificato da**
   - **Ora di aggiornamento**

5. Se si desidera aggiungere un commento a un incidente:

   a. Nella scheda **Comunicazione** della pagina dei dettagli dell'incidente digitare i commenti nel campo di testo.

      Sono supportati markdown e file allegati. La dimensione massima del file è 10 MB.

   b. Fare clic sul pulsante **Invia**.

      Il commento viene aggiunto alla scheda **Comunicazione** nella pagina dei dettagli dell'incidente. È possibile modificare o eliminare i commenti entro 10 minuti dalla pubblicazione.

6. Fare riferimento alla scheda **Cronologia** per visualizzare le informazioni sulle modifiche apportate all'incidente.

   Sotto il titolo è disponibile un'opzione per mostrare le modifiche relative a:

   - **Tutti gli eventi**
   - **Solo incidenti**
   - **Solo reazioni**
   - **Solo comunicazione**

   Accanto a questa opzione sono presenti i seguenti pulsanti:

   - Il pulsante **Colonne** con l'icona a forma di ingranaggio per selezionare le colonne da visualizzare nella scheda **Cronologia**.
   - Il pulsante **Filtro** con l'icona a imbuto per mostrare le modifiche relative solo alle caselle di controllo selezionate.
   - Il pulsante **Cerca** con l'icona della lente di ingrandimento per mostrare le modifiche relative solo alle parole o ai caratteri immessi.

Tipi di reazioni

Gli analisti SOC di MDR esaminano gli incidenti e creano reazioni che è possibile accettare o rifiutare. Si tratta della modalità predefinita di gestione degli incidenti in Kaspersky Managed Detection and Response.

Tuttavia, è possibile creare manualmente le reazioni utilizzando le funzionalità di Kaspersky Endpoint Detection e Response Optimum.

> Questo articolo descrive solo i tipi di reazioni degli analisti SOC.

Ogni reazione può avere una serie di parametri presenti nella scheda **Reazioni** di un incidente.

I tipi di reazioni disponibili sono:

- **Ottieni file**

  Copia di un file dall'infrastruttura a Kaspersky SOC. Se si accetta questa reazione, il file specificato verrà copiato in Kaspersky SOC.

  Questo tipo di reazione può ottenere file contenenti dati personali e/o riservati.

  I parametri possibili sono:

  - **Percorso file infetto**

    Il percorso assoluto del file. Ad esempio, `C:\\file.exe`.

  - **Dimensione massima del file**

    La dimensione massima del file, in MB.

    Se il file infetto supera la dimensione massima del file specificata, il tentativo di accettare la reazione avrà esito negativo e la reazione non verrà eseguita, ma verrà visualizzata nella scheda **Cronologia** di un incidente.

- **Isola**

Isolamento della risorsa specificata dalla rete.

> Nel caso in cui sia necessario disabilitare urgentemente l'isolamento della rete, contattare il Servizio di assistenza tecnica o scrivere una richiesta nella scheda **Comunicazione** dell'incidente.

I parametri possibili sono:

- **Password per disabilitare l'isolamento**

  La password per disabilitare l'isolamento. Una volta ricevuta la richiesta di disabilitazione dell'isolamento della rete, il Servizio di assistenza tecnica invierà la procedura con i dettagli sull'utilizzo della password.

- **ID attività**

  L'identificatore univoco dell'attività utilizzato in abbinamento alla **Password per disabilitare l'isolamento** per la disabilitazione manuale dell'isolamento di rete.

- **Dettagli password**

  È possibile verificare la validità della **Password** generando da essa una chiave derivata e confrontando il valore risultante con il valore nel parametro **Chiave derivata**.

  - **Versione**

    La versione numerica delle regole di creazione della password. Una versione 1 significa che vengono applicati i seguenti parametri di PBKDF2 per la creazione di una chiave derivata:

    - Algoritmo di hash HMACSHA256
    - 10.000 iterazioni
    - Lunghezza chiave di 32 byte

  - **Salt**

    Salt in formato HEX per ottenere una chiave derivata tramite PBKDF2.

  - **Chiave derivata**

    La chiave derivata in formato HEX.

- **Durata dell'isolamento della risorsa**

  Il periodo di tempo in secondi dopo il quale l'isolamento verrà disabilitato automaticamente. Se non è specificato alcun periodo di tempo personalizzato, viene applicato il periodo di tempo predefinito di sette giorni. Il valore massimo è 2.678.400 secondi.

- **Regole di esclusione**

  Matrice di regole con porte, protocolli, indirizzi IP e processi personalizzati a cui non viene applicato l'isolamento.

  - **Direzione**

    La direzione del traffico. I valori possibili sono: **In entrata**, **In uscita**, **Entrambi**.

  - **Protocollo**

    Il numero di protocollo secondo la specifica IANA.

    I valori possibili sono:

    - **1** (ICMP)
    - **6** (TCP)
    - **17** (UDP)
    - **58** (IPv6-ICMP)

  - **Intervallo porte remote**

    L'intervallo di porte remote specificato nei campi **Da** e **A** nidificati.

  - **Indirizzo IPv4 remoto**

    L'indirizzo IPv4 remoto o la subnet mask.

  - **Indirizzo IPv6 remoto**

    L'indirizzo IPv6 remoto o la subnet mask.

  - **Intervallo porte locali**

    L'intervallo di porte locali specificato nei campi **Da** e **A** nidificati.

  - **Indirizzo IPv4 locale**

    L'indirizzo IPv4 locale o la subnet mask.

  - **Indirizzo IPv6 locale**

    L'indirizzo IPv6 locale o la subnet mask.

  - **Processo**

    Il percorso dell'immagine del processo specificata nel campo **Immagine** → **Percorso** nidificato.

- **Disabilita isolamento**

  Disabilitare l'isolamento di rete della risorsa specificata.

- Elimina chiave del Registro di sistema

  Eliminare una chiave del Registro di sistema o di un ramo del Registro di sistema nella risorsa specificata.

  I parametri possibili sono:

  - **Chiave**

    Il percorso assoluto della chiave, che inizia con `HKEY_LOCAL_MACHINE` o `HKEY_USERS`. Ad esempio `HKEY_LOCAL_MACHINE\\SYSTEM\\WebClient`.

    Se la chiave è un collegamento simbolico, solo questa chiave verrà eliminata mentre la chiave di destinazione del collegamento rimarrà intatta.

  - **Valore**

    Il valore della chiave.

    Se questo parametro non è specificato, la chiave verrà eliminata in modo ricorsivo. Durante l'eliminazione ricorsiva, ogni sottochiave che è un collegamento simbolico verrà eliminata mentre la relativa chiave di destinazione rimarrà intatta.

    Se il valore della chiave è una stringa vuota, il valore predefinito verrà eliminato.

- Dump della memoria

  Creazione di un dump della memoria e invio a Kaspersky SOC.

  I parametri possibili sono:

  - **Tipo di dump**

    Un dump della memoria può essere di due tipi:

    - **Dump della memoria completo**

      Un dump dell'intera memoria di una risorsa.

    - **Dump del processo**

      Un dump di un processo specificato.

  - **Dimensione massima del file**

    La dimensione massima del file per il dump in formato ZIP, in MB. Il valore predefinito è 100 MB.

  - **Processo**

    L'ID del processo e i dettagli dell'immagine.

    - **Immagine**

      - **Percorso**

        Il percorso assoluto del file. Ad esempio, `%systemroot%\\system32\\svchost.exe`.

      - **SHA256**

        Il checksum SHA256 in formato HEX.

      - **MD5**

        Il checksum MD5 in formato HEX.

    - **ID univoco**

      L'identificatore univoco del processo.

  - **Limite conteggio processi**

    Il numero massimo di processi che possono essere contenuti nel file di dump.

- Termina processo

  Terminare un processo sulla risorsa specificata con Kaspersky Endpoint Security for Windows. Il processo da terminare può essere specificato tramite il nome o l'identificatore di processo (PID).

- Esegui script

  Eseguire uno script sulla risorsa specificata con Kaspersky Endpoint Security for Windows.

  Affinché questa risposta funzioni, il componente PowerShell deve essere installato nella risorsa. È possibile visualizzare lo script da eseguire e la relativa descrizione in MDR Web Console.

- **Sposta il file in Quarantena**

  Inserisce un file potenzialmente pericoloso in un archivio locale speciale. I file in questo archivio sono criptati e non minacciano la sicurezza del dispositivo. La richiesta di conferma specifica la risorsa, il percorso del file e l'hash del file (MD5 o SHA256).

- Ripristina il file dalla Quarantena

  Ripristina il file precedentemente spostato in Quarantena nella posizione originale. Se nella posizione originale è presente un file con lo stesso nome, il ripristino non viene eseguito.

- Ottieni artefatti

Disponibile se è stata configurata l'integrazione con Kaspersky Anti Targeted Attack

Copia i file relativi agli avvisi di Kaspersky Anti Targeted Attack dall'infrastruttura Kaspersky Anti Targeted Attack in Kaspersky SOC. I file copiati vengono utilizzati dagli analisti SOC di MDR per esaminare gli avvisi di Kaspersky Anti Targeted Attack.

I parametri possibili sono:

- ID nodo della soluzione Kaspersky Anti Targeted Attack.
- ID avviso Kaspersky Anti Targeted Attack.
- Categorie di file da copiare in Kaspersky SOC correlate agli avvisi:
  - File PCAP e Payload relativi a un avviso IDS.
  - Rapporto sul risultato della scansione in Sandbox. Include schermate dell'esecuzione di oggetti, registro attività e altri dati di scansione.
  - Il file infetto inviato a Sandbox.
  - Dettagli su tutti i file relativi all'avviso.

Disponibile se è stata configurata l'integrazione con Kaspersky NEXT XDR Expert 2.0

Copia i file relativi agli avvisi o agli incidenti di Kaspersky NEXT XDR Expert 2.0 dall'infrastruttura Kaspersky NEXT XDR Expert in Kaspersky SOC. I file copiati vengono utilizzati dagli analisti SOC di MDR per indagare su avvisi e incidenti di Kaspersky NEXT XDR Expert.

I parametri possibili sono:

- ID nodo della soluzione Kaspersky NEXT XDR Expert.
- ID incidente o avviso Kaspersky NEXT XDR Expert.

- Categorie di file da copiare in Kaspersky SOC correlate agli avvisi o agli incidenti:
  - File caricati nell'avviso o nell'incidente Kaspersky NEXT XDR Expert.
  - Rapporto sul risultato della scansione in Sandbox. Include schermate dell'esecuzione di oggetti, registro attività e altri dati di scansione.
  - Il file infetto inviato a Sandbox.
  - File correlati alle azioni di reazione dell'utente per l'avviso o l'incidente:
    - Recupero dei file
    - Raccolta di analisi forensi
    - Acquisizione della chiave del registro di sistema
    - Recupero dei file di servizio del file system NTFS
    - Acquisizione del dump della memoria di processo
    - Spostamento dei file in Quarantena
- Dettagli su tutti i file relativi all'avviso.
- Nomi e ids dei file copiati.

In questo tipo di azione di reazione è possibile trasmettere file contenenti dati personali e riservati.

Elaborazione delle reazioni agli incidenti in Web Console MDR

È possibile visualizzare, accettare e rifiutare le reazioni agli incidenti.

Per visualizzare le reazioni a un incidente:

1. Nella finestra di Web Console MDR passare alla voce di menu **Incidenti**.

   Verrà visualizzato l'elenco degli incidenti.

2. Fare clic sulla stringa con l'incidente di cui si desidera visualizzare i dettagli.

   Verrà visualizzata la pagina dell'incidente.

3. Nella pagina dell'incidente fare clic sulla scheda **Reazioni**.

   Verrà visualizzato l'elenco delle reazioni.

   Ogni riga rappresenta una reazione. Vengono visualizzate le seguenti informazioni sulla reazione:

   - **Stato**

     Stato della reazione.

   - **ID risorsa**

     Identificatore della risorsa per la reazione da eseguire.

   - **Tipo**

     Tipo dell'oggetto che costituisce la reazione.

   - **Parametri**

     Percorso locale specifico del sistema operativo per ottenere il file di reazione e dimensione del file prevista in MB. La dimensione massima del file è 10 MB.

   - **Commento**

     Ultimo commento alla reazione.

   - **Modificato da**

     Ultimo utente che ha modificato la descrizione della reazione.

   Per visualizzare la descrizione della reazione, fare clic sulla stringa con la reazione.

Per accettare o rifiutare le reazioni a un incidente:

1. Nella finestra della console passare alla voce di menu **Incidenti**.

   Verrà visualizzato l'elenco degli incidenti.

2. Fare clic sulla stringa con l'incidente di cui si desidera visualizzare i dettagli.

   Verrà visualizzata la pagina dell'incidente.

3. Nella pagina dell'incidente fare clic sulla scheda **Reazioni**.

   Verrà visualizzato l'elenco delle reazioni.

4. Selezionare una reazione da approvare o rifiutare selezionando la casella di controllo all'estremità sinistra della stringa che contiene la reazione.

   È inoltre possibile selezionare più reazioni selezionando le relative caselle di controllo a sinistra. Per selezionare tutte le reazioni, selezionare la casella di controllo nella parte sinistra dell'intestazione della tabella delle reazioni.

5. Per approvare o rifiutare una o più reazioni, selezionare il pulsante **Accetta** o **Rifiuta** sotto l'elenco delle reazioni. Verrà visualizzata la casella dei commenti. Inserire il commento e fare clic sul pulsante **Invia**.

   È inoltre possibile fare clic su una reazione nella scheda **Reazioni** per verificarne i dettagli e accettarla o rifiutarla nel riquadro laterale visualizzato. Per rifiutare la reazione, è necessario immettere il commento nel campo nel riquadro laterale.

Lo stato della reazione verrà modificato.

Accettazione automatica delle reazioni in Web Console MDR

È possibile abilitare l'accettazione automatica delle reazioni offerte. In questo caso, le azioni proposte nelle reazioni, ad esempio l'eliminazione di un file infetto, verranno eseguite automaticamente. Quando questa funzionalità è disabilitata, le misure offerte nelle reazioni devono essere accettate o rifiutate manualmente.

Se si utilizzano i tenant, è possibile abilitare l'accettazione automatica delle reazioni per tutti i tenant o solo per i tenant selezionati. Se non si utilizzano i tenant, si abilita o si disabilita questa funzionalità per l'organizzazione corrente.

Per abilitare l'accettazione automatica delle reazioni:

1. Nella finestra di Web Console MDR passare alla voce di menu **Impostazioni**.
2. Fare clic sulla scheda **Incidenti**.
3. Selezionare una delle seguenti opzioni:

   - **Abilitato per tutti i tenant**

     Quando questa opzione è selezionata, l'accettazione automatica delle reazioni è abilitata sia per i tenant esistenti che per quelli appena creati.

   - **Abilitato per i tenant selezionati di seguito**

     Selezionare i tenant per i quali si desidera abilitare l'accettazione automatica delle reazioni. Per i tenant appena creati, l'accettazione automatica delle reazioni è disabilitata per impostazione predefinita.

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

L'accettazione automatica delle reazioni è abilitata e le azioni offerte nelle reazioni verranno eseguite automaticamente per tutti i tenant o per i tenant selezionati. È possibile disabilitare questa opzione in qualsiasi momento.

Diritti di accesso per visualizzare o modificare le impostazioni di accettazione automatica

I ruoli utente di Kaspersky Managed Detection and Response hanno i seguenti diritti di accesso alle impostazioni di accettazione automatica:

Operazione	Amministratore MDR	Senior Security Officer	Security Officer
Accedere alla scheda **Incidenti**	✓	✓	—
Modificare l'opzione attualmente selezionata	✓	—	—
Visualizzare l'opzione attualmente selezionata	✓	✓	—
Abilitare l'accettazione automatica per tutti i tenant	✓	—	—
Abilitare l'accettazione automatica per tenant specifici	✓	✓ (solo per i tenant a cui l'utente ha accesso)	—
Visualizzare l'impostazione di accettazione automatica di un tenant specifico	✓	✓ (solo per i tenant a cui l'utente ha accesso)	—

Accettazione automatica delle reazioni in Kaspersky Security Center

È possibile abilitare l'accettazione automatica delle reazioni offerte. In questo caso, le azioni di reazione proposte nelle reazioni, ad esempio l'eliminazione di un file infetto, verranno eseguite automaticamente. Quando questa funzionalità è disabilitata, le misure offerte nelle reazioni devono essere accettate o rifiutate manualmente.

Se si utilizzano i tenant, è possibile abilitare l'accettazione automatica delle reazioni per tutti i tenant o solo per i tenant selezionati. Se non si utilizzano i tenant, si abilita o si disabilita questa funzionalità per l'organizzazione corrente.

È possibile modificare le impostazioni di accettazione automatica se si dispone del ruolo utente Amministratore MDR. Gli utenti con il ruolo di Security Officer non sono autorizzati a modificare le impostazioni. Gli utenti con il ruolo di Senior Security Officer possono eseguire le seguenti operazioni:

- Visualizzare l'opzione attualmente selezionata
- Consentire la modifica dell'opzione di accettazione automatica delle reazioni per ciascun tenant Abilitare o disabilitare l'accettazione automatica delle reazioni per tenant specifici se è selezionata l'opzione **Consentire la modifica dell'opzione di accettazione automatica delle reazioni per ciascun tenant**

Per configurare l'accettazione automatica delle reazioni:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Impostazioni**.
2. Nel gruppo di parametri **Accettazione automatica delle reazioni**, selezionare l'opzione richiesta:
   - **Disabilita l'accettazione automatica delle risposte per tutti i tenant**

     Selezionare questa opzione se si desidera accettare o rifiutare manualmente le azioni di reazione.
   - **Consenti la modifica dell'opzione di accettazione automatica delle reazioni per tutti i tenant**

     Selezionare questa opzione se si desidera abilitare l'accettazione automatica delle reazioni per tutti i tenant dell'organizzazione, inclusi i tenant esistenti e quelli creati di recente.
   - **Consentire la modifica dell'opzione di accettazione automatica delle reazioni per ciascun tenant**

     Selezionare questa opzione se si desidera configurare l'accettazione automatica delle reazioni per ogni tenant individualmente. Selezionare quindi le caselle di controllo relative ai tenant per cui si desidera che le azioni di reazione vengano eseguite automaticamente. Per i tenant appena creati, l'accettazione automatica delle reazioni è disabilitata per impostazione predefinita.

     Se si seleziona l'opzione **Tutti i tenant**, l'accettazione automatica delle reazioni viene abilitata per i nuovi tenant creati per impostazione predefinita.
3. Fare clic sul pulsante **Salva**.

   Il pulsante **Salva** diventa attivo solo se sono state modificate le impostazioni.

Chiusura degli incidenti in Web Console MDR

È possibile chiudere un incidente se si sa che si tratta di un duplicato o che non verrà risolto. In altri casi, non è necessario chiudere gli incidenti in quanto devono essere risolti dagli analisti SOC di MDR. Gli analisti SOC di MDR risolvono un incidente se vengono applicate le misure che hanno consigliato all'interno di questo incidente. Un incidente risolto viene chiuso automaticamente 72 ore dopo.

Per chiudere un incidente:

1. In Web Console MDR passare alla voce di menu **Incidenti**.

   Verrà visualizzato l'elenco degli incidenti.
2. Fare clic sulla stringa con l'incidente di cui si desidera visualizzare i dettagli.

   Verrà visualizzata la pagina dell'incidente.
3. Nella scheda **Riepilogo** della pagina fare clic sul pulsante **Chiudi incidente** nella parte inferiore della finestra.

   Il pulsante **Chiudi incidente** non è disponibile per gli incidenti con stato **Chiuso**.

   Verrà visualizzata la sezione **Chiudi incidente**.

4. Nel campo **Motivo per cui si sta chiudendo questo incidente** specificare eventuali informazioni aggiuntive da comunicare agli analisti SOC di Kaspersky Managed Detection and Response. Ad esempio, è possibile fornire dettagli sul motivo per cui si ritiene che questo incidente sia una situazione standard, che non rappresenta una minaccia per l'infrastruttura. È possibile lasciare vuoto questo campo.

5. Sotto il campo del commento, selezionare l'opzione **Vero positivo** o **Falso positivo**, a seconda del motivo della chiusura.

   Selezionare l'opzione **Vero positivo** se Kaspersky Managed Detection and Response ha rilevato una minaccia, ma non si desidera che gli analisti SOC di MDR indaghino sull'incidente e lo risolvano.

   Selezionare l'opzione **Falso positivo** se Kaspersky Managed Detection and Response ha rilevato come minaccia un'attività che non è pericolosa. Kaspersky Managed Detection and Response utilizza queste informazioni per migliorare gli algoritmi di rilevamento automatico.

6. Nella parte inferiore della sezione fare clic sul pulsante **Chiudi**.

   La sezione **Chiudi incidente** verrà nascosta.

L'incidente verrà chiuso. Da questo momento, Kaspersky Managed Detection and Response non eseguirà alcuna azione in relazione a questo incidente.

Invio di un incidente al team di Reazione agli Incidenti per ulteriori indagini

È possibile inviare un incidente al team Incident Response per eseguire indagini. Questo servizio coinvolge l'insieme completo delle azioni di reazione, a partire dall'analisi iniziale e dalle azion di reazione anticipata, fino al rilevamento di ulteriori segnali di attacco e alla preparazione di un piano per l'eliminazione delle possibili conseguenze.

Quando si paga l'abbonamento al servizio, si ottiene un certo numero di ore di indagine. Le ore di indagine vengono utilizzate quando si invia un incidente al team Incident Response. Se non si dispone di orari per le indagini, è comunque possibile inviare un incidente per le indagini acquistando un servizio commerciale e creando manualmente una richiesta.

I risultati dell'indagine vengono ricevuti nella scheda **Comunicazione** dell'incidente.

Per inviare un incidente a IR Retainer:

1. Nella finestra di Web Console MDR passare alla voce di menu **Incidenti**.

   Verrà visualizzato l'elenco degli incidenti.

2. Fare clic sulla stringa con l'incidente che si desidera inviare al team Incident Response.

   Verrà visualizzata la pagina dell'incidente.

3. Nella sezione **Azioni** della scheda **Riepilogo**, eseguire una delle seguenti operazioni:

   - Se sono disponibili orari per le indagini, fare clic sul pulsante **Riassegna l'incidente al team IR**, quindi confermare che si desidera inviare l'incidente a IR Retainer.

   - Se non si dispone di orari per le indagini, fare clic sul collegamento, quindi compilare il modulo di creazione della richiesta per acquistare un servizio commerciale.

L'incidente viene inviato. Gli esperti del team Incident Response contatteranno l'utente tramite la console MDR il prima possibile dopo aver ricevuto l'incidente.

Utilizzo delle funzionalità di Kaspersky Endpoint Detection and Response Optimum

La soluzione Kaspersky Endpoint Detection and Response Optimum fornisce le seguenti funzionalità di reazione (di seguito denominate anche reazioni EDR) che è possibile eseguire e configurare manualmente.

- Isolamento di rete
- Sposta file in Quarantena
- Invia file a Cloud Sandbox
- Elimina file
- Esegui scansione delle aree critiche
- Scansione IOC
- Prevenzione dell'esecuzione
- Avvia processo
- Termina processo
- Ottieni file

Ulteriori dettagli su queste reazioni EDR sono disponibili nella Guida online di Kaspersky Endpoint Detection and Response Optimum.

Le reazioni EDR descritte in questa sezione sono disponibili per le risorse con Kaspersky Endpoint Security for Windows 11.7 o versioni successive. Se nelle risorse si utilizza Kaspersky Endpoint Security for Windows 11.6 o una versione precedente, Kaspersky Endpoint Agent deve essere installato su queste risorse per utilizzare le reazioni EDR.

Per attivare le funzioni di Kaspersky Endpoint Detection and Response Optimum, è necessario immettere uno dei seguenti codici di attivazione per le risorse tramite Kaspersky Security Center:

- Kaspersky Endpoint Detection and Response Optimum
- Componente aggiuntivo Kaspersky Endpoint Detection and Response Optimum

Per gestire le azioni di reazione agli avvisi EDR, in Kaspersky Security Center passare alla sezione **Monitoraggio e rapporti** → **Avvisi**.

.

Multi-tenancy

La multi-tenancy è un meccanismo che consente di diventare un fornitore Kaspersky Managed Detection and Response per altre organizzazioni. Una volta che si dispone di un account MDR, è possibile creare tenant nell'account MDR.

È possibile creare fino a 100 tenant nell'account MDR.

L'account in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console deve disporre di un ruolo con i seguenti diritti di accesso: **Accesso agli incidenti** e **Gestione dei tenant,** per poter visualizzare, aggiungere, modificare ed eliminare i tenant nella sezione **MDR** di Kaspersky Security Center.

Se l'organizzazione dispone di più licenze, è possibile gestire i tenant solo in Kaspersky Security Center.

Per diventare un fornitore MDR, è necessario avere accesso all'infrastruttura del tenant per poter eseguire scenari di distribuzione.

Tutti i tenant sono indipendenti e isolati, il che significa che nessuno dei dati di un tenant è accessibile da un altro tenant.

Solo gli utenti a cui è stato assegnato il ruolo di amministratore MDR possono aggiungere, modificare ed eliminare i tenant in Web Console MDR.

Gestione dei tenant in Kaspersky Security Center

Questa sezione fornisce informazioni sulla gestione dei tenant esistenti e sull'aggiunta di nuovi tenant in Kaspersky Security Center.

Visualizzazione dei tenant in Kaspersky Security Center

È possibile visualizzare i tenant disponibili utilizzando l'elenco dei tenant.

L'account in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console deve disporre di un ruolo con i seguenti diritti di accesso: **Accesso agli incidenti** e **Gestione dei tenant,** per poter visualizzare, aggiungere, modificare ed eliminare i tenant nella sezione **MDR** di Kaspersky Security Center.

Per visualizzare i tenant:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**. Ogni riga rappresenta un tenant. È possibile fare clic in qualsiasi punto della riga per visualizzare le informazioni sul tenant.

2. I seguenti attributi del tenant sono presenti sopra l'elenco:

   - **Nome**

     Un nome del tenant arbitrario e in formato leggibile specificato durante la creazione o la modifica del tenant. Il nome di un tenant può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 100 caratteri.

   - **Stato**

     Uno dei seguenti stati del tenant:

     - **Attivo**

       Un tenant può utilizzare Kaspersky Managed Detection and Response.

     - **Inattivo**

       Un tenant non può utilizzare Kaspersky Managed Detection and Response.

       È possibile impostare manualmente lo stato di inattività nella scheda tenant. Inoltre, lo stato inattivo viene impostato automaticamente alla fine del ciclo di vita del tenant.

   - **Numero di risorse**

     Numero di risorse assegnate al tenant.

   - **Descrizione**

     Informazioni in formato libero immesse durante la creazione o la modifica del tenant. È possibile specificare lo scopo del tenant o il numero previsto di risorse. La descrizione può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 2000 caratteri.

   - **Data di creazione**

     Data di creazione del tenant.

   - **Data di scadenza**

     Data di scadenza del tenant.

     I tenant sono ordinati in base alla data di scadenza in ordine decrescente.

È anche possibile visualizzare i tenant in Web Console MDR.

Visualizzazione delle impostazioni dei tenant in Kaspersky Security Center

È possibile visualizzare le impostazioni di ogni tenant nel proprio account.

L'account in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console deve disporre di un ruolo con i seguenti diritti di accesso: **Accesso agli incidenti** e **Gestione dei tenant,** per poter visualizzare, aggiungere, modificare ed eliminare i tenant nella sezione **MDR** di Kaspersky Security Center.

Per visualizzare le impostazioni del tenant:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**. Ogni riga rappresenta un tenant. È possibile fare clic in qualsiasi punto della riga per visualizzare le informazioni sul tenant.

2. Fare clic sulla riga con il tenant di cui si desidera visualizzare i dettagli.

   Verrà visualizzata la sezione **Impostazioni tenant**.

   L'impostazione inizia con l'interruttore **Attivo**, che mostra se un tenant è attivo o meno. Se necessario, è possibile spostare l'interruttore **Attivo**. Di seguito sono presenti i seguenti campi:

   - **Nome**

     Un nome del tenant arbitrario e in formato leggibile specificato durante la creazione o la modifica del tenant. Il nome di un tenant può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 100 caratteri.

   - **ID**

     Un IDS tenant univoco generato automaticamente.

   - **Descrizione**

     Informazioni in formato libero immesse durante la creazione o la modifica del tenant. È possibile specificare lo scopo del tenant o il numero previsto di risorse. La descrizione può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 2000 caratteri.

   - **Risorse assegnate**

     Numero di risorse assegnate al tenant.

   - **File di configurazione per il tenant**

     Questa sezione mostra informazioni sul file di configurazione MDR per il tenant:

     - **Licenza**: la licenza che corrisponde al tenant.
     - **Data di scadenza**: durata di vita del tenant. È possibile specificare manualmente la data di scadenza durante la creazione del tenant. La data di scadenza non può essere uguale o successiva all'ultimo giorno del periodo della licenza MDR.
     - **Azione**: è possibile fare clic sul collegamento **Scarica il file di configurazione** per scaricare l'archivio ZIP con il file di configurazione MDR.

     Fare clic sul pulsante **X** per eliminare un file di configurazione. È possibile eliminare un file di configurazione solo se si aggiunge un altro file di configurazione al tenant.

     Fare clic sul pulsante **Aggiungi** per aggiungere un nuovo file di configurazione. Specificare la licenza e la data di scadenza.

3. Nella parte inferiore della sezione **Impostazioni tenant** fare clic sul pulsante **Chiudi** per chiudere la sezione.

È anche possibile visualizzare le impostazioni del tenant in Web Console MDR.

Modifica delle impostazioni dei tenant in Kaspersky Security Center

È possibile modificare le impostazioni di ogni tenant nell'account.

L'account in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console deve disporre di un ruolo con i seguenti diritti di accesso: **Accesso agli incidenti** e **Gestione dei tenant,** per poter visualizzare, aggiungere, modificare ed eliminare i tenant nella sezione **MDR** di Kaspersky Security Center.

Per modificare le impostazioni del tenant:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**. Ogni riga rappresenta un tenant. È possibile fare clic in qualsiasi punto della riga per visualizzare le informazioni sul tenant.

2. Fare clic sulla riga con il tenant di cui si desidera modificare i dettagli.

   Verrà visualizzata la sezione **Impostazioni tenant**. Qui è possibile eseguire le seguenti azioni:

   - Attivare o disattivare il tenant tramite l'interruttore **Attivo**.
   - Modificare il valore del campo **Descrizione**.
   - Eliminare un file di configurazione facendo clic sul pulsante **X**. È possibile eliminare un file di configurazione solo se si aggiunge un altro file di configurazione al tenant.
   - Aggiungere un nuovo file di configurazione facendo clic sul pulsante **AD**. Specificare la licenza e la data di scadenza.

3. Nella parte inferiore della sezione **Impostazioni tenant** fare clic sul pulsante **Salva**.
   - La sezione **Impostazioni tenant** verrà nascosta. Dopo aver fatto clic sul pulsante **Salva**, Kaspersky Managed Detection and Response genera il nuovo file di configurazione MDR conforme alle impostazioni aggiornate del tenant. È possibile fare clic sul collegamento **Scarica il file di configurazione** per scaricare l'archivio ZIP con il file di configurazione MDR.

Le impostazioni del tenant verranno modificate. Le impostazioni aggiornate vengono applicate alle risorse dei gruppi di amministrazione selezionati.

È inoltre possibile modificare le impostazioni del tenant in Web Console MDR.

Aggiunta di nuovi tenant in Kaspersky Security Center

Se si desidera diventare un fornitore Kaspersky Managed Detection and Response per un'altra organizzazione, è necessario aggiungere un nuovo tenant al proprio account.

L'account in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console deve disporre di un ruolo con i seguenti diritti di accesso: **Accesso agli incidenti** e **Gestione dei tenant,** per poter visualizzare, aggiungere, modificare ed eliminare i tenant nella sezione **MDR** di Kaspersky Security Center.

Per aggiungere un nuovo tenant:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**.

2. Nella parte superiore della finestra fare clic sull'icona con il segno più (+).

   Verrà visualizzata la sezione **Impostazioni tenant**.

3. Se necessario, spostare l'interruttore **Attivo**.

   L'interruttore **Attivo** è attivato per impostazione predefinita.

4. Compilare i campi seguenti:

- **Nome**

  Un nome del tenant arbitrario e in formato leggibile specificato durante la creazione o la modifica del tenant. Il nome di un tenant può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 100 caratteri.

- **Descrizione**

  Informazioni in formato libero immesse durante la creazione o la modifica del tenant. È possibile specificare lo scopo del tenant o il numero previsto di risorse. La descrizione può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 2000 caratteri.

- **File di configurazione per il tenant**

  Questa sezione mostra informazioni sul file di configurazione MDR per il tenant:

  - **Licenza**: la licenza che corrisponde al tenant.
  - **Data di scadenza**: durata di vita del tenant. È possibile specificare manualmente la data di scadenza durante la creazione del tenant. La data di scadenza non può essere uguale o successiva all'ultimo giorno del periodo della licenza MDR.
  - **Azione**: è possibile fare clic sul collegamento **Scarica il file di configurazione** per scaricare l'archivio ZIP con il file di configurazione MDR.

  Fare clic sul pulsante **X** per eliminare un file di configurazione. È possibile eliminare un file di configurazione solo se si aggiunge un altro file di configurazione al tenant.

  Fare clic sul pulsante **Aggiungi** per aggiungere un nuovo file di configurazione. Specificare la licenza e la data di scadenza.

5. Nella parte inferiore della sezione **Impostazioni tenant** fare clic sul pulsante **Salva**.

   La sezione **Impostazioni tenant** verrà nascosta. Dopo aver fatto clic sul pulsante **Salva**, Kaspersky Managed Detection and Response genera un file di configurazione MDR per il nuovo tenant. È possibile fare clic sul collegamento **Scarica il file di configurazione** per scaricare l'archivio ZIP con il file di configurazione MDR.

Verrà aggiunto il nuovo tenant.

È anche possibile aggiungere nuovi tenant in Web Console MDR.

Eliminazione di tenant in Kaspersky Security Center

Quando si elimina un tenant che contiene alcune risorse, tutte le relative risorse vengono disconnesse dalla soluzione MDR. Per continuare a gestire le risorse del tenant, è possibile spostarle sul tenant radice o su un nuovo tenant prima di eliminare il tenant.

L'account in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console deve disporre di un ruolo con i seguenti diritti di accesso: **Accesso agli incidenti** e **Gestione dei tenant,** per poter visualizzare, aggiungere, modificare ed eliminare i tenant nella sezione **MDR** di Kaspersky Security Center.

Per eliminare un tenant:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**.

2. Nell'elenco **Tenant** spostare il puntatore del mouse sul tenant che si desidera eliminare, quindi fare clic sull'icona del cestino (🗑) a destra della riga.

3. Confermare l'eliminazione.

Il tenant selezionato verrà eliminato.

È anche possibile eliminare i tenant in Web Console MDR.

Spostamento delle risorse tra tenant

Quando si elimina un tenant che contiene alcune risorse, tutte le relative risorse interrompono l'invio della telemetria alla soluzione MDR. Prima di eliminare un tenant, spostare tutte le relative risorse nel tenant principale o in un nuovo tenant.

L'account in Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console deve disporre di un ruolo con i seguenti diritti di accesso: **Accesso agli incidenti** e **Gestione dei tenant,** per poter visualizzare, aggiungere, modificare ed eliminare i tenant nella sezione **MDR** di Kaspersky Security Center.

Per spostare le risorse in un nuovo tenant:

1. Nella sezione **MDR** di Kaspersky Security Center creare un nuovo tenant. In seguito verranno aggiunte risorse a questo tenant.

   Quando si crea un nuovo tenant, è necessario scaricare un file di configurazione MDR.

2. In Kaspersky Security Center Web Console creare un nuovo gruppo di amministrazione.

3. Aggiungere le risorse che si desidera spostare in un nuovo tenant nel nuovo gruppo di amministrazione.

4. Creare un nuovo criterio per Kaspersky Endpoint Agent o un'applicazione EPP per il gruppo di amministrazione creato.

5. Applicare il file di configurazione MDR al criterio creato.

   Per informazioni dettagliate sui diversi scenari di distribuzione, fare riferimento alla Distribuzione di Kaspersky Managed Detection and Response.

Dopo l'applicazione del criterio alle risorse del gruppo di amministrazione, le risorse vengono spostate dal tenant root al tenant appena creato.

Per spostare le risorse nel tenant principale:

1. Scaricare un file di configurazione MDR per il tenant principale:

   - In Web Console MDR (https://mdr.kaspersky.com/guide), passare alla sezione **Getting Started** e fare clic sul collegamento **file di configurazione di MDR**.

   - In Kaspersky Security Center Web Console o in Kaspersky Security Center Cloud Console, accedere a **MDR** > **Per iniziare** (Getting Started) e fare clic sul collegamento **Download**.

2. In Kaspersky Security Center Web Console creare un nuovo gruppo di amministrazione.

3. Aggiungere le risorse che si desidera spostare in un nuovo tenant nel nuovo gruppo di amministrazione.

4. Creare un nuovo criterio per Kaspersky Endpoint Agent o un'applicazione EPP per il gruppo di amministrazione creato.

5. Applicare il file di configurazione MDR al criterio creato.

   Dopo l'applicazione del criterio alle risorse del gruppo di amministrazione, le risorse vengono spostate dal tenant predefinito al tenant appena creato.

Gestione dei tenant in Web Console MDR

Questa sezione fornisce informazioni sulla gestione dei tenant in MDR Web Console.

Visualizzazione dei tenant in Web Console MDR

Per visualizzare i tenant:

1. Nella finestra di Web Console MDR passare alla voce di menu **Impostazioni**.
2. Fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**. Ogni riga rappresenta un tenant. È possibile fare clic in qualsiasi punto della riga per visualizzare le informazioni sul tenant.
3. I seguenti attributi del tenant sono presenti sopra l'elenco:

   - **Nome**

     Un nome del tenant arbitrario e in formato leggibile specificato durante la creazione o la modifica del tenant. Il nome di un tenant può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 100 caratteri.

   - **Stato**

     Uno dei seguenti stati del tenant:

     - **Attivo**

       Un tenant può utilizzare Kaspersky Managed Detection and Response.

     - **Inattivo**

       Un tenant non può utilizzare Kaspersky Managed Detection and Response.

       È possibile impostare manualmente lo stato di inattività nella scheda tenant. Inoltre, lo stato inattivo viene impostato automaticamente alla fine del ciclo di vita del tenant.

   - **Numero di risorse**

     Numero di risorse assegnate al tenant.

   - **Descrizione**

     Informazioni in formato libero immesse durante la creazione o la modifica del tenant. È possibile specificare lo scopo del tenant o il numero previsto di risorse. La descrizione può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 2000 caratteri.

   - **Data di creazione**

     Data di creazione del tenant.

   - **Data di scadenza**

Data di scadenza del tenant.

I tenant sono ordinati in base alla data di scadenza in ordine decrescente.

Visualizzazione delle impostazioni dei tenant in Web Console MDR

Per visualizzare le impostazioni del tenant:

1. In Web Console MDR passare alla voce di menu **Impostazioni**.
2. Fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**. Ogni riga rappresenta un tenant. È possibile fare clic in qualsiasi punto della riga per visualizzare le informazioni sul tenant.
3. Fare clic sulla riga con il tenant di cui si desidera visualizzare i dettagli.

   Verrà visualizzata la sezione **Impostazioni tenant**.

   L'impostazione inizia con l'interruttore **Attivo**, che mostra se un tenant è attivo o meno. Se necessario, è possibile spostare l'interruttore **Attivo**. Di seguito sono presenti i seguenti campi:

   - Nome del tenant

     Un nome del tenant arbitrario e in formato leggibile specificato durante la creazione o la modifica del tenant. Il nome di un tenant può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 100 caratteri.

   - Descrizione

     Informazioni in formato libero immesse durante la creazione o la modifica del tenant. È possibile specificare lo scopo del tenant o il numero previsto di risorse. La descrizione può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 2000 caratteri.

   - Numero di risorse

     Numero di risorse assegnate al tenant.

   - Durata

     Data di scadenza del file di configurazione del tenant.
4. Nella parte inferiore della sezione **Impostazioni tenant** fare clic sul pulsante **Annulla** per chiudere la sezione.

Modifica delle impostazioni dei tenant in Web Console MDR

La possibilità di aggiungere, modificare ed eliminare tenant è disponibile solo per l'utente a cui è assegnato il ruolo Amministratore MDR.

Per modificare le impostazioni del tenant:

1. Aprire la console MDR.
2. Nella sezione **Impostazioni** della console MDR fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**. Ogni riga rappresenta un tenant. È possibile fare clic in qualsiasi punto della riga per visualizzare le informazioni sul tenant.
3. Fare clic sulla riga con il tenant di cui si desidera modificare i dettagli.

   Verrà visualizzata la sezione **Impostazioni tenant**.
4. Se necessario, spostare l'interruttore **Attivo**.
5. Se necessario, modificare i valori dei campi.
6. Nella parte inferiore della sezione **Impostazioni tenant** fare clic sul pulsante **Salva**.

   La sezione **Impostazioni tenant** verrà nascosta. Dopo aver fatto clic sul pulsante **Salva**, Kaspersky Managed Detection and Response genera un nuovo file di configurazione MDR conforme alle impostazioni aggiornate del tenant.
7. Nell'elenco **Tenant** fare clic sulla riga con il tenant modificato.

   Verrà visualizzata la sezione **Impostazioni tenant**. Nella parte inferiore della sezione sono presenti due pulsanti per il download del file di configurazione MDR per la distribuzione del tenant:

   - **File per le risorse con KEA**

     File da utilizzare nella distribuzione per i programmi Kaspersky con Kaspersky Endpoint Agent.
   - **File per le risorse senza KEA**

     File da utilizzare nella distribuzione per Kaspersky Endpoint Security senza Kaspersky Endpoint Agent.
8. Fare clic sul pulsante **File per le risorse con KEA** o **File per le risorse senza KEA** per scaricare il nuovo file di configurazione MDR.
9. Nella parte inferiore della sezione **Impostazioni tenant** fare clic sul pulsante **Annulla** per chiudere la sezione.

Le impostazioni del tenant verranno modificate. Ora è necessario distribuire il nuovo file di configurazione MDR nelle risorse del tenant per applicare le impostazioni modificate.

Aggiunta di nuovi tenant in Web Console MDR

La possibilità di aggiungere, modificare ed eliminare tenant è disponibile solo per l'utente a cui è assegnato il ruolo Amministratore MDR.

Per aggiungere un nuovo tenant:

1. Nella finestra di Web Console MDR passare alla voce di menu **Impostazioni**.
2. Fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**.
3. Nella parte superiore della finestra fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la sezione **Impostazioni tenant**.
4. Se necessario, spostare l'interruttore **Attivo**.

   L'interruttore **Attivo** è attivato per impostazione predefinita.
5. Compilare i campi seguenti:

   - **Nome del tenant**

     Un nome del tenant arbitrario e in formato leggibile specificato durante la creazione o la modifica del tenant. Il nome di un tenant può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 100 caratteri.

   - **Descrizione**

     Informazioni in formato libero immesse durante la creazione o la modifica del tenant. È possibile specificare lo scopo del tenant o il numero previsto di risorse. La descrizione può contenere lettere latine, cifre e caratteri speciali. Non può contenere più di 2000 caratteri.

   - **Durata**

     Data di scadenza del file di configurazione del tenant.
6. Nella parte inferiore della sezione **Impostazioni tenant** fare clic sul pulsante **Salva**.

   La sezione **Impostazioni tenant** verrà nascosta. Dopo aver fatto clic sul pulsante **Salva**, Kaspersky Managed Detection and Response genera un file di configurazione MDR per il nuovo tenant.
7. Nell'elenco **Tenant** fare clic sulla riga con il nuovo tenant.

   Verrà visualizzata la sezione **Impostazioni tenant**. In questo blocco, è possibile scaricare il file di configurazione MDR per la distribuzione del tenant:

8. Fare clic sul pulsante **File per le risorse con KEA** o **File per le risorse senza KEA** per scaricare il nuovo file di configurazione MDR.

9. Nella parte inferiore della sezione **Impostazioni tenant** fare clic sul pulsante **Annulla** per chiudere la sezione.

Verrà aggiunto il nuovo tenant. Ora è possibile distribuire il file di configurazione MDR scaricato nelle risorse del tenant.

I tenant creati nella console MDR non sono disponibili nella sezione **MDR** di Kaspersky Security Center. Utilizzare Web Console MDR per lavorare con questi tenant.

Eliminazione di tenant in Web Console MDR

Quando si elimina un tenant che contiene alcune risorse, tutte le relative risorse vengono disconnesse dalla soluzione MDR. Gli incidenti assegnati a un tenant eliminato non sono più disponibili. Questa azione è irreversibile. Prima di eliminare un tenant, spostare tutte le relative risorse nel tenant principale o in un nuovo tenant.

La possibilità di aggiungere, modificare ed eliminare tenant è disponibile solo per l'utente a cui è assegnato il ruolo Amministratore MDR.

Per eliminare un tenant:

1. In Web Console MDR passare alla voce di menu **Impostazioni**.

2. Fare clic sulla scheda **Tenant**.

   Verrà visualizzato l'elenco **Tenant**.

3. Nell'elenco dei tenant, passare il cursore del mouse sul tenant che si desidera eliminare e fare clic sul pulsante **Elimina tenant** con l'icona del cestino a destra.

   Viene visualizzata la finestra **Conferma eliminazione tenant**.

4. Fare clic sul pulsante **Elimina** per eliminare il tenant.

I tenant creati nella console MDR non sono disponibili nella sezione **MDR** di Kaspersky Security Center. Utilizzare Web Console MDR per lavorare con questi tenant.

Gestione della soluzione tramite l'API REST

Questa funzionalità è disponibile in MDR Expert, MDR Advanced (disponibile solo in alcune regioni) e MDR Prime (disponibile solo in alcune regioni). Vedere il confronto delle soluzioni di licenza in questa sezione.

Per avere accesso all'API REST in Kaspersky Security Center, l'account in Kaspersky Security Center Web Console deve disporre dei seguenti diritti di accesso: Accesso agli incidenti e Accesso all'API REST.

Per alcuni livelli di licenza commerciale sarà solo possibile generare un token di aggiornamento in Web Console MDR per utilizzarlo per la configurazione del plug-in MDR, senza accesso all'API REST in Kaspersky Security Center.

Kaspersky Managed Detection and Response consente di ottenere, creare e aggiornare a livello di codice entità MDR tramite l'API REST. L'API REST opera tramite HTTP e comprende un set di metodi di richiesta/risposta. In altre parole, è possibile gestire Kaspersky Managed Detection and Response tramite una soluzione di terze parti, anziché con Web Console MDR.

Per iniziare a utilizzare l'API REST, è necessario creare un token di aggiornamento e un token di accesso.

APRIRE IL RIFERIMENTO PER L'API REST

Scenario: esecuzione dell'autorizzazione basata su token

In questo scenario viene illustrato come eseguire un'autorizzazione basata su token per l'utilizzo con l'API REST.

Prerequisiti

Assicurarsi di disporre di un account MDR a cui è assegnato uno dei seguenti ruoli:

- Il ruolo Amministratore MDR
- Un ruolo personalizzato con i seguenti diritti di accesso (applicabile solo per Kaspersky Security Center):
  - Accesso agli incidenti
  - Accesso all'API REST

Fasi

L'autorizzazione basata su token procede per fasi:

1. **Creazione di un token di aggiornamento in Web Console MDR**

   È necessario un token di aggiornamento per creare un token di accesso. Un token di aggiornamento è valido per 24 ore. È possibile utilizzare un token di aggiornamento solo una volta.

2 **Creazione di un token di accesso tramite l'API REST**

È necessario un token di accesso per utilizzare l'API REST. Un token di accesso è valido per 1 ora. È possibile utilizzare più volte un token di accesso durante il relativo ciclo di vita.

Quando si crea un token di accesso, l'API REST genera un nuovo token di aggiornamento e lo include nella risposta. Alla scadenza del token di accesso, è possibile creare un nuovo token di accesso utilizzando il token di aggiornamento più recente generato dall'API.

Un token di aggiornamento generato dall'API è valido per 7 giorni.

Risultati

Al termine di questo scenario, è possibile iniziare a utilizzare l'API REST inviando richieste con il token di accesso.

Creazione di una connessione API in Kaspersky Security Center

Quando si crea una nuova connessione API, viene generato un token di aggiornamento. Un *token di aggiornamento* è una sequenza univoca di lettere, cifre e simboli. Una volta creato, un token di aggiornamento consente di creare un token di accesso.

Per creare una connessione API:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **API**.

   Verrà visualizzato l'elenco **Connessioni API**.

2. Nella parte superiore della finestra fare clic sull'icona con il segno più (+).

   Verrà visualizzata la sezione **Aggiungere una nuova connessione API**.

3. Specificare le seguenti impostazioni:

- **Nome connessione**

  Il nome di una connessione può contenere lettere latine, cifre e caratteri speciali. Il nome di una connessione viene specificato come `author_name` nelle risposte API REST e visualizzato come autore del commento nella scheda **Comunicazione** di un incidente.

- **Diritti di accesso**

  Selezionare quali diritti di accesso concedere per l'esecuzione di azioni tramite l'API HTTP:

  - Accesso completo, oltre ad API e tenant

    Diritti di accesso del ruolo Amministratore MDR. Un amministratore MDR è un utente con privilegi avanzati che ha accesso a tutte le funzioni di Kaspersky Managed Detection and Response concesse dalla licenza. L'amministratore MDR può concedere l'accesso alle origini dati client ad altri utenti. L'utente che attiva Kaspersky Managed Detection and Response diventa automaticamente l'amministratore MDR. Pertanto, è consigliabile utilizzare un indirizzo e-mail aziendale per il processo di attivazione invece di un indirizzo e-mail personale. La creazione dell'amministratore MDR con un indirizzo e-mail personale può comportare rischi per la sicurezza, come il furto dell'account dell'amministratore MDR.

    In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	✓	—
Gestione delle reazioni	✓	—
Gestione dei tenant	✓	—
Pianificazione per il riepilogo incidenti	✓	—
Accesso all'API REST	✓	—

  - Accesso agli incidenti, gestione delle reazioni e impostazioni di accettazione automatica

    Diritti di accesso del ruolo Senior Security Officer. Un Senior Security Office è un dipendente che ha accesso alle funzioni di Kaspersky Managed Detection and Response concesse dalla licenza, ma non ha accesso all'API REST. Il Senior Security Officer ha il diritto di accettare e rifiutare le reazioni.

    In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	✓	—
Gestione delle reazioni	✓	—
Gestione dei tenant	—	✓
Pianificazione per il riepilogo incidenti	—	✓
Accesso all'API REST	—	✓

  - Accesso agli incidenti

Diritti di accesso del ruolo Security Officer. Un Security Officer è un dipendente che ha accesso alle funzioni di Kaspersky Managed Detection and Response concesse dalla licenza, ma non ha accesso all'API REST. Il Security Officer non può accettare e rifiutare le reazioni.

In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	—	✓
Gestione delle reazioni	—	✓
Gestione dei tenant	—	✓
Pianificazione per il riepilogo incidenti	—	✓
Accesso all'API REST	—	✓

- **Tenant**

  Se necessario, selezionare il valore (o i valori) nell'elenco a discesa **Tenant**.

  L'utente può visualizzare solo le risorse e gli incidenti relativi ai tenant specificati.

4. Fare clic sul pulsante **Genera**.

   Verrà visualizzato il campo **Token JWT**.

5. Fare clic sul pulsante **Chiudi**.

   La nuova connessione API viene visualizzata nell'elenco **Connessioni API**. Ora è possibile utilizzare il token di aggiornamento per creare un token di accesso.

È inoltre possibile creare connessioni API in Web Console MDR.

Creazione di una connessione API in Web Console MDR

Un *token di aggiornamento* è una sequenza univoca di lettere, cifre e simboli. Una volta creato, un token di aggiornamento consente di creare un token di accesso.

Per creare un token di aggiornamento:

1. Nella finestra di Web Console MDR passare alla voce di menu **Impostazioni**.
2. Fare clic sulla scheda **API**.

   Verrà visualizzato l'elenco **Tutti i token**.
3. Nella parte superiore della finestra fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la sezione **Genera token**.

4. Specificare le seguenti impostazioni:

- **Nome connessione**

  Il nome di un token.

  Il nome di un token può contenere lettere dell'alfabeto latino, cifre e caratteri speciali. Il nome di un token viene specificato come `author_name` nelle risposte API REST e visualizzato come autore del commento nella scheda **Comunicazione** di un incidente.

  > Per alcuni livelli di licenza commerciale, si tratta dell'unico campo disponibile durante la creazione di un token di aggiornamento.

- **Ruolo utente**

  Il ruolo utente per specificare le autorizzazioni che verranno concesse per l'esecuzione di azioni tramite l'API HTTP.

  Sono disponibili i seguenti ruoli utente:

  - Amministratore MDR

    L'utente con privilegi avanzati che ha accesso a tutte le funzioni di Kaspersky Managed Detection and Response concesse dalla licenza. L'amministratore MDR può concedere l'accesso alle origini dati client ad altri utenti. L'utente che attiva Kaspersky Managed Detection and Response diventa automaticamente l'amministratore MDR. Pertanto, è consigliabile utilizzare un indirizzo e-mail aziendale per il processo di attivazione invece di un indirizzo e-mail personale. La creazione dell'amministratore MDR con un indirizzo e-mail personale può comportare rischi per la sicurezza, come il furto dell'account dell'amministratore MDR.

    In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	✓	—
Gestione delle reazioni	✓	—
Gestione dei tenant	✓	—
Pianificazione per il riepilogo incidenti	✓	—
Accesso all'API REST	✓	—

  - Senior Security Officer

Un dipendente che ha accesso alle funzioni di Kaspersky Managed Detection and Response concesse dalla licenza, ma non ha accesso all'API REST. Il Senior Security Officer ha il diritto di accettare e rifiutare le reazioni.

In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	✓	—
Gestione delle reazioni	✓	—
Gestione dei tenant	—	✓
Pianificazione per il riepilogo incidenti	—	✓
Accesso all'API REST	—	✓

- Security Officer

  Un dipendente che ha accesso alle funzioni di Kaspersky Managed Detection and Response concesse dalla licenza, ma non ha accesso all'API REST. Il Security Officer non può accettare e rifiutare le reazioni.

  In Kaspersky Security Center questo ruolo corrisponde ai seguenti diritti di accesso:

Area funzionale	Consenti	Nega
Accesso agli incidenti	✓	—
Impostazioni di accettazione automatica	—	✓
Gestione delle reazioni	—	✓
Gestione dei tenant	—	✓
Pianificazione per il riepilogo incidenti	—	✓
Accesso all'API REST	—	✓

- **Tenant**

  Se necessario, selezionare il valore (o i valori) nell'elenco a discesa **Tenant**.

  Vengono suggeriti i tenant già esistenti nella console e il valore **Tenant radice**.

  L'utente può visualizzare solo le risorse e gli incidenti relativi ai tenant specificati. Se sono presenti risorse e incidenti non assegnati ad alcun tenant, l'utente può visualizzarli se si seleziona il valore **Tenant radice**.

  È possibile selezionare il valore **Tenant radice** oltre a specificare i nomi dei tenant.

5. Nella parte inferiore della sezione fare clic sul pulsante **Genera**.

   La sezione **Informazioni token** sostituirà la sezione **Genera token**.

6. Fare clic sul pulsante **Chiudi** nella parte inferiore della sezione **Informazioni token**.

   Il token di aggiornamento creato viene visualizzato nell'elenco **Tutti i token**. Ora è possibile utilizzare questo token di aggiornamento per creare un token di accesso.

Modifica di una connessione API in Kaspersky Security Center

È possibile modificare le connessioni API esistenti.

Per modificare una connessione API:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **API**.
   Verrà visualizzato l'elenco **Connessioni API**.
2. Fare clic sulla connessione API che si desidera modificare.
   Verrà visualizzata una sezione contenente le informazioni sulla connessione.
3. Modificare le impostazioni di connessione.
4. Fare clic sul pulsante **Salva**.

Le nuove impostazioni della connessione API selezionata vengono salvate.

Modifica di una connessione API in Web Console MDR

È possibile modificare le connessioni API esistenti.

Per modificare una connessione API:

1. In Web Console MDR fare clic sulla scheda **API**.
   Verrà visualizzato l'elenco **Tutti i token**.
2. Fare clic sul token della connessione API che si desidera modificare.
   Verrà visualizzata una sezione contenente le informazioni sulla connessione.
3. Modificare le impostazioni di connessione.
4. Fare clic sul pulsante **Salva**.

Le nuove impostazioni della connessione API selezionata vengono salvate.

Creazione di un token di accesso in Kaspersky Security Center

Un *token di accesso* è una sequenza univoca di caratteri (lettere, cifre e caratteri speciali) che autorizza a utilizzare i metodi dell'API REST.

Per creare un token di accesso:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **API**.
   Verrà visualizzato l'elenco **Connessioni API**.
2. Fare clic su una connessione con stato **Attivazione in sospeso**.
   Verrà visualizzata una sezione contenente le informazioni sulla connessione.
3. Nel campo **Token JWT** fare clic sul pulsante **Aggiorna**.
   Verrà visualizzato un token di aggiornamento.
4. Selezionare e salvare il valore nel campo **ID cliente**.
5. Selezionare e salvare la sequenza di caratteri del token negli Appunti.
6. Inviare una richiesta POST all'endpoint `/session/confirm`.
   Sostituire `{client_id}` e `{refresh_token}` con i valori selezionati e salvati nei passaggi precedenti.

Esempio (Python):

```
##################################################
# Parte generale
##################################################

import time
import datetime
import requests
import jwt

# Il certificato è richiesto per l'autenticazione di una risorsa esterna
# È possibile scaricare il certificato da https://mdr.kaspersky.com,
# salvarlo sul disco e aggiungere il percorso nella variabile:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# L'ID del client e i token
# Per i dettagli su come ottenere l'ID e i token, fare riferimento alla guida https://support.kaspersky.com/MDR/it-IT/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f"  # (Incollare il valore)
REFRESH_TOKEN = "ReFrEsHToKeN"  # (Incollare il valore)
ACCESS_TOKEN = "AcCeSsToKeN"  # (Incollare il valore)


##################################################
# Ottenere il token di accesso e un token di aggiornamento per l'aggiornamento successivo del token di accesso
##################################################

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN data e ora di scadenza: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN è attuale")
    else:
        print(
            "È necessario aggiornare REFRESH_TOKEN; prelevarlo dalla Console MDR (https://support.kaspersky.com/MDR/en-US/258285.htm)"
        )
        exit()
else:
    print(
        "È necessario compilare il valore REFRESH_TOKEN; prelevarlo dalla Console MDR (https://support.kaspersky.com/MDR/en-US/258285.htm)"
    )
    exit()

# Verificare la presenza e la validità del token di accesso
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN data e ora di scadenza: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN è attuale")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# Se necessario, aggiornare il token di accesso e aggiornare il token per il prossimo aggiornamento del token di accesso
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body, verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    #  È necessario salvare il token di aggiornamento per ottenere il token di accesso successivo alla scadenza del token di accesso corrente
    refresh_token = result_json["refresh_token"]
    print(
        f'Il nuovo REFRESH_TOKEN per l'orario successivo per la richiesta ACCESS_TOKEN (sostituire il valore di REFRESH_TOKEN con questo valore): "
{refresh_token}"'
    )

    #  È necessario un nuovo token di accesso per recuperare i dati
    access_token = result_json["access_token"]
    print(f'Il nuovo ACCESS_TOKEN (sostituire il valore di ACCESS_TOKEN con questo valore): "{access_token}"')

# Il token di accesso viene aggiunto all'intestazione della richiesta
headers = {"Authorization": f"Bearer {access_token}"}
```

Esempio (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

L'API REST invia una risposta con il token di accesso e un nuovo token di aggiornamento:

```
{
"access_token": "SamPLET346yoKEnSamPLEToK25EnSamPLEToK35EnS",
"refresh_token": "tOKenSaMPlet259OKenS123aMPle926tOKenSaMPle"
}
```

Ora è possibile inviare richieste all'API REST utilizzando il token di accesso. Ogni richiesta all'API REST richiede un token di accesso. Una richiesta senza token di accesso restituirà solo un errore di autorizzazione.

È inoltre possibile creare un token di accesso in Web Console MDR.

Creazione di un token di accesso in Web Console MDR

Per creare un token di accesso:

1. Nella finestra di Web Console MDR passare alla voce di menu **Impostazioni**.
2. Fare clic sulla scheda **API**.

   Verrà visualizzato l'elenco **Tutti i token**. Ogni riga rappresenta un token. È possibile fare clic in qualsiasi punto della riga per visualizzare le informazioni sul token.
3. Fare clic su un token con stato **Attivazione in sospeso**.

   Verrà visualizzata una sezione **Informazioni token**.
4. Nel campo **Token JWT** fare clic sul pulsante **Aggiorna**.

   Verrà visualizzato un token di aggiornamento.
5. Selezionare e salvare il valore nel campo **ID cliente**.
6. Selezionare e salvare la sequenza di caratteri del token negli Appunti.
7. Inviare una richiesta POST all'endpoint `/session/confirm` (vedere gli esempi di seguito).

   Sostituire `{client_id}` e `{refresh_token}` con i valori selezionati e salvati nei passaggi precedenti.

Esempio (Python):

```
##################################################
# Parte generale
##################################################

import time
import datetime
import requests
import jwt

# Il certificato è richiesto per l'autenticazione di una risorsa esterna
# È possibile scaricare il certificato da https://mdr.kaspersky.com,
# salvarlo sul disco e aggiungere il percorso nella variabile:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# L'ID del client e i token
# Per i dettagli su come ottenere l'ID e i token, fare riferimento alla guida https://support.kaspersky.com/MDR/it-IT/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f"  # (Incollare il valore)
REFRESH_TOKEN = "ReFrEsHToKeN"  # (Incollare il valore)
ACCESS_TOKEN = "AcCeSsToKeN"  # (Incollare il valore)


##################################################
# Ottenere il token di accesso e un token di aggiornamento per l'aggiornamento successivo del token di accesso
##################################################

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN data e ora di scadenza: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN è attuale")
    else:
        print(
            "È necessario aggiornare REFRESH_TOKEN; prelevarlo dalla Console MDR (https://support.kaspersky.com/MDR/en-US/258285.htm)"
        )
        exit()
else:
    print(
        "È necessario compilare il valore REFRESH_TOKEN; prelevarlo dalla Console MDR (https://support.kaspersky.com/MDR/en-US/258285.htm)"
    )
    exit()

# Verificare la presenza e la validità del token di accesso
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN data e ora di scadenza: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN è attuale")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# Se necessario, aggiornare il token di accesso e aggiornare il token per il prossimo aggiornamento del token di accesso
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body, verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    #  È necessario salvare il token di aggiornamento per ottenere il token di accesso successivo alla scadenza del token di accesso corrente
    refresh_token = result_json["refresh_token"]
    print(
        f'Il nuovo REFRESH_TOKEN per l'orario successivo per la richiesta ACCESS_TOKEN (sostituire il valore di REFRESH_TOKEN con questo valore): "
{refresh_token}"'
    )

    #  È necessario un nuovo token di accesso per recuperare i dati
    access_token = result_json["access_token"]
    print(f'Il nuovo ACCESS_TOKEN (sostituire il valore di ACCESS_TOKEN con questo valore): "{access_token}"')

# Il token di accesso viene aggiunto all'intestazione della richiesta
headers = {"Authorization": f"Bearer {access_token}"}
```

Esempio (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

L'API REST invia una risposta con il token di accesso e un nuovo token di aggiornamento:

```
{
"access_token": "SamPLET346yoKEnSamPLEToK25EnSamPLEToK35EnS",
"refresh_token": "tOKenSaMPlet259OKenS123aMPle926tOKenSaMPle"
}
```

Ora è possibile inviare richieste all'API REST utilizzando il token di accesso. Ogni richiesta all'API REST richiede un token di accesso. Una richiesta senza token di accesso restituirà solo un errore di autorizzazione.

Utilizzo dell'API REST

L'utilizzo di MDR tramite l'API REST include l'acquisizione, la creazione e l'aggiornamento di risorse, incidenti e utenti.

APRIRE IL RIFERIMENTO PER L'API REST

I metodi dell'API REST richiedono il valore `client_id`. È possibile ottenere il valore `client_id` nella sezione **Informazioni token** di qualsiasi token di aggiornamento in Web Console MDR.

Di seguito sono riportati esempi di script per Python e Shell che dimostrano le funzionalità principali dell'API REST:

- Definire il percorso del certificato, l'URL dell'API REST, l'ID client e i token
- Ottenere il token di accesso e un token di aggiornamento per l'aggiornamento successivo del token di accesso
- Ottenere il numero di risorse
- Ottenere l'elenco delle risorse o i dettagli delle risorse
- Ottenere il numero di incidenti, l'elenco degli incidenti o i dettagli dell'incidente
- Ottenere l'elenco delle risposte per l'incidente
- Confermare, rifiutare la risposta o aggiornare l'elenco delle risposte
- Ottenere l'elenco dei commenti per l'incidente specificato o creare un nuovo commento per l'incidente specificato

Esempio (Python):

```
##################################################
#  Parte generale
##################################################

import time
import datetime
import requests
import jwt

#  Il certificato è richiesto per l'autenticazione di una risorsa esterna
#  È possibile scaricare il certificato da https://mdr.kaspersky.com,
#  salvarlo sul disco e aggiungere il percorso nella variabile:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

#  MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

#  L'ID del client e i token
#  Per i dettagli su come ottenere l'ID e i token, fare riferimento alla guida
https://support.kaspersky.com/MDR/it-IT/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f"  # ( Incollare il valore )
REFRESH_TOKEN = "ReFrEsHToKeN"  # ( Incollare il valore )
ACCESS_TOKEN = "AcCeSsToKeN"  # ( Incollare il valore )


##################################################
#  Ottenere il token di accesso e un token di aggiornamento per l'aggiornamento successivo del token di accesso
##################################################

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN  data e ora di scadenza:  {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN  è attuale ")
    else:
        print(
            " È necessario aggiornare  REFRESH_TOKEN;  prelevarlo dalla Console MDR
(https://support.kaspersky.com/MDR/en-US/258285.htm) "
        )
        exit()
else:
    print(
        " È necessario compilare il valore  REFRESH_TOKEN ; prelevarlo dalla Console MDR
(https://support.kaspersky.com/MDR/en-US/258285.htm) "
    )
    exit()

#  Verificare la presenza e la validità del token di accesso
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN  data e ora di scadenza:  {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN  è attuale ")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

#  Se necessario, aggiornare il token di accesso e aggiornare il token per il prossimo aggiornamento del token di
accesso
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body,
verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    #  È necessario salvare il token di aggiornamento per ottenere il token di accesso successivo alla scadenza
del token di accesso corrente
    refresh_token = result_json["refresh_token"]
    print(
```

```
        f' 'Il nuovo REFRESH_TOKEN per l'orario successivo per la richiesta ACCESS_TOKEN (sostituire il valore di
REFRESH_TOKEN con questo valore) : "{refresh_token}"'
    )

    #  È necessario un nuovo token di accesso per recuperare i dati
    access_token = result_json["access_token"]
    print(f' Il nuovo ACCESS_TOKEN (sostituire il valore di ACCESS_TOKEN con questo valore):  "{access_token}"')

# Il token di accesso viene aggiunto all'intestazione della richiesta
headers = {"Authorization": f"Bearer {access_token}"}


##################################################
# Ottenere il numero di risorse
##################################################

# La data e l'ora sono espresse in millisecondi da 1970-01-01T00:00:00Z
request_body = {
    "max_last_seen": int(time.time())
    * 1000,  # Limitazione dell'ora massima per l'ultima visualizzazione della risorsa all'ora corrente
    "min_last_seen": 1639311132000,  # Limitazione dell'ora minima per l'ultima visualizzazione della risorsa con
la costante - Domenica, 12 dicembre 2021 12:12:12 (GMT)
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


##################################################
# Ottenere l'elenco delle risorse
##################################################

request_body = {
#  Parametri di ricerca:
    "max_last_seen": int(time.time())
    * 1000,  # Limitazione dell'ora massima per l'ultima visualizzazione della risorsa all'ora corrente
    "min_last_seen": 1639311132000,  # Limitazione dell'ora minima per l'ultima visualizzazione della risorsa con
la costante - Domenica, 12 dicembre 2021 12:12:12 (GMT)
    "domain": "",
    "host_names": ["MA-MDR-KES-S", "SIN-MDR-KSC"],  # (Incollare il valore) Elenco nomi host
    "is_isolated": False,
    "network_interface": "10.70.104.1",
    "os_version": "Windows",  # La risorsa deve contenere la riga specificata nel nome del sistema operativo
    "product": "",
    "search_phrase": "mdr",  # Frase da cercare per contenuto campo:  "host_name", "domain",
"installed_product_info", "network_interfaces", "os_version"
    "statuses": ["OK", "ABSENT"],  # Ricerca delle risorse con gli stati correnti elencati qui
    #  Opzioni per la visualizzazione dei risultati della ricerca:
    "sort": "first_seen:asc",  # Ordinare i risultati in base all'ora della prima occorrenza; in caso di recupero
dei risultati pagina per pagina, è necessario specificare un campo per l'ordinamento che non cambierà da query a
query, ad esempio  "first_seen"  (non specificare campi i cui valori cambiano continuamente, ad esempio il campo
"last_seen" ; questo può portare a risultati errati)
    "page_size": 100,  # Risorse per pagina - 100
    "page": 1,  # Ottenere la prima pagina dei risultati di ricerca
    "version": 2, # Versione della soluzione
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


##################################################
# Ottenere i dettagli della risorsa
##################################################

request_body = {
    "asset_id": "0xFA6A68CC9A9415963DE841048A3BE929",  # (Incollare il valore) ID risorsa
    "version": 2,  # Versione della soluzione
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
).json()
print(result)


##################################################
```

```
# Ottenere il numero degli incidenti
#####################################################

request_body = {
    "max_update_time": int(time.time())
    * 1000,  # Limitare l'ora massima dell'ultimo aggiornamento dell'incidente all'ora corrente
    "min_update_time": 1639311132000,  # Limitazione dell'ora minima dell'ultimo aggiornamento dell'incidente con
la costante - Domenica 12 dicembre 2021 12:12:12 (GMT)
    "affected_hosts": [
        "MA-MDR-KES-S:0xFA6A68CC9A94145456E841048A3BE929"
    ],  # (Incollare il valore) Elenco degli host in formato "host_name:asset_id"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Ottenere l'elenco degli incidenti
#####################################################

request_body = {
# Parametri di ricerca:
    "max_creation_time": int(time.time())
    * 1000,  # Limitare l'ora massima di creazione dell'incidente all'ora corrente
    "min_creation_time": 1639311132000,  # Limitazione dell'ora minima per la creazione dell'incidente con la
costante - Domenica 12 dicembre 2021 12:12:12 (GMT)
    "asset_ids": [
        "0xFA6A68CC9A9415963DE841048A3BE929"
    ], # (Incollare il valore) Elenco delle risorse per cui si ottengono gli incidenti
    "priorities": ["HIGH"],
    "resolutions": ["True positive"],
    "response_statuses": ["Confirmed"],
    "response_types": ["hash"],
    "statuses": ["Closed"],
    # Parametri per fornire risultati
    "markdown_to_html": True,  # Risultati in formato HTML; se il valore è "False", i risultati sono in formato
Markdown
    "sort": "creation_time:asc",  # Ordinare i risultati in base alla data e all'ora di creazione dell'incidente;
in caso di recupero dei risultati pagina per pagina, è necessario specificare un campo per l'ordinamento che non
cambierà da query a query, ad esempio "creation_time" (non specificare campi i cui valori cambiano continuamente,
ad esempio il campo "update_time"; questo può portare a risultati errati)
    "page_size": 100,  # Incidenti per pagina - 100
    "page": 1,  # Ottenere la prima pagina dei risultati di ricerca
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Ottenere i dettagli degli incidenti
#####################################################

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m",  # (Incollare il valore) ID incidente
    "markdown_to_html": True,  # Risultati in formato HTML; se il valore è "False", i risultati sono in formato
Markdown
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Ottenere un elenco di reazioni per l'incidente
#####################################################

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m",  # (Incollare il valore) ID incidente
    "page_size": 10,  # Reazioni per pagina - 10
    "page": 1,  # Ottenere la prima pagina dei risultati di ricerca
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
```

```
)
print(result.json())


#####################################################
# Confermare la reazione
#####################################################

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W",  # (Incollare il valore) ID reazione
    "comment": "comment_text",  # Commento da aggiungere alla reazione
    "status": "Confirmed", # Nuovo stato della reazione - "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Rifiutare la reazione
#####################################################

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W",  # (Incollare il valore) ID reazione
    "comment": "comment_text",  # Commento da aggiungere alla reazione
    "status": "Declined",  # Nuovo stato della reazione - "Declined"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())


#####################################################
# Aggiornare l'elenco delle reazioni
#####################################################

request_body = {
    "responses_ids": [
        "CEgYG4UBMUGN-LWULP7W",
        "2ESl6IgB4cAOUyXBb5IB",
    ],  # (Incollare i valori) ID reazione
    "comment": "comment_text",  # Commento da aggiungere alle reazioni
    "status": "Confirmed",  # Nuovo stato delle reazioni - "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())
```

Esempio (Shell):

```
# Ottenere il token di accesso e il nuovo token di aggiornamento
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d
'{"refresh_token": "{refresh_token}"}'
# Esempio di risposta; successivamente, è necessario utilizzare access_token per recuperare i dati e refresh_token
per recuperare il nuovo token di accesso e il token di aggiornamento.
{
"access_token": "SamPLET346yoKEnSamPLEToK25EnSamPLEToK35EnS",
"refresh_token": "tOKenSaMPlet259OKenS123aMPle926tOKenSaMPle"
}

# Ottenere il numero di risorse
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/count -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"max_last_seen": 1704103200000, "min_last_seen": 1704762000000}'

# Ottenere l'elenco delle risorse
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/list -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"max_last_seen": 1704103200000, "min_last_seen": 1704762000000,
"domain": "", "host_names": ["MA-MDR-KES-S","SIN-MDR-KSC"], "is_isolated": false, "network_interface":
"10.70.104.1", "os_version": "Windows", "product": "", "search_phrase": "mdr", "statuses": ["OK","ABSENT"],
"sort": "first_seen:asc", "page_size": 100, "page": 1, "version": 2}'

# Ottenere i dettagli della risorsa
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/details -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"asset_id": "0xFA6A68CC9A9415963DE841048A3BE929", "version": 2}'

# Ottenere il numero degli incidenti
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/count -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"max_update_time": 1704103200000, "min_update_time": 1704762000000,
"affected_hosts": ["MA-MDR-KES-S:0xFA6A68CC9A9415963DE841048A3BE929"]}'

# Ottenere l'elenco degli incidenti
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/list -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"max_creation_time": 1704103200000, "min_creation_time":
1704762000000, "asset_ids": ["0xFA6A68CC9A9415963DE841048A3BE929"], "priorities": ["HIGH"], "resolutions": ["True
positive"], "response_statuses": ["Confirmed"], "response_types": ["hash"], "statuses": ["Closed"],
"markdown_to_html": true, "sort": "creation_time:asc", "page_size": 100, "page": 1}'

# Ottenere i dettagli degli incidenti
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/details -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"incident_id": "60gWG4UBMUGN-LWUuv1m", "markdown_to_html": true}'

# Ottenere un elenco di reazioni per l'incidente
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/responses/list -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"incident_id": "60gWG4UBMUGN-LWUuv1m", "page_size": 10, "page": 1}'

# Aggiornare la reazione
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/response/update -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"response_id": "CEgYG4UBMUGN-LWULP7W", "comment": "comment_text",
"status": "Confirmed"}'

# Aggiornare l'elenco delle reazioni
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/responses/update -H "Content-Type: application/json" -H
"Authorization: Bearer {access_token}" -d '{"responses_ids": ["CEgYG4UBMUGN-LWULP7W", "2ESl6IgB4cAOUyXBb5IB"],
"comment": "comment_text", "status": "Confirmed"}'
```

Esempio di risposta dell'API REST con il token di accesso e il nuovo token di aggiornamento:

```
{
"access_token": "SamPLET346yoKEnSamPLEToK25EnSamPLEToK35EnS",
"refresh_token": "tOKenSaMPlet259OKenS123aMPle926tOKenSaMPle"
}
```

Esempio di risposta dell'API REST con la struttura e i valori dei commenti:

```
[{
  "comment_id": "bfu6TiNghqp",
  "author_name": "John Doe",
  "text": "<p>Primo commento</p>",
  "creation_time": 1601295428640
}, {
  "comment_id": "bfu6TiNghqt",
```

```
  "author_name": "Jane Doe",
  "text": "<p>Secondo commento</p>",
  "creation_time": 1601295433441
}]
```

Esempio di risposta dell'API REST quando l'API REST crea un nuovo commento e invia una risposta con i dettagli del commento:

```
{
  "comment_id": "AXTej0Qi4bfu6TiNgmvT",
  "author_name": "Nome token",
  "text": "Nuovo commento creato tramite l'API REST",
  "creation_time": 1601461748122
}
```

Revoca di un token di aggiornamento in Kaspersky Security Center

È possibile revocare i token di aggiornamento dalle connessioni API che hanno attualmente lo stato *Attivo* o *Inattivo*.

Per revocare un token di aggiornamento:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **API**.

   Verrà visualizzato l'elenco **Connessioni API**.

2. Fare clic sulla connessione API da cui si desidera revocare un token di aggiornamento.

   Verrà visualizzata una sezione contenente le informazioni sulla connessione.

3. Fare clic sul pulsante **Revoca**.

Il token di aggiornamento viene revocato.

Eliminazione di una connessione API in Kaspersky Security Center

È possibile eliminare le connessioni API esistenti.

Per eliminare una connessione API:

1. Nella sezione **MDR** di Kaspersky Security Center fare clic sulla scheda **API**.

   Verrà visualizzato l'elenco **Connessioni API**.

2. Spostare il puntatore del mouse sulla connessione API che si desidera eliminare, quindi fare clic sull'icona del cestino (🗑) a destra della riga.

La connessione API selezionata viene eliminata.

Eliminazione di una connessione API in Web Console MDR

È possibile modificare le connessioni API esistenti.

Per modificare una connessione API:

1. In Web Console MDR fare clic sulla scheda **API**.

   Verrà visualizzato l'elenco **Tutti i token**.

2. Spostare il puntatore del mouse sulla connessione API che si desidera eliminare, quindi fare clic sull'icona del cestino (🗑) a destra della riga.

La connessione API selezionata viene eliminata.

Problemi noti

Kaspersky Managed Detection and Response presenta una serie di limitazioni che non sono critiche per il funzionamento dell'applicazione:

- Se si clona una risorsa virtuale o fisica con un Kaspersky Endpoint Security for Linux già connesso alla soluzione MDR, i dati di telemetria delle risorse clonate non vengono trasmessi correttamente. Per queste risorse clonate, rimuovere Kaspersky Endpoint Security for Linux, eliminare il file install_id nella cartella /var/opt/kaspersky/epagent/, quindi reinstallare Kaspersky Endpoint Security for Linux.

- Per le risorse con Kaspersky Endpoint Security for Windows nella configurazione Endpoint Detection and Response Agent (EDR Agent), gli stati *Avviso* e *Critico* per i componenti di controllo e protezione non vengono visualizzati.

- Non è possibile utilizzare le funzionalità di Kaspersky Endpoint Detection and Response Optimum per le risorse con Kaspersky Endpoint Security for Windows nella configurazione di EDR Agent.

- Le **applicazioni Kaspersky che funzionano con la sezione MDR** della scheda delle risorse in Web Console MDR possono contenere applicazioni EPP (Endpoint Protection Platform) obsolete, che non vengono più utilizzate per lavorare con Kaspersky Managed Detection and Response. Si verifica quando un'applicazione EPP obsoleta è stata sostituita con una nuova nella risorsa. Per queste applicazioni obsolete, il campo **Ultima visualizzazione** contiene la data precedente, mentre per la nuova applicazione EPP il campo **Ultima visualizzazione** contiene la data più recente.

- La soluzione MDR che utilizza la configurazione KPSN non supporta una gerarchia di Kaspersky Security Center Administration Server se solo il Server primario nella gerarchia dispone dell'accesso a Internet.

Contattare il Servizio di assistenza tecnica

In questa sezione viene descritto come ottenere assistenza tecnica e vengono illustrate le condizioni per usufruirne.

Come ottenere assistenza tecnica

Se non si riesce a trovare una soluzione al problema nella documentazione di Kaspersky Managed Detection and Response o in una delle fonti di informazioni su Kaspersky Managed Detection and Response, contattare il Servizio clienti di Kaspersky. Gli specialisti del Servizio di assistenza tecnica risponderanno a tutte le domande sull'installazione e sull'utilizzo di Kaspersky Managed Detection and Response.

Kaspersky garantisce l'assistenza per Kaspersky Managed Detection and Response durante il relativo ciclo di vita (consultare la pagina relativa al ciclo di vita dell'assistenza dell'applicazione). 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 specialisti di Kaspersky tramite richieste online. È possibile utilizzare Kaspersky CompanyAccount per tenere traccia dello stato delle richieste online e memorizzarne 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.

Fonti di informazioni sulla soluzione

Nella pagina Kaspersky Managed Detection and Response è possibile visualizzare informazioni generali sulla soluzione, le relative funzioni e caratteristiche.

Glossario

Applicazione EPP

Un'applicazione inclusa in un sistema di protezione per dispositivi endpoint (Endpoint Protection Platform o EPP). Le applicazioni EPP vengono installate nei dispositivi endpoint all'interno dell'infrastruttura IT di un'organizzazione (ad esempio dispositivi mobili, computer o laptop). Un esempio di applicazione EPP è Kaspersky Endpoint Security for Windows nell'ambito della soluzione EPP Kaspersky Endpoint Security for Business.

Endpoint Protection Platform (EPP)

Un sistema integrato di protezione complessa per dispositivi endpoint (ad esempio dispositivi mobili, computer o laptop) che include varie tecnologie di sicurezza. Un esempio di Endpoint Protection Platform è Kaspersky Endpoint Security for Business.

Incidente

Un'attività valutata come critica dalla tecnologia di rilevamento e che richiede una reazione immediata da parte di Kaspersky Managed Detection and Response.

IOC

Un indicatore di compromissione (o IOC) mostra le prove su un dispositivo che indicano una violazione della sicurezza.

Reazione

La reazione agli incidenti è una metodologia strutturata per la gestione di incidenti di sicurezza, violazioni e minacce informatiche.

Risorsa

Un dispositivo con un'applicazione EPP Kaspersky installata (ad esempio Kaspersky Endpoint Security for Windows).

Tattica MITRE

L'obiettivo che l'autore di un attacco desiderava raggiungere durante un attacco informatico contro l'infrastruttura del cliente.

Tecnica MITRE

Il metodo utilizzato dall'autore di un attacco per eseguire azioni dannose durante un attacco informatico all'infrastruttura del cliente. Ogni tattica MITRE contiene una serie di tecniche MITRE.

Telemetria

Dati inviati dalle risorse a Kaspersky Managed Detection and Response.

Tenant

Un tenant è un'organizzazione a cui si fornisce Kaspersky Managed Detection and Response.

Informazioni sul codice di terze parti

Nello sviluppo della soluzione è stato utilizzato codice di terze parti.

Per informazioni sul codice di terze parti in Kaspersky Managed Detection and Response Console, contattare l'assistenza di Kaspersky Managed Detection and Response.

Le informazioni sul codice di terze parti utilizzato nel plug-in MDR sono disponibili nel file legal_notices.txt.

Note relative ai marchi registrati

I marchi registrati e i marchi di servizi sono di proprietà dei rispettivi titolari.

Apple, Mac, macOS e Safari sono marchi di Apple Inc.

Amazon AWS, Amazon Web Services sono marchi di Amazon.com, Inc. o delle relative consociate.

Active Directory, Internet Explorer, Microsoft, Microsoft Edge, Outlook, PowerShell, Windows PowerShell, Windows and Windows Server sono marchi del gruppo di aziende Microsoft.

Firefox e Mozilla sono marchi di Mozilla Foundation negli Stati Uniti e in altri paesi.

Google e Google Chrome sono marchi di Google LLC.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e in altri paesi.

Python è un marchio o un marchio registrato di Python Software Foundation.

Configurazione dei criteri di controllo per l'utilizzo con Kaspersky Managed Detection and Response

Si consiglia di configurare le seguenti impostazioni di controllo per garantire un funzionamento stabile e ottimizzare l'efficienza di Kaspersky Managed Detection and Response:

- **Configurazione dei criteri di controllo degli eventi di Windows**

Per massimizzare l'efficienza di Kaspersky Managed Detection and Response, è necessario configurare i criteri di controllo degli eventi di Windows nelle risorse.

Per configurare i criteri di controllo degli eventi di Windows:

1. Nelle risorse che eseguono Windows premere **WINDOWS+R** per aprire la finestra **Esegui**.
2. Nel campo **Apri** digitare `gpedit.msc`, quindi premere **INVIO** o fare clic su **OK**. Verrà visualizzata la finestra **Editor Criteri di gruppo locali**.
3. Nella struttura della console fare clic su **Configurazione computer → Impostazioni di Windows → Impostazioni di sicurezza → Configurazione avanzata dei criteri di controllo → Criteri di controllo di sistema - Oggetto Criteri di gruppo locale**.
4. Fare clic sul nodo **Accesso all'account.** Impostare i seguenti valori sul lato destro della finestra:

Sottocategoria	Eventi di controllo
Controlla convalida delle credenziali	Esito positivo e negativo
Controlla servizio di autenticazione Kerberos	Esito positivo e negativo
Controlla operazioni dei ticket di servizio Kerberos	Esito positivo e negativo

5. Fare clic sul nodo **Gestione account.** Impostare i seguenti valori sul lato destro della finestra:

Sottocategoria	Eventi di controllo
Controlla gestione account computer	Esito positivo e negativo
Controlla Gestione gruppi di sicurezza	Esito positivo
Controlla Gestione account utente	Esito positivo e negativo

6. Fare clic sul nodo **Accesso DS**. Impostare i seguenti valori sul lato destro della finestra:

Sottocategoria	Eventi di controllo
Controlla accesso al servizio di directory	Esito positivo e negativo
Controlla le modifiche al servizio di directory	Esito positivo e negativo

7. Fare clic sul nodo **Accesso/fine sessione**. Impostare i seguenti valori sul lato destro della finestra:

Sottocategoria	Eventi di controllo
Controlla Blocco account	Errore
Controlla Accesso	Esito positivo e negativo
Controlla accesso speciale	Esito positivo e negativo

8. Fare clic sul nodo **Accesso agli oggetti**. Impostare i seguenti valori sul lato destro della finestra:

Sottocategoria	Eventi di controllo
Servizi di certificazione del controllo	Esito positivo e negativo
Controlla Condivisione file	Esito positivo
Controlla Connessione a Piattaforma filtro Windows	Esito positivo
Controlla Altri eventi di accesso agli oggetti	Esito positivo

9. Fare clic sul nodo **Modifica criterio**. Impostare i seguenti valori sul lato destro della finestra:

Sottocategoria	Eventi di controllo
Controlla modifica ai criteri	Esito positivo
Controlla Modifica criteri a livello di regola MPSSVC	Esito positivo

10. Fare clic sul nodo **Utilizzo privilegi**. Impostare il seguente valore sul lato destro della finestra:

Sottocategoria	Eventi di controllo
Controlla Utilizzo privilegi sensibili	Esito positivo

11. Fare clic sul nodo **Sistema**. Impostare i seguenti valori sul lato destro della finestra:

Sottocategoria	Eventi di controllo
Controlla Modifica stato sicurezza	Esito positivo
Controlla Estensione sistema di sicurezza	Esito positivo

12. Nella struttura della console fare clic su **Configurazione computer** → **Modelli amministrativi** → **Componenti di Windows** → **Windows PowerShell**. Impostare il seguente valore sul lato destro della finestra:

Sottocategoria	Eventi di controllo
Abilitare la registrazione dei blocchi di script di PowerShell	Abilitata

13. Chiudere la finestra **Editor Criteri di gruppo locali**.

    Tutte le modifiche vengono salvate automaticamente.

I criteri di controllo degli eventi di Windows sono ora configurati per l'utilizzo con Kaspersky Managed Detection and Response.

- Configurazione del controllo per gli oggetti di Active Directory

Per ottimizzare l'efficienza di Kaspersky Managed Detection and Response, è necessario configurare il controllo nei controller di dominio di Windows.

Per configurare il controllo per gli oggetti di Active Directory:

1. Nel controller di dominio Windows premere **Win+R** per aprire la finestra **Esegui**.
2. Nel campo **Apri** digitare `dsa.msc`, quindi premere **INVIO** o fare clic su **OK**. Viene visualizzata la finestra **Utenti e computer di Active Directory**.
3. Nella struttura della console fare clic con il pulsante destro del mouse su <nome di dominio> e selezionare **Trova**. Viene visualizzata la finestra **Trovare utenti, contatti e gruppi**.
4. Immettere **Amministratore** nel campo **Nome**, quindi fare clic su **Trova ora**.
5. Nell'area **Risultati della ricerca** fare clic con il pulsante destro del mouse sull'oggetto **Amministratore** e selezionare **Proprietà** → **Sicurezza** → **Avanzate** - scheda **Controllo**.
6. Fare clic su **Aggiungi** per aprire la finestra **Voci di controllo per l'amministratore**. Fare clic su **Seleziona un principale+++**, immettere `Tutti`, fare clic su **Controlla nomi**, quindi fare clic su **OK**.
7. Nella finestra **Voci di controllo per l'amministratore** selezionare le caselle di controllo **Elenca contenuto**, **Autorizzazioni di lettura**, **Autorizzazioni di modifica**, **Proprietario della modifica, Leggi tutte le proprietà** e **Scrivi tutte le proprietà**.
8. Fare clic sui pulsanti **OK** → **Applica** → **OK**.

   Il controllo per l'oggetto di Active Directory **Amministratore** è ora configurato per l'utilizzo con Kaspersky Managed Detection and Response.
9. Eseguire gli stessi passaggi per i seguenti oggetti di Active Directory predefiniti e per gli utenti e i gruppi di dominio sensibili, esistenti e abilitati nel sistema:

- **Amministratori**
- **Gruppo di replica delle password RODC consentito**
- **Editori di certificati**
- **Controller di dominio clonabili**
- **Gruppo di replica delle password RODC vietato**
- **DnsAdmins**
- **DnsUpdateProxy**
- **Amministratori di dominio**
- **Computer di dominio**
- **Controller di dominio**
- **Amministratori aziendali**
- **Amministratori principali dell'azienda**

- Controller di dominio di sola lettura aziendali
- Proprietari del creatore di criteri di gruppo
- Amministratori chiave
- krbtgt
- Utenti protetti
- Server RAS e IAS
- Controller di dominio di sola lettura
- Amministratori dello schema

- Configurazione del controllo per Servizi certificati Active Directory, modelli di certificato e oggetti certificato

Per ottimizzare l'efficienza di Kaspersky Managed Detection and Response, è necessario configurare il controllo per il servizio **Servizi certificati Active Directory**, i modelli di certificato e gli oggetti negli host con **Servizi certificati Active Directory** (AD CS) abilitati.

*Per configurare il controllo per il servizio **Servizi certificati Active Directory**:*

1. Premere **WIN+R** per aprire la finestra **Esegui**.
2. Nel campo **Apri** digitare `cmd`, quindi premere **INVIO** o fare clic su **OK**. Viene visualizzata la finestra **Prompt dei comandi**.
3. Per configurare le impostazioni di controllo per l'Autorità di certificazione, immettere i comandi seguenti, quindi premere INVIO:

   ```
   certutil -setreg CA\AuditFilter 127
   certutil -setreg policy\EditFlags +EDITF_AUDITCERTTEMPLATELOAD
   ```

4. Per riavviare il servizio **Servizi certificati**, immettere il comando seguente, quindi premere INVIO:

   ```
   net stop certsvc && net start certsvc
   ```

Per configurare il controllo di sicurezza per i modelli di certificato:

1. Premere **WIN+R** per aprire la finestra **Esegui**.
2. Nel campo **Apri** digitare `adsiedit.msc`, quindi premere **INVIO** o fare clic su **OK**.
3. Fare clic con il pulsante destro del mouse su **ADSI Edit**, quindi selezionare **Connetti a**.
4. Nella sezione **Punto di connessione** selezionare il valore **Configurazione** nel campo Selezionare un **contesto dei nomi conosciuto**.
5. Fare doppio clic su **Configurazione/Schema** nel riquadro di sinistra.
6. Selezionare la cartella **CN=Configurazione,DC=...** → **CN=Servizi** → **CN=Servizi chiave pubblica** → **CN=Modelli certificato**.
7. Fare clic con il pulsante destro del mouse sulla cartella **CN=Modelli certificato**, selezionare **Proprietà,** quindi aprire la scheda **Sicurezza**.
8. Fare clic sul pulsante **Avanzate**, quindi selezionare la scheda **Controllo**.
9. Fare clic sul principale **Tutti**, selezionare le caselle di controllo **Scrivi tutte le proprietà**, **Elimina**, **Autorizzazioni di modifica**, **Proprietario della modifica**, **Tutte le scritture convalidate** e fare clic su **OK**.

Per configurare il controllo di sicurezza per l'oggetto NTAuthCertificates:

1. Nel campo **Apri** digitare `adsiedit.msc`, quindi premere **INVIO** o fare clic su **OK**.
2. Fare clic con il pulsante destro del mouse su **ADSI Edit**, quindi selezionare **Connetti a**.
3. Nella sezione **Punto di connessione** selezionare il valore **Configurazione** nel campo Selezionare un **contesto dei nomi conosciuto**.
4. Fare doppio clic su **Configurazione/Schema** nel riquadro di sinistra.

5. Selezionare la cartella **CN=Configurazione,DC=...** → **CN=Servizi** → **CN=Servizi chiave pubblica** → **CN=NTAuthCertificates**.

6. Fare clic con il pulsante destro del mouse sulla cartella **CN=NTAuthCertificates**, selezionare **Proprietà,** quindi aprire la scheda **Sicurezza**.

7. Fare clic sul pulsante **Avanzate**, quindi selezionare la scheda **Controllo**.

8. Fare clic sul principale **Tutti**, selezionare le caselle di controllo **Scrivi tutte le proprietà**, **Elimina**, **Autorizzazioni di modifica**, **Proprietario della modifica**, **Tutte le scritture convalidate** e fare clic su **OK**.

Video di onboarding

Guardare il video per saperne di più sulle funzionalità principali della soluzione MDR.

Soluzione MDR. Video di onboarding