

The Kaspersky logo is displayed in a bold, lowercase, sans-serif font. It is positioned within a white, rounded rectangular area that is set against a background of green and teal abstract shapes.

kaspersky

Kaspersky Managed Detection and Response

© 2026 AO Kaspersky Lab

Inhalt

[Hilfe zu Kaspersky Managed Detection and Response](#)

[Neuerungen](#)

[Kaspersky Managed Detection and Response](#)

[Funktionsweise von Kaspersky Managed Detection and Response](#)

[Verantwortungsbereiche](#)

[Hardware- und Softwareanforderungen](#)

[Komponenten von Kaspersky Managed Detection and Response](#)

[Kaspersky Managed Detection and Response aktivieren und bereitstellen](#)

[Erforderliche Komponenten für den Betrieb von MDR](#)

[Integration mit Anwendungen und Lösungen von Kaspersky](#)

[Das MDR-Plug-ins konfigurieren](#)

[Aktivierung und Bereitstellung von MDR, wenn aktuelle Anwendungsversionen und ein einzelner Mandant verwendet werden](#)

[Aktivierung und Bereitstellung von MDR, wenn aktuelle Anwendungsversionen und Mehrmandantenfähigkeit verwendet werden](#)

[Aktivierung und Bereitstellung von MDR, wenn ältere Anwendungsversionen verwendet werden](#)

[KPSN-Konfigurationsdatei bereitstellen](#)

[MDR-Konfigurationsdatei \(BLOB\) bereitstellen](#)

[Bereitstellung durch Erfassen und Kopieren des Geräte-Images](#)

[MDR-Lösung in Kaspersky-Anwendungen aktivieren](#)

[MDR-Lösung in Kaspersky-Anwendungen aktivieren. Lizenzen von Kaspersky MDR Add-ons](#)

[MDR-Lösung in Kaspersky-Anwendungen aktivieren. Lizenzen von Kaspersky MDR](#)

[MDR-Lösung in Kaspersky-Anwendungen aktivieren. Lizenzen für Kaspersky Symphony MDR, Kaspersky Next Complete Security, Kaspersky Optimum Security und Kaspersky Next MXDR Optimum](#)

[MDR-Lösung in Kaspersky-Anwendungen aktivieren. Add-on-Lizenz für Kaspersky Managed Detection and Response for Industrial CyberSecurity](#)

[Lizenzierung](#)

[Vergleich der kommerziellen Lizenzstufen](#)

[Über den Aktivierungscode](#)

[Einen neuen Aktivierungscode angeben](#)

[Lizenzen in Kaspersky Security Center verwalten](#)

[Fehlerbehebung bei Lizenzproblemen](#)

[Über die MDR-Erklärung](#)

[Über die Bereitstellung von Daten](#)

[Regionen der Datenverarbeitung](#)

[Über die Erklärung zur Datenverarbeitung](#)

[Benutzeroberflächen von Kaspersky Managed Detection and Response](#)

[MDR-Abschnitt in Kaspersky Security Center](#)

[MDR-Plug-in in Kaspersky Security Center einrichten](#)

[Zugriffsrechte in Kaspersky Security Center konfigurieren](#)

[MDR-Einstellungen in Kaspersky Security Center anzeigen und bearbeiten](#)

[Funktionen des MDR-Plug-ins auf einem virtuellen Administrationsserver verwenden](#)

[Verwendung der MDR-Funktionen in Kaspersky Security Center über einen Proxyserver](#)

[Änderung der Zertifikate zur Verwendung der MDR-Funktionen in Kaspersky Security Center mit einem Proxyserver oder einer Antiviren-Software](#)

[MDR-Funktionen in Kaspersky Security Center ein- und ausblenden](#)

[MDR Web Console](#)

[Sprache der Benutzeroberfläche in Kaspersky Security Center ändern](#)

[Sprache der Benachrichtigungen und Berichte in Kaspersky Security Center ändern](#)

[Sprache der Benutzeroberfläche in der MDR Web Console ändern](#)

[Über die MDR-Konfigurationsdatei](#)

[Über Kaspersky Security Network](#)

[KPSN-Konfigurationsdateien regelmäßig aktualisieren](#)

[MDR-Lösung auf den Betrieb ohne KPSN-Konfigurationsdateien umstellen](#)

[Dashboards für die Überwachung in der MDR Web Console](#)

[Zusammenfassende Informationen erhalten](#)

[Zusammenfassung aller Assets als CSV-Datei abrufen \(MDR Web Console\)](#)

[Informationen zu Vorfällen als PDF abrufen \(MDR Web Console\)](#)

[Regelmäßige Zustellung von Berichten in der MDR Web Console einrichten](#)

[Benachrichtigungen erhalten](#)

[Benachrichtigungen in der MDR Web Console einrichten](#)

[Benachrichtigungen zum Asset-Status](#)

[Erweiterte Benachrichtigungen erhalten](#)

[Erweiterte Benachrichtigungen in der MDR Web Console aktivieren](#)

[Benutzer verwalten](#)

[Neue Benutzer über die MDR Web Console einladen](#)

[Benutzerrollen in der MDR Web Console ändern](#)

[Methoden zur Benachrichtigung der Benutzer in der MDR Web Console bearbeiten](#)

[Benutzerzugriff auf Mandanten in der MDR Web Console bearbeiten](#)

[Benutzerkonten löschen](#)

[Assets verwalten](#)

[Assets in der MDR Web Console anzeigen und durchsuchen](#)

[Assets in der MDR Web Console filtern](#)

[Detaillierte Informationen zu Assets in der MDR Web Console anzeigen](#)

[Status der Assets](#)

[Status der Assets in Kaspersky Security Center überprüfen](#)

[So vermeiden Sie den Verlust von Telemetriedaten der Assets](#)

[Vorfälle verwalten](#)

[Über Vorfälle](#)

[Vorfälle in der MDR Web Console anzeigen und durchsuchen](#)

[Vorfälle in der MDR Web Console filtern](#)

[Benutzerdefinierte Vorfälle in der MDR Web Console erstellen](#)

[Detaillierte Informationen über Vorfälle in der MDR Web Console anzeigen](#)

[Reaktionen auf Vorfälle in der MDR Web Console verarbeiten](#)

[Arten von Reaktionen](#)

[Auto-Akzeptieren von Reaktionen in der MDR Web Console](#)

[Auto-Akzeptieren von Reaktionen in Kaspersky Security Center](#)

[Vorfälle in der MDR Web Console schließen](#)

[Vorfall zur weiteren Untersuchung an das Sicherheitsvorfall-Reaktionsteam senden](#)

[Integration von Kaspersky Unified Monitoring and Analysis](#)

[Vorfälle für Managed Detection and Response aus XDR-Vorfällen erstellen](#)

[Integration von Kaspersky Digital Footprint Intelligence für MDR](#)

[Funktionen von Kaspersky Endpoint Detection and Response Expert verwenden](#)

[Reaktionen](#)

[Verwalten von Mandanten](#)

[Mandanten in Kaspersky Security Center verwalten](#)

[Mandanten in Kaspersky Security Center anzeigen](#)

[Mandanteneinstellungen in Kaspersky Security Center anzeigen](#)

[Mandanteneinstellungen in Kaspersky Security Center bearbeiten](#)

[Neue Mandanten in Kaspersky Security Center hinzufügen](#)

[Mandanten in Kaspersky Security Center löschen](#)

[Assets zwischen Mandanten verschieben](#)

[Mandanten in der MDR Web Console verwalten](#)

[Mandanten in der MDR Web Console anzeigen](#)

[Mandanteneinstellungen in der MDR Web Console anzeigen](#)

[Mandanteneinstellungen in der MDR Web Console bearbeiten](#)

[Neue Mandanten in der MDR Web Console hinzufügen](#)

[Mandanten in der MDR Web Console löschen](#)

[Die Lösung mittels REST-API verwalten](#)

[Szenario: Tokenbasierte Autorisierung durchführen](#)

[Eine API-Verbindung in Kaspersky Security Center erstellen](#)

[Eine API-Verbindung in der MDR Web Console erstellen](#)

[Eine API-Verbindung in Kaspersky Security Center bearbeiten](#)

[Eine API-Verbindung in der MDR Web Console bearbeiten](#)

[Einen Zugriffstoken in Kaspersky Security Center erstellen](#)

[Einen Zugriffstoken in der MDR Web Console erstellen](#)

[Die REST-API verwenden](#)

[Einen Aktualisierungstoken in Kaspersky Security Center widerrufen](#)

[Eine API-Verbindung in Kaspersky Security Center löschen](#)

[Eine API-Verbindung in der MDR Web Console löschen](#)

[Kaspersky Managed Detection and Response deaktivieren](#)

[Die Nutzung von Kaspersky Managed Detection and Response beenden](#)

[Die Nutzung von Kaspersky Managed Detection and Response vorübergehend aussetzen](#)

[Widerruf Ihrer Einwilligung in die Nutzungsbedingungen der MDR-Lösung](#)

[Bekannte Probleme](#)

[Anfrage an den Technischen Support](#)

[Technischen Support erhalten](#)

[Technischer Support über Kaspersky CompanyAccount](#)

[Informationsquellen zu dieser Lösung](#)

[Glossar](#)

[Asset](#)

[Endpoint Protection Platform \(EPP\)](#)

[EPP-Anwendung](#)

[IOC](#)

[Mandant](#)

[MITRE Tactic](#)

[MITRE Technique](#)

[Reaktion](#)

[Telemetriedaten](#)

[Vorfall](#)

[Informationen über den Code von Drittherstellern](#)

[Markenrechtliche Hinweise](#)

Hilfe zu Kaspersky Managed Detection and Response

Neue Funktionen

- [Neue Funktionen im aktuellsten Release der Lösung](#)

Hardware- und Softwareanforderungen

- [Prüfen Sie, welche Betriebssysteme und EPP Anwendungen unterstützt werden](#)

Gegenüberstellung von Funktionen

- [Vergleich der Lösungen nach kommerziellen Lizenzen: MDR Optimum, MDR Expert, MDR Basic, MDR Advanced und MDR Prime](#)

Erste Schritte

- On-premises-Bereitstellung
- Cloud-basierte Bereitstellung
- [Kaspersky Managed Detection and Response aktivieren](#)

Überwachung und Berichterstellung

- [Benachrichtigungen erhalten](#)
- [Erweiterte Benachrichtigungen erhalten](#)
- [Zusammenfassende Informationen erhalten](#)
- [Dashboards für die Überwachung](#)



Bereitstellung von Daten und Schutz personenbezogener Daten

- [Über die Bereitstellung von Daten](#)
- [Kaspersky Security Network](#)

Neuerungen

Kaspersky Managed Detection and Response bietet mehrere neue Funktionen und Verbesserungen.

August 2026

Das MDR-Plug-in Version 3.1.1 für die Open Single Management Plattform Version 2.2 wurde veröffentlicht.

Juli 2026

- Benachrichtigungen zum Asset-Status

MDR unterstützt jetzt die [automatische Zustellung von Benachrichtigungen, wenn der Zustand Ihrer geschützten Assets Aufmerksamkeit erfordert](#). Konfigurieren Sie Schwellenwerte für die Asset-Status OK, Warning, Critical und Offline und erhalten Sie E-Mail- oder Telegram-Benachrichtigungen, wenn die konfigurierten Bedingungen erfüllt sind. So können Sie Probleme mit der Telemetrieerfassung oder Konnektivität schnell erkennen, ohne die Seite Assets kontinuierlich überwachen zu müssen.

Juni 2026

- Kaspersky DFI-Integration für MDR

Unser MDR-Dienst nutzt jetzt Informationen über kompromittierte Anmeldeinformationen aus dem Kaspersky DFI-Dienst, um Erkennung, Untersuchungen und Threat Hunting-Workflows zu optimieren. Durch die Korrelation abgeflossener Anmeldeinformationen mit Sicherheitsereignissen und die Berücksichtigung dieser Informationen bei proaktiven Threat-Hunting-Aktivitäten kann MDR potenzielle Kontokompromittierungen früher erkennen, die Priorisierung von Vorfällen verbessern und das Risiko eines unbefugten Zugriffs verringern.

Wichtige Funktionen:

- Anreicherung von Alarmen mit Kontext über abgeflossene Anmeldeinformationen
 - Korrelation abgeflossener Anmeldeinformationen mit Sicherheitsereignissen
 - Auf Anmeldeinformationen basierendes Threat Hunting und Erkennung von Kompromittierungen
 - Aktualisierte Support-Matrix für MDR-Anwendungen
- Die Tabelle „Kompatible Kaspersky-Anwendungen und -Lösungen“ wurde aktualisiert. Einige alte Produktversionen wurden in die Kategorie „Eingeschränkte MDR-Kompatibilität“ verschoben (bestimmte MDR-Funktionen sind möglicherweise nicht verfügbar), während die Unterstützung für Kaspersky Endpoint Agent eingestellt wurde.

Weitere Informationen finden Sie im [aktuellen Artikel in der Online-Hilfe](#).

Mai 2026

- Das MDR-Plug-in Version 3.0.2 für die Open Single Management Platform Version 2.1 wurde veröffentlicht.
- Beim Schließen von Vorfällen in der MDR Console können Benutzer jetzt direkt ein Feedback hinterlassen. Dies trägt dazu bei, die Servicequalität zu verbessern und die Kundenzufriedenheit effizienter zu erfassen.
- MDR-Administratoren können jetzt [in der MDR Console für jeden Mandanten das erwartete Asset-Limit definieren](#).

Wenn die Anzahl der verbundenen Assets das Limit überschreitet, wird sowohl in der Mandantenliste als auch auf der Seite mit den Eigenschaften der Mandanten eine Benachrichtigung angezeigt. Dies hilft Administratoren, den Umfang von Onboarding-Vorgängen zu überwachen und zu erwartende Lizenzanforderungen einzuschätzen.

Diese Funktion wird dem MDR-Plug-in in einer kommenden Version hinzugefügt.

- Das Format der per E-Mail und Telegram zugestellten Benachrichtigungen wurde verbessert, um die Lesbarkeit zu erhöhen und den Zugriff auf wichtige Informationen zu beschleunigen.

Das Update betrifft Benachrichtigungen bezüglich:

- Vorfälle
- Kommentare in der Kommunikation mit MDR-Analysten
- Reaktionsmaßnahmen
- Statusaktualisierung für Lizenzschlüssel

März 2026

Die Unterstützung für Kaspersky Embedded Systems Security für Linux Version 4.0 oder höher wurde hinzugefügt. Mit einer Lizenz für Kaspersky MDR können Sie jetzt in Kaspersky Embedded Security for Linux die [MDR-Lösung aktivieren](#).

Dezember 2025

- Die Unterstützung folgender EPP-Anwendungen wurde hinzugefügt:
 - Kaspersky Embedded Systems Security für Windows Version 4.0 oder höher
 - Kaspersky Industrial CyberSecurity for Nodes Windows Version 4.5
- Zusätzlich zur MDR Web Console können Sie jetzt [erweiterte Benachrichtigungen per Telegram](#) im MDR Plug-in einrichten.
- Über die Oberfläche der MDR Web Console können Sie [Vorfälle zur weiteren Untersuchung an das Incident Response-Team senden](#).

- Die Unterstützung folgender Kaspersky-Lösungen wurde hinzugefügt:
 - Integration mit Kaspersky Endpoint Detection and Response Version 8.0 oder höher, die folgende Funktionalität ermöglicht:
 - [Die Möglichkeit, MDR-Vorfälle aus XDR-Vorfällen zu erstellen.](#)
 - Die Möglichkeit, Get artefacts als [Art für die Reaktion](#) auszuwählen.
 - Integration mit Kaspersky Anti Targeted Attack Version 8.0 oder höher, durch die Get artefacts als [Art für die Reaktion](#) hinzugefügt wird.

Lesen Sie den folgenden Artikel: [Integration mit Anwendungen und Lösungen von Kaspersky](#)

Oktober 2025

Sie können jetzt in der MDR Web Console [erweiterte Telegram-Benachrichtigungen](#) einrichten.

Juli 2025

- Es wurde die Möglichkeit hinzugefügt, die MDR-Lösung in den folgenden Anwendungen anhand eines Aktivierungscodes zu aktivieren:
 - Kaspersky Endpoint Security für Linux, Version 12.3
 - Kaspersky Endpoint Security für Linux, Version 12.3 im Light Agent-Modus
 - Kaspersky Endpoint Security für Windows Version 12.6 oder höher
 - Kaspersky Endpoint Security für Windows, Version 12.8 oder höher im Light Agent-Modus
 - Kaspersky Endpoint Security for Mac, Version 12.2

Weitere Informationen dazu finden Sie im folgenden Artikel: [MDR-Lösung in Kaspersky-Anwendungen aktivieren.](#)
- Die MDR-Lösung kann jetzt ohne KPSN-Konfigurationsdatei mit den folgenden Anwendungen betrieben werden:
 - Kaspersky Endpoint Security für Linux, Version 12.3
 - Kaspersky Endpoint Security für Linux, Version 12.3 im Light Agent-Modus
 - Kaspersky Endpoint Security für Windows Version 12.6 oder höher
 - Kaspersky Endpoint Security für Windows, Version 12.8 oder höher im Light Agent-Modus

- Kaspersky Endpoint Security for Mac, Version 12.2
- Weitere Informationen dazu finden Sie in folgendem Artikel: [MDR-Lösung auf den Betrieb ohne KPSN-Konfigurationsdateien umstellen](#).
- Die MDR-Lösung unterstützt jetzt [Kaspersky Endpoint Security für Windows, Version 12.8 oder höher im Light Agent-Modus](#) ².
- Die Version 2.5.1. des MDR-Plug-ins unterstützt jetzt die MDR-Ausführung ohne KPSN-Konfigurationsdatei.
- Kaspersky Endpoint Security für Linux, Version 12.3 unterstützt jetzt die folgenden Reaktionsmaßnahmen:
 - Isolieren
 - Isolation deaktivieren
 - Datei in Quarantäne verschieben
 - Datei aus Quarantäne wiederherstellen
 - Prozess beenden
 - Prozess starten

Mai 2025

- Im Abschnitt [Lizenzierung](#) des MDR-Plug-ins für Kaspersky Security Center:
 - Für jede MDR-Lizenz wird jetzt der Name des Clients angezeigt, an den die Lizenz ausgestellt wurde.
 - Für bestimmte Lizenzen auf Mandanten ist jetzt eine Nutzungsmatrix verfügbar.
- Im Abschnitt [Mandanten](#) des MDR-Plug-ins für Kaspersky Security Center:
 - Beim Erstellen einer MDR-Konfigurationsdatei für einen bestimmten Mandanten wird jetzt der Name des Mandanten angezeigt, für den die Lizenz ausgestellt wird.
 - Die Liste der Mandanten zeigt jetzt den Root-Mandanten an, der nach dem Aktivieren des Clients standardmäßig erstellt wird. Sie können die Konfigurationsdateien für alle aktuellen Lizenzen des Root-Mandanten herunterladen.

Februar 2025

- Der MDR Web Console wurde der Abschnitt **Licensing** hinzugefügt. In ihm stehen die folgenden Funktionen zur Verfügung:
 - Anzeigen der folgenden MDR-Lizenzen: aktuell verwendet, nicht verwendet und abgelaufen
 - Anzeigen der Gesamtanzahl der Assets sowie deren Beschränkung für jede Lizenz

- Herunterladen der MDR-Konfigurationsdatei für den Root-Mandanten

Um MDR-Konfigurationsdatei für andere Mandanten herunterzuladen, verwenden Sie den [Abschnitt Mandanten](#).

- Eingeben eines neuen Aktivierungscodes.

Wenn Ihre Organisation über mehrere Lizenzen verfügt, können Sie diese nur im MDR-Plug-in für Kaspersky Security Center verwalten. Der Abschnitt **Licensing** in der MDR Web Console kann nur angezeigt und nicht geändert werden.

- Das MDR-Plug-in für Kaspersky Security Center unterstützt jetzt das [Anwenden mehrerer Lizenzen](#) in Ihrer Organisation. In ihm stehen die folgenden Funktionen zur Verfügung:

- Anzeigen der folgenden MDR-Lizenzen: aktuell verwendet, nicht verwendet und abgelaufen
- Beenden einer aktuellen MDR-Lizenz
- Eingeben eines neuen Aktivierungscodes für eine Lizenz
- Herunterladen der MDR-Konfigurationsdatei des Root-Mandanten für eine Lizenz
- Auswählen einer Lizenz für eine MDR-Konfigurationsdatei beim Erstellen oder Bearbeiten eines Mandanten im [Abschnitt Mandanten](#).

Dezember 2024

- Für Geräte mit Kaspersky Endpoint Security für Windows (ab Version 12.4) wurde die Aktivierung von Managed Detection and Response vereinfacht. Für die MDR-Lösung von Kaspersky benötigen Sie lediglich eine Standard-Lizenz.

Beachten Sie, dass für die folgenden Szenarios die Verwendung der MDR-Konfigurationsdatei (BLOB) weiterhin erforderlich ist:

- Sie besitzen mehr als einen Mandanten.
- Sie verwenden die MDR-Lösung zusammen mit Kaspersky Endpoint Detection and Response Optimum.
- Es wurde die Unterstützung zur Verwaltung der MDR-Lösung über die Kaspersky Security Center für Linux hinzugefügt (ab Version 15.1).
- Der Hilfe wurden [ausführliche Informationen über die Anforderungen an den Kommunikationskanal](#) hinzugefügt.

Oktober 2024

Veröffentlichung des MDR-Plug-ins für Kaspersky Security Center Version 2.4.1. Es enthält die folgenden Verbesserungen:

- Dem MDR-Plug-in für Kaspersky Security Center wurde die Möglichkeit hinzugefügt, das automatische Akzeptieren von Reaktionsmaßnahmen (Auto-Akzeptieren) für ausgewählte Mandanten zu konfigurieren.
- Verbesserte Funktionalität und Benutzeroberfläche des [Abschnitts mit der Liste der inaktiven Assets](#). Dies sind Assets, die zwar zu Kaspersky Security Center hinzugefügt wurden und die MDR-Komponente installiert haben, die aber nie Telemetriedaten an Kaspersky Managed Detection and Response gesendet haben. Sie können die Assets nach ihren MDR-Statuswerten filtern, detaillierte Informationen zu jedem Asset anzeigen und die Asset-Liste in eine csv-Datei exportieren.

Diese Funktion wird in Kaspersky Security Center 15.1 Windows oder höher, Kaspersky Security Center 15.1 Linux oder höher sowie in Kaspersky Next Expert View ordnungsgemäß ausgeführt.

- In der MDR Web Console kann jetzt eine [Aufgabe zum regelmäßigen Versenden von Berichten über offene Vorfälle](#) angelegt werden. Diese Funktion wurde vom MDR-Abschnitt in Kaspersky Security Center entfernt.

Juli 2024

In der MDR Web Console kann jetzt das automatische Akzeptieren von Reaktionsmaßnahmen (Auto-Akzeptieren) für die ausgewählten Mandanten konfiguriert werden.

Juni 2024

- Es stehen jetzt neue [Reaktionsmaßnahmen](#) zur Verfügung:
 - Datei in Quarantäne verschieben
 - Datei aus Quarantäne wiederherstellen
 - Auf einem Asset ein Skript starten
- Die [Dokumentation der REST-API](#) wurde aktualisiert und enthält neue Beispiel-Skripte.
- Die folgenden [Berichte](#) wurden neu gestaltet:
 - MITRE ATT&CK-Mapping zur tiefgründigen Bedrohungsanalyse.
 - Liste der Computer, die am häufigsten von Angreifern angegriffenen werden. Dies hilft den Kunden dabei, sich auf kritische Risiken zu konzentrieren.

- Unterstützung der Mandantenfähigkeit:
 - Sie können für bestimmte Mandanten Berichte erstellen und [Zeitpläne zum Versenden zusammenfassender Berichte festlegen](#).
 - Sie können in den Widgets im [Dashboard zur Überwachung](#) nahtlos Statistiken anzeigen, die bestimmten Mandanten entsprechen.
 - Sie können für bestimmte Mandanten die automatische Bestätigung zur Ausführung einer Reaktionsaufgabe konfigurieren.
 - Die MDR-API zur Verwaltung von Mandanten wurde erweitert.

Dezember 2023

- Die MDR Web Console enthält jetzt das Dashboard **Telemetry statistics**, das die Anzahl der Telemetrie-Ereignisse, Sicherheits-Ereignisse und Vorfälle anzeigt.
- Kaspersky Managed Detection and Response unterstützt jetzt Kaspersky Endpoint Security für Windows in der Konfiguration als Agent von Endpoint Detection and Response Agent (EDR Agent) (mit [diesen Einschränkungen](#)).

November 2023

- Die Anzeige der Asset-Statuswerte wurde in der MDR Web Console und im MDR-Plug-in für Kaspersky Security Center verbessert: Der [Asset-Status](#) zeigt jetzt für Assets die Funktionsfähigkeit der Komponenten der EPP-Anwendung, den Update-Status der Antiviren-Datenbanken und den Übertragungsstatus der Telemetriedaten an.
- Der Asset-Status zeigt jetzt an, wenn es auf Assets zu Verlusten von Telemetriedaten kommt. Dies erlaubt das Identifizieren von Assets, die Probleme bei der Übertragung von Telemetriedaten haben. Für Neukunden ist diese Funktion bereits aktiviert. Für Bestandskunden wird die Funktion nach und nach freigeschaltet.

Oktober 2023

Saudi-Arabien wurde als neue Kunden-Region hinzugefügt. Für die Kunden aus dieser Region werden die Telemetriedaten im Königreich Saudi-Arabien gespeichert.

September 2023

Veröffentlichung des MDR-Plug-ins für Kaspersky Security Center Version 2.3.1. In dieser Version wurden die Funktionen für das Vorfallsmanagement aus dem MDR-Abschnitt von Kaspersky Security Center entfernt. Sie können die Vorfälle auch in der [MDR Web Console](#) verwalten.

Juli 2023

Veröffentlichung des MDR-Plug-ins für Kaspersky Security Center Version 2.3.0. Es enthält diese folgenden Verbesserungen:

- Sie können jetzt im MDR-Plug-in erweiterte Benachrichtigungen einrichten.
- Sie können jetzt die MDR-Funktionen in Kaspersky Security Center mit dem MDR-Plug-in über einen Proxyserver verwenden.
- Sie können jetzt die Zertifikate ändern, um die MDR-Funktionen in Kaspersky Security Center mit einem Proxyserver oder einer Antiviren-Software zu verwenden.

Juli 2022

Veröffentlichung des MDR-Plug-ins Version 2.1.17. Diese Version des Plug-ins ist kompatibel mit Kaspersky Security Center ab Version 14.

Mai 2022

Allgemeine Verbesserungen:

- **USA/Kanada** wurde als neue Kunden-Region hinzugefügt. Für die Kunden aus dieser Region werden die Telemetriedaten in Nordeuropa gespeichert.
- Die Beschreibung des MDR-Bereitstellungsvorgangs wurde in der Hilfe geändert.

Verbesserungen im MDR-Plug-in:

- Im Abschnitt **Einstellungen** können Sie jetzt die Sprache ändern, die für Benachrichtigungen in Telegram und E-Mails sowie für Chat-Konversationen über Vorfälle verwendet wird.
- Verbesserte Benutzeroberfläche zur Arbeit mit Bildern und Tabellen auf den Vorfall-Karten.
- MDR Expert. Im Abschnitt **Nutzung des Dienstes** können Sie überprüfen, wie viele Vorfälle gemäß SLA erstellt werden können.

Fehlerbehebungen und andere Verbesserungen:

- Die Suche in Vorfall- und Asset-Listen erfolgt jetzt auf Basis einer vollständigen Übereinstimmung der gesuchten Teilzeichenfolge an einer beliebigen Stelle in der Zeichenfolge.
- Nachdem Sie in Kaspersky Endpoint Security for Mac Version 11.2 oder höher einen MDR-Aktivierungscode eingegeben und eine KPSN-Konfigurationsdatei hinzugefügt haben, müssen Sie Ihr Mac-Gerät nicht mehr neu starten, um mit der Übertragung von Telemetriedaten zu beginnen.
- Bei der Berechnung der Lizenzen für virtuelle Maschinen mit Kaspersky Security for Virtualization Light Agent Version 5.2 oder höher werden Assets, die seit über 24 Stunden keine Telemetrie übertragen haben, nicht berücksichtigt.

März 2022

Benutzer von [MDR Optimum](#) können jetzt mit den SOC-Analysten von Kaspersky zu einem Vorfall chatten (mit folgender Einschränkung: Anfragen werden nur in Bezug auf einen bestimmten Vorfall bearbeitet und es wird kein SLA angewendet).

Oktober 2021

- Das Plug-in für Kaspersky Managed Detection and Response für die Kaspersky Security Center Web Console und Kaspersky Next Expert View wurde mit erweiterter Funktionalität für die Funktion [Status der MDR-Assets](#) aktualisiert:
 - Verbesserte Benutzeroberfläche für die Funktion "Status der MDR-Assets".
 - Die Asset-Liste zeigt alle Assets mit sämtlichen Statuswerten an, die zuvor nur in der MDR Web Console verfügbar waren.
 - Es wurden Filter- und Sortieroptionen hinzugefügt, um mit der Asset-Liste zu arbeiten.

- Kaspersky Managed Detection and Response wird in Kaspersky Next Expert View unterstützt, was die Verwaltung der Lösung in der vereinheitlichten Verwaltungskonsole von Kaspersky Security Center ermöglicht. Kaspersky Managed Detection and Response stellt folgende Funktionen zur Verfügung:

- Arbeiten mit Vorfällen:

- Vorfälle ansehen, erstellen und kommentieren
- Kaspersky Security Operation Center wegen eines Vorfalls kontaktieren und die von den SOC-Analysten vorgeschlagenen Reaktionen akzeptieren oder ablehnen

- Mittels Kaspersky Endpoint Detection and Response auf einen Vorfall reagieren

Die folgenden Reaktionen sind verfügbar:

- Netzwerkisolation von Geräten anwenden.
- Regeln zur Blockierung nach Hash erstellen.
- Aufgaben je nach Art der Vorfälle erstellen, z B. löschen, in Quarantäne verschieben, Prozesse beenden oder Untersuchung anhand von Gefährdungsindikatoren (IOC) durchführen.
- Überwachen der Ereignisse von Kaspersky Managed Detection and Response auf den Dashboards der Überwachungskonsole von der Kaspersky Security Center Web Console
- Konfigurieren der Benachrichtigungen über Ereignisse von Kaspersky Managed Detection and Response per E-Mail und Telegram
- Konfigurieren des Zeitplans zum Senden der Zusammenfassung zur MDR-Performance per E-Mail
- Anzeigen von Geräten, auf denen Probleme mit der MDR-Performance auftreten
- Neuer Aktivierungsassistent, der eine Verbindung mit MDR in der Kaspersky Security Center Web Console ermöglicht
- Automatische Konfiguration von KPSN, die kein manuelles Herunter- und Hochladen einer Konfigurationsdatei in den Einstellungen von Kaspersky Security Center mehr erfordert
- Verwalten von Verbindungen zur öffentlichen MDR-API: Token anzeigen, erstellen, bearbeiten und löschen
- Verwalten von Mandanten der Organisation, einschließlich deren Erstellung
- Abrufen von Informationen über die Anzahl der Vorfälle zur Registrierung auf Benutzerseite, die gemäß den Bedingungen des Service Level Agreements (SLA) bearbeitet werden können

Diese Funktionen sind auch in der Kaspersky Security Center Web Console verfügbar.

- Die Verwaltung mehrerer MDR-Administratorkonten wurde in der MDR Web Console hinzugefügt: Benutzerkonten erstellen und Berechtigungen von Benutzerkonten verwalten

- Neue Versionen kompatibler Programme erfordern keine zusätzliche Installation von Kaspersky Endpoint Agent mehr. Die Integration der Funktionalität von Kaspersky Managed Detection and Response ist mit den folgenden EPP-Anwendungen kompatibel:
 - Kaspersky Endpoint Security für Windows 11.6 oder höher
 - Kaspersky Endpoint Security for Mac 11.2
 - Kaspersky Endpoint Security für Linux 11.2
 - Kaspersky Security for Virtualization 5.2 Light Agent

Ausführliche Informationen zu den verschiedenen Bereitstellungsszenarien finden Sie unter [Bereitstellung von Kaspersky Managed Detection and Response](#).

- Kaspersky Endpoint Security für Windows und für Linux wurde mit der Integration der Funktionalität von Kaspersky Managed Detection and Response die Filterung nach Ereignistyp hinzugefügt, welche es ermöglicht, die Belastung der Kanäle und den Datenverkehr beim Senden von Telemetriedaten zu verringern.
- Die folgenden Arten von Reaktionen werden unterstützt: [Datei vom Gerät abrufen](#), [Gerät isolieren](#), [Isolierung des Geräts deaktivieren](#), [Registrierungsschlüssel löschen](#), Prozess beenden
Das Ausführen dieser Vorgänge ist nach einer Bestätigung durch den Benutzer mit der Rolle "MDR-Administrator" möglich.
- Das Web-Plug-in für Kaspersky Security Center Web Console und Kaspersky Next Expert View unterstützt die folgenden neuen Lokalisierungen: Französisch, Deutsch, Italienisch und Spanisch.

März 2021

Ein neues Web-Plug-in für die Kaspersky Security Center Web Console ermöglicht die Verwendung der folgenden Funktionen von Kaspersky Managed Detection and Response:

- Anzeigen von Vorfällen
- Erstellen von Vorfällen
- Hinzufügen von Kommentaren zu den Vorfällen
- Kontaktaufnahme mit dem Kaspersky Security Operation Center aufgrund eines Vorfalls
- Akzeptieren oder Ablehnen von Reaktionen, die von SOC-Analysten vorschlagen wurden
- Möglichkeit zu unabhängigen Reaktion auf einen Vorfall:
 - Isolieren der Assets vom Netzwerk
 - Erstellen von Regeln zur Blockierung nach Hash
 - Erstellen von vorfallsbezogenen Aufgaben zum Löschen oder zum Verschieben in Quarantäne sowie zum Beenden von Prozessen und zum Suchen nach Gefährdungsindikatoren (IOC)

- Überwachen der Ereignisse von Kaspersky Managed Detection and Response auf den Dashboards der Überwachungskonsole von der Kaspersky Security Center Web Console
- Konfigurieren von Benachrichtigungen via E-Mail oder Telegram über Ereignisse von Kaspersky Managed Detection and Response
- Konfigurieren des Zeitplans zum Senden der Zusammenfassung von Vorfällen per E-Mail

Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response ist eine Lösung, die Sicherheitsvorfälle in Ihrer Infrastruktur mithilfe von Telemetrie und fortschrittlichen Machine-Learning-Technologien automatisch erkennt, analysiert und anschließend Informationen über den Vorfall an Kaspersky-Experten weiterleitet. Die Experten können den Vorfall dann entweder selbst bearbeiten oder Empfehlungen zum Umgang mit dem Vorfall geben.

Kaspersky Managed Detection and Response (auch als MDR bezeichnet) bietet für Unternehmen, die Schwierigkeiten beim Gewinnen von Fachwissen und Mitarbeitern haben, oder denen begrenzte interne Ressourcen zur Verfügung stehen, einen ununterbrochenen Schutz vor der wachsenden Anzahl an Bedrohungen, die in der Lage sind, automatisierte Sicherheitsbarrieren umgehen. Diese Lösung unterstützt Sie beim Ausbauen der Widerstandsfähigkeit Ihres Unternehmens gegenüber Cyberbedrohungen, während er Ihre vorhandenen Ressourcen freisetzt, welche wiederum für andere Aufgaben zur Verfügung stehen.

Im Gegensatz zu ähnlichen Angeboten auf dem Markt setzt diese Lösung auf eine nachgewiesene Erfolgsbilanz von effektiver und gezielter Angriffsforschung, um selbst gegen die komplexesten Bedrohungen zu eine kontinuierliche Verteidigung gewährleisten.

Kaspersky Managed Detection and Response (MDR) steht auf dem Gebiet der USA oder für US-amerikanische Personen nicht zur Verfügung. Die Verwendung der MDR-Lösung innerhalb des genannten Gebiets oder durch US-amerikanische Personen stellt einen Verstoß gegen die [Nutzungsbedingungen der MDR-Lösung](#) dar. Um eine Verletzung der Nutzungsbedingungen der MDR-Lösung zu vermeiden, muss auf allen Assets, die sich innerhalb des genannten Territoriums befinden, oder von US-amerikanische Personen [die Verwendung von MDR dauerhaft eingestellt werden](#). Wenn sich Nicht-US-amerikanische Personen vorübergehend auf dem Gebiet der USA aufhalten, müssen sie für diesen Zeitraum [die Verwendung von MDR auf ihren Assets einstellen](#).

Funktionsweise von Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response analysiert die Telemetriedaten von EPP-Anwendungen und generiert Sicherheitsereignisse, die von der Erkennungstechnologie als Vorfälle klassifiziert werden können.

Kaspersky Managed Detection and Response bezieht Daten von EPP-Anwendungen, die MDR unterstützen, Daten verarbeiten und diese anschließend über die Infrastruktur von [Kaspersky Security Network](#) an Kaspersky Managed Detection and Response senden. Eine Liste der verarbeiteten Daten finden Sie im Abschnitt [Bereitstellung von Daten](#). Die EPP-Anwendungen werden auf den Assets innerhalb der IT-Infrastruktur Ihres Unternehmens installiert (z. B. Mobilgeräte, Computer oder Laptops). Ein Beispiel für eine EPP-Anwendung ist Kaspersky Endpoint Security für Windows.

Die MDR Web Console wird zur Bearbeitung von Vorfällen verwendet. Alternativ dazu können Sie Kaspersky Managed Detection and Response auch in eine Drittanbieter-Lösung integrieren. Weitere Informationen dazu erhalten Sie in dem Artikel [Die Lösung mittels REST-API verwalten](#).

Kaspersky Managed Detection and Response kann einen Vorfall automatisch lösen oder von den Benutzern eine Reaktion auf eine potenzielle Sicherheitsbedrohung anfordern. Weitere Informationen dazu erhalten Sie im Artikel [Arten von Reaktionen](#). Um eine zeitnahe Reaktion auf potenzielle Sicherheitsbedrohungen zu gewährleisten, kann Kaspersky Managed Detection and Response bei verdächtigen Ereignissen eine Zustimmung von Ihnen anfordern. Solche Anfragen sollten Sie rechtzeitig bearbeiten.

Eine detaillierte Untersuchung des Vorfalls (z. B. das Ermitteln vorangegangener Ereignisse, Umstände und des detaillierten Angriffsmechanismus) wird von der Komponente "Kaspersky Incident Response" übernommen. Diese ist nicht in Kaspersky Managed Detection and Response enthalten und muss separat erworben werden.

Die Verwendung von Kaspersky Managed Detection and Response umfasst die von Ihnen mit Unterstützung von Kaspersky-Experten durchgeführte Verarbeitung von Vorfällen. Weitere Informationen finden Sie in diesem Artikel: [Verantwortungsbereiche](#).

Verantwortungsbereiche

Die Verwendung von Kaspersky Managed Detection and Response umfasst das Verarbeiten von Vorfällen durch Benutzer mit Unterstützung durch die MDR-Lösung. Darüber hinaus befasst sich der Technische Support von Kaspersky auch mit Fragen in Bezug auf die Software-Lösung.

In der unteren Tabelle sind die Verantwortungsbereiche für Benutzer, die MDR-Lösung und den Technischen Support von Kaspersky aufgeführt.

Aufgabe	Die MDR-Lösung	Technischer Support von Kaspersky	MDR-Benutzer
MDR aktivieren , MDR bereitstellen , Assets verwalten , Benachrichtigungen einrichten , Benutzer verwalten , MDR-Nutzung beenden	–	Beraten	Ausführung der Aufgabe
Verwendung der MDR Web Console zum Verwalten von Vorfällen	–	Beraten	Aufgabe ausführen
Erkennung, Analyse und Ausstellung von Reaktionsempfehlungen für Vorfälle auf Basis von Telemetriedaten	Ausführung der Aufgabe	–	Informationen abrufen
Klärung von Details im Rahmen der Untersuchung und Beantwortung von Fragen der MDR-Lösung für geeignetere Reaktionsempfehlungen	Informationen abrufen	–	Ausführung der Aufgabe
Erstellung von Anfragen zur Verwendung der Tools und Funktionen von MDR, um Vorfälle zu bearbeiten	Ausführung der Aufgabe	–	Informationen abrufen
Koordinierung der Anfragen zur Verwendung der Tools und Funktionen von MDR, um Vorfälle zu bearbeiten	Informationen abrufen	–	Ausführung der Aufgabe
Ausführen von Aufgaben außerhalb des Funktionsumfangs von MDR	Beraten	–	Ausführung der Aufgabe
Manuelle Erstellung eines Vorfalls (Wichtig: es muss ein MDR-Asset ausgewählt und der Vorfall im Detail beschrieben werden)	Informationen abrufen	–	Ausführung der Aufgabe
Behebung von Problemen mit Komponenten der Kaspersky-Infrastruktur, die sich auf MDR auswirken	Informationen abrufen	Beraten	Ausführung der Aufgabe
Verwaltung von Erkennungsregeln	Ausführung der Aufgabe	–	–

Hardware- und Softwareanforderungen

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Erforderliche EPP-Anwendungen und unterstützte Konfigurationen

Um Kaspersky Managed Detection and Response verwenden zu können, muss in Ihrer Infrastruktur mindestens eine der folgenden EPP-Anwendungen bereitgestellt sein:

- Laptops, Desktops, Tablets und Server
 - [Kaspersky Endpoint Security für Windows](#) 
 - [Kaspersky Endpoint Security für Linux](#) 
 - [Kaspersky Endpoint Security for Mac](#) 
- Industrielle Endpoints
 - [Kaspersky Industrial CyberSecurity for Nodes Windows](#) 
- Virtuelle Systeme
 - [Kaspersky Security for Virtualization Light Agent](#) 
- Embedded Systeme
 - [Kaspersky Embedded Systems Security for Windows](#) 
 - [Kaspersky Embedded Systems Security für Linux](#) 
- Überwachung von Netzwerkereignissen
 - [Kaspersky Anti Targeted Attack Platform](#) 

Betriebssysteme

Kaspersky Managed Detection and Response ist kompatibel mit denselben Betriebssystemen wie die weiter unten aufgeführten EPP-Anwendungen. Für kompatible EPP-Anwendungen finden Sie weitere Informationen in deren Dokumentationen in den Abschnitten zu *Hard- und Softwarevoraussetzungen* (s. a. folgenden Tabelle).

Kompatible Anwendungen und Lösungen von Kaspersky

Kaspersky Managed Detection and Response ist mit den in der folgenden Tabelle aufgeführten Versionen von Kaspersky-Anwendungen kompatibel.

Kaspersky-Anwendung	Empfohlene Versionen und deren Support-Zeiträume	Eingeschränkte MDR-Kompatibilität *	Hinweise
Kaspersky Endpoint Security für Windows	12.10 oder höher 	12.6–12.9 	In Kaspersky Endpoint Security für Windows Version 12.6 bis 12.9 kann die MDR-Lösung mit einem Aktivierungscode aktiviert werden. In Kaspersky Endpoint Security für Windows Version 12.10 oder höher kann die MDR-Lösung auch mit einer Schlüsseldatei aktiviert werden.
Kaspersky Endpoint Security für Windows im Light Agent-Modus	12.9 oder höher 	12.8 	In Kaspersky Endpoint Security für Windows Version 12.6 bis 12.9 im Light Agent-Modus kann die MDR-Lösung mit einem Aktivierungscode aktiviert werden. In Kaspersky Endpoint Security für Windows Version 12.10 oder höher im Light Agent-Modus kann die MDR-Lösung auch mit einer Schlüsseldatei aktiviert werden.
Kaspersky Endpoint Security für Windows in der Konfiguration von Endpoint Detection and Response Agent (EDR Agent) Beginnend mit Version 12.3 von Kaspersky Endpoint Security für Windows enthält die Anwendung die Konfiguration des Agenten für Detection and Response (EDR-Agent). Endpoint Detection and Response Agent ist eine Anwendung, die auf einzelnen Workstations und Servern in der IT-Infrastruktur einer Organisation installiert wird, um Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform (EDR) zu unterstützen. Der EDR-Agent überwacht kontinuierlich die auf diesen Computern ausgeführten Prozesse, die offenen Netzwerkverbindungen und die geänderten Dateien. Für den EDR-Agenten sind keine Schutz- und Kontrollkomponenten verfügbar. Der EDR-Agent ist mit EPP-Anwendungen von Drittanbietern  kompatibel. Auf diese Weise können Sie die Infrastruktur-Sicherheitstools von Drittanbietern zusammen mit Detection and Response von Kaspersky verwenden. Weitere Informationen finden Sie in der Online-Hilfe von Kaspersky Endpoint Security für Windows  .	12.8 oder höher 	12.6–12.7 	- Für Assets mit Kaspersky Endpoint Security für Windows in der EDR Agent-Konfiguration werden die Statuszustände <i>Warnung</i> und <i>Kritisch</i> für Schutz- und Kontrollkomponenten nicht angezeigt. - Sie können die Funktionen von Kaspersky Endpoint Detection and Response Optimum nicht für Assets mit Kaspersky Endpoint Security für Windows in der EDR Agent-Konfiguration verwenden. - Eine Liste der EPP-Anwendungen von Drittanbietern, die mit dem EDR-Agenten kompatibel sind, finden Sie in der Online-Hilfe von Kaspersky Endpoint Security für Windows . In Kaspersky Endpoint Security für Windows Version 12.6 bis 12.9 mit der Konfiguration „Endpoint Detection and Response Agent“ (EDR Agent) kann die MDR-Lösung mit einem Aktivierungscode aktiviert werden. In Kaspersky Endpoint Security für Windows Version 12.10 oder höher mit der Konfiguration „Endpoint Detection and Response Agent“ (EDR Agent) kann die MDR-Lösung auch mit einer Schlüsseldatei aktiviert werden.
Kaspersky Endpoint Security für Linux	12.4 oder höher 	12.1–12.3 	Wenn Sie Kaspersky Endpoint Security für Linux verwenden und das Paket des Linux-Audit-Daemons (auch als auditd bezeichnet) nicht installiert haben, werden Ereignisse des System-Audits im Kernel-Protokoll dmesg protokolliert. Es wird empfohlen, das Paket "auditd" zu installieren, um die Protokollrotation von Kaspersky Endpoint Security für Linux einfacher zu verwalten. In Kaspersky Endpoint Security für Linux Version 12.3 oder höher kann die MDR-Lösung sowohl mit einer Schlüsseldatei als auch mit einem Aktivierungscode aktiviert werden.
Kaspersky Endpoint Security für Linux im Light Agent-Modus	12.4 oder höher 	12.1–12.3 	In Kaspersky Endpoint Security für Linux Version 12.3 oder höher im Light Agent-Modus kann die MDR-Lösung sowohl mit einer Schlüsseldatei als auch mit einem Aktivierungscode aktiviert werden.
Kaspersky Endpoint Security for Mac	12.2 oder höher 	12–12.1 	In Kaspersky Endpoint Security for Mac kann die Aktivierung MDR-Lösung mit einem Aktivierungscode aktiviert werden.

Kaspersky-Anwendung	Empfohlene Versionen und deren Support-Zeiträume	Eingeschränkte MDR-Kompatibilität *	Hinweise
Kaspersky Security for Virtualization Light Agent	6.3 oder höher 	5.2–6.2 	Weitere Informationen finden Sie im folgenden Artikel: Unterstützte Anwendungsversionen im Light Agent-Modus .
Kaspersky Embedded Systems Security for Windows	4.0 oder höher 	4.0 	In Kaspersky Endpoint Security für Windows kann die MDR-Lösung sowohl mit einer Schlüsseldatei als auch mit einem Aktivierungscode aktiviert werden.
Kaspersky Embedded Systems Security für Linux	4.0 oder höher 	4.0 	In Kaspersky Embedded Systems Security für Linux kann die MDR-Lösung sowohl mit einer Schlüsseldatei als auch mit einem Aktivierungscode aktiviert werden.
Kaspersky Industrial CyberSecurity for Nodes Windows	4.5 	4.5 	Verwenden Sie das MDR-Plug-in Version 3.0.0 oder höher, um mehrere Aktivierungscodes für die Lizenz von Kaspersky Industrial CyberSecurity for Nodes anzuwenden. Wenn Sie nur einen Aktivierungscode für die Lizenz von Kaspersky Industrial CyberSecurity for Nodes besitzen, können Sie die MDR Web Console verwenden. Das Anwenden neuer Aktivierungscodes für Kaspersky Industrial CyberSecurity for Nodes ist in der Region "Königreich Saudi-Arabien" nicht möglich, wenn Sie eine der folgenden Lizenzen besitzen: • 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 Agent	-	4.0 oder höher 	Es wird empfohlen, zu Kaspersky Endpoint Security für Windows zu wechseln. Kaspersky Endpoint Agent wird nur verwendet, wenn Sie Kaspersky Security für Windows Server einsetzen.

* Die MDR-Integration ist mit bestimmten funktionalen Einschränkungen verfügbar (z. B. reduzierte Telemetrie oder weniger automatisierte Reaktionsaktionen).

Weitere Informationen über die unterstützten Versionen der Programme und Lösungen von Kaspersky finden Sie auf der [Webseite über den Produkt-Support-Lebenszyklus](#) .

Weitere Informationen über die Integration mit anderen Kaspersky-Lösungen erhalten Sie in diesem Artikel: [Integration mit Anwendungen und Lösungen von Kaspersky](#).

Kaspersky Security Center

In der folgenden Tabelle sind die Komponenten von Kaspersky Security Center aufgeführt, die von der MDR-Lösung unterstützt werden.

Komponenten von Kaspersky Security Center	Versionen und deren Support-Zeiträume	Hinweise
Kaspersky Security Center Windows	15.1 oder höher 	Wird mit dem MDR-Plug-in für Kaspersky Security Center verwendet.
Kaspersky Security Center Linux	15.1 oder höher 	Wird mit dem MDR-Plug-in für Kaspersky Security Center verwendet.
Kaspersky Next Expert View	Expert View	
MDR-Plug-in für Kaspersky Security Center	Aktuellste Version	Die unterstützte Mindestversion ist Version 2.5.1.

MDR Web Console

Für die MDR Web Console gelten die folgenden Hardware- und Softwareanforderungen:

- Monitor mit einer Bildschirmauflösung von 1024x768 oder höher
- Einer der folgenden Browser:
 - Apple Safari 18.3 oder höher auf macOS
 - Google Chrome 143.0.7499.40 oder höher (offizieller Build)
 - Microsoft Edge 143.0.3650.66 oder höher
 - Mozilla Firefox Extended Support Release 140.5.0.2342 oder höher

Netzwerkleistung

Die folgende Tabelle zeigt den auf Grundlage unserer statistischen Daten errechneten Durchsatz des Netzwerkanals an.

Betriebssystem	Geschätzte Bandbreite für 1000 Assets
Windows	4,3 Mbit/s
Windows Server	5,2 Mbit/s
Linux (Durchschnitt für Hosts und Server)	14,7 Mbit/s
macOS	8,5 Mbit/s

Bei diesen Bandbreitenwerten handelt es sich um Näherungswerte, da die erforderliche Bandbreite stark von der Art der Belastung des Assets abhängt, das Telemetrie-Ereignisse generiert. Der Spitzendurchsatz kann deutlich höher ausfallen. Wenn in Ihrer Infrastruktur der Spitzendurchsatz regelmäßig erreicht wird, müssen Sie eine entsprechend höhere Netzwerkbandbreite bereitstellen. Höhere Belastung können durch unterschiedliche Bedingungen auftreten. Beispiel:

- Kompilieren von Programmcode durch Entwickler
- Vollständige Untersuchung des Systems
- Server mit hoher Auslastung (z. B. DNS und Domänencontroller)
- Vielzahl an Netzwerkverbindungen

Funktionalität und Kompatibilität der MDR-Plug-in-Versionen mit Kaspersky Security Center und Open Single Management Platform

Die folgende Tabelle zeigt, welche Versionen von Kaspersky Security Center und Open Single Management Platform mit den MDR-Plug-in-Versionen kompatibel sind.

MDR-Plug-in-Version	Kompatible Version von Kaspersky Security Center	In der MDR-Plug-in-Version hinzugefügte Funktionen
2.5.1	Kaspersky Security Center Windows, Version 15.1 oder höher Kaspersky Security Center Windows Linux, Version 16.1 oder höher	Verwendung mehrerer Lizenzschlüssel. Die Möglichkeit, eine MDR-Konfigurationsdatei (BLOB) für einen bestimmten Lizenzschlüssel zu generieren. Konfiguration von automatischen Reaktionsaktionen für Mandanten. Konfigurierbare mandantenspezifische Berichte.
2.5.2	Kaspersky Security Center Windows, Version 15.1 oder höher Kaspersky Security Center Windows Linux, Version 16.1 oder höher	Betrieb ohne KPSN-Konfigurationsdateien.
3.0.0	Kaspersky Security Center Windows, Version 15.1 oder höher Kaspersky Security Center Windows Linux, Version 16.1 oder höher	Unterstützung für folgende EPP-Anwendungen: - Kaspersky Industrial CyberSecurity for Nodes Windows Version 4.5 oder höher - Kaspersky Embedded Systems Security für Windows Version 4.0 oder höher
3.1.0	Kaspersky Security Center Windows, Version 15.1 oder höher Kaspersky Security Center Windows Linux, Version 16.1 oder höher	Unterstützung für folgende EPP-Anwendungen: Kaspersky Embedded Systems Security für Linux Version 4.0 oder höher Die Möglichkeit, das Asset-Limit für Mandanten anzugeben. Ab Version 3.1.0 des MDR-Plug-ins können Benachrichtigungen in Kaspersky Security Center nicht mehr konfiguriert werden. Verwenden Sie die MDR Web Console, um Benachrichtigungen zu konfigurieren.

Kompatibilität der MDR-Plug-in-Versionen mit Open Single Management Platform

MDR-Plug-in-Version	Kompatible Version von Open Single Management Platform	In der MDR-Plug-in-Version hinzugefügte Funktionen
3.0.1	2.0	Integration mit Kaspersky Endpoint Detection and Response Expert: - Erstellen von MDR-Vorfällen aus EDR-Vorfällen. - Die Reaktionsaktion Get artefacts, mit der Sie Dateien im Zusammenhang mit Alarmen oder Vorfällen von Kaspersky EDR nach Kaspersky SOC kopieren können. Die Unterstützung von Open Single Management Platform, Version 2.0, ist auf die MDR-Plug-in-Version 3.0.1 beschränkt.
3.0.2	2.1	MDR-Integration mit Open Single Management Platform, Version 2.1.
3.1.0	2.1	Unterstützung für folgende EPP-Anwendungen: Kaspersky Embedded Systems Security für Linux Version 4.0 oder höher Die Möglichkeit, das Asset-Limit für Mandanten anzugeben. Ab der MDR-Plug-in-Version 3.1.0 können Benachrichtigungen in Open Single Management Platform nicht mehr konfiguriert werden. Verwenden Sie die MDR Web Console, um Benachrichtigungen zu konfigurieren.
3.1.1	2.2	MDR-Integration mit Open Single Management Platform, Version 2.2.

Komponenten von Kaspersky Managed Detection and Response

Beschreibung der Komponenten von Kaspersky Managed Detection and Response:

- Ein [Asset](#) ist das Gerät einer Organisation, das durch Kaspersky-Lösungen geschützt ist.
- Die Endpoint Protection Platform (EPP) ist eine Anwendung von Kaspersky, welche Assets und die darauf gespeicherten Daten vor Malware und anderen Bedrohungen schützt.

- Kaspersky Endpoint Agent ist eine Programmkomponente, die in der IT-Infrastruktur des Unternehmens auf Workstations und Servern installiert wird. Kaspersky Endpoint Agent überwacht kontinuierlich die auf diesen Computern laufenden Prozesse, die aktiven Netzwerkverbindungen und die geänderten Dateien. In neueren Versionen der EPP-Anwendungen wurde er durch die integrierte Funktionalität ersetzt.
- Kaspersky Network Agent ist eine Komponente von Kaspersky Security Center, welche die Interaktion zwischen dem Administrationsserver und den Kaspersky-Programmen ermöglicht, die auf einem bestimmten Netzknoten (Workstation oder Server) installiert sind. Diese Komponente ist allen Microsoft Windows-Anwendungen von Kaspersky gemeinsam. Für Kaspersky-Programme, die für Unix-ähnliche Betriebssysteme und macOS entwickelt wurden, existieren separate Versionen des Administrationsagenten.
- Kaspersky Security Center ist eine Anwendung, die sich an Administratoren von Unternehmensnetzwerken und Mitarbeiter richtet, die für den Schutz von Assets in einer Vielzahl von Organisationen verantwortlich sind.
- Kaspersky Security Network ist eine Infrastruktur von Cloud-Diensten, die den Zugriff auf die Online-Wissensdatenbank von Kaspersky, welche Informationen über die Reputationen von Dateien, Webressourcen und Software enthält, erlaubt. Die Verwendung von Daten aus Kaspersky Security Network gewährleistet eine schnellere Reaktion der Kaspersky-Programme auf Bedrohungen, verbessert die Leistung einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.
- Kaspersky Managed Detection and Response (auch als MDR bezeichnet) ist eine Lösung, die kontinuierlich verwalteten Schutz bietet und es Unternehmen ermöglicht, ausweichende Bedrohungen automatisch zu eliminieren. Dadurch können sich IT-Sicherheitsteams auf kritischere Aufgaben konzentrieren, die deren Aufmerksamkeit erfordern.
- Die MDR Web Console bietet eine Webschnittstelle zur Verwaltung und Wartung des Schutzsystems für Kunden, deren Organisationsnetzwerke von Kaspersky Managed Detection and Response verwaltet wird. Zusätzlich zur MDR Web Console wurde das Web-Plug-in für Kaspersky Security Center hinzugefügt, um die Verwaltung von Kaspersky Managed Detection and Response in einer einzigen Administrationskonsole zu ermöglichen.
- Die MDR-API stellt die Schnittstelle zur Anwendungsprogrammierung dar, mit der das Netzwerkschutzsystem einer von Kaspersky Managed Detection and Response verwalteten Kundenorganisation gesteuert und unterstützt wird.

Kaspersky Managed Detection and Response aktivieren und bereitstellen

In diesem Abschnitt wird beschrieben, wie Sie Kaspersky Managed Detection and Response aktivieren und bereitstellen.

Um Kaspersky Managed Detection and Response zu aktivieren und bereitzustellen, benötigen Sie eine der folgenden Lösungen für die zentrale Verwaltung der Netzwerksicherheit:

- Lokal: [Kaspersky Security Center Web Console](#) ², [Open Single Management Platform](#) ².
- Cloud-basiert: [Kaspersky Next Expert View](#) ².

Die Schritte zur Bereitstellung von Kaspersky Managed Detection and Response hängen davon ab, welche [EPP-Anwendungen](#) ² auf Ihren Assets installiert sind und ob die [Mehrmandantenfähigkeit](#) verwendet wird.

Aktuelle Anwendungsversionen, ein einzelner Mandant

[Aktivieren und stellen Sie MDR nur mit aktuellen Anwendungen und einem einzelnen Mandanten bereit](#), wenn die folgenden Bedingungen erfüllt sind:

- Auf allen Ihren Assets sind aktuelle Anwendungsversionen installiert:
 - Kaspersky Endpoint Security für Windows Version 12.10 oder höher
 - Kaspersky Endpoint Security für Linux Version 12.3 oder höher
 - Kaspersky Endpoint Security for Mac Version 12.2 oder höher
 - Kaspersky Industrial CyberSecurity for Nodes Windows Version 4.5 oder höher
 - Kaspersky Embedded Systems Security für Windows Version 4.0 oder höher
 - Kaspersky Embedded Systems Security für Linux Version 4.0 oder höher
- Sie planen nicht, die Mehrmandantenfähigkeit sofort nach der Bereitstellung zu konfigurieren. Sie können die Mehrmandantenfähigkeit später konfigurieren.
- Sie verfügen über eine der folgenden Lizenzen:
 - Kaspersky Next Complete Security
 - Kaspersky Optimum Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MXDR Optimum

- Kaspersky MDR
- Kaspersky Managed Detection and Response

Aktuelle Anwendungsversionen, Mehrmandantenfähigkeit

Aktivieren Sie MDR und stellen Sie MDR ausschließlich mithilfe aktueller Anwendungen und der Mehrmandantenfähigkeit bereit, wenn die folgenden Bedingungen erfüllt sind:

- Auf allen Ihren Assets sind aktuelle Anwendungsversionen installiert:
 - Kaspersky Endpoint Security für Windows Version 12.10 oder höher
 - Kaspersky Endpoint Security für Linux Version 12.3 oder höher
 - Kaspersky Endpoint Security for Mac Version 12.2 oder höher
 - Kaspersky Industrial CyberSecurity for Nodes Windows Version 4.5 oder höher
- Sie planen, die Mehrmandantenfähigkeit sofort nach der Bereitstellung zu konfigurieren.
- Sie verfügen über eine der folgenden Lizenzen:
 - Kaspersky Next Complete Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MXDR Optimum
 - Kaspersky MDR
 - Kaspersky Managed Detection and Response
 - Kaspersky MDR Expert Add-on
 - Kaspersky MDR Optimum Add-on
 - Kaspersky Managed Detection and Response Basic Add-on
 - Kaspersky Managed Detection and Response Advanced Add-on
 - Kaspersky Managed Detection and Response Prime Add-on

Ältere Anwendungsversionen

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Aktivieren Sie MDR und stellen Sie MDR bereit, wenn Ihre Infrastruktur Assets mit älteren Anwendungsversionen enthält:

- Kaspersky Endpoint Security für Windows, Version 12.9 und älter
- Kaspersky Endpoint Security für Linux, Version 12.2 oder älter
- Kaspersky Endpoint Security for Mac, Version 12.1 und älter
- Kaspersky Security for Virtualization Light Agent, Version 5.2
- Kaspersky Security für Windows Server mit Kaspersky Endpoint Agent für Windows

Erforderliche Komponenten für den Betrieb von MDR

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

In der folgenden Tabelle sind die Komponenten aufgeführt, die zum Übertragen von Telemetriedaten der Assets erforderlich sind. Wenn eine dieser Komponenten deaktiviert ist oder fehlt, stellt Kaspersky Managed Detection and Response das Senden von Telemetriedaten von dem Asset ein.

Der Light Agent-Modus wird für folgende Versionen unterstützt:

- Kaspersky Endpoint Security für Windows Version 12.8 oder höher
- Kaspersky Endpoint Security für Linux Version 12.1 oder höher

Komponente	Dokumentation
Verhaltensanalyse	Kaspersky Endpoint Security für Windows  Kaspersky Endpoint Security für Linux  Kaspersky Embedded Systems Security for Windows  Kaspersky Embedded Systems Security für Linux  Kaspersky Industrial CyberSecurity for Nodes 
Schutz vor bedrohlichen Dateien	Kaspersky Endpoint Security für Windows  Kaspersky Endpoint Security für Linux  Kaspersky Endpoint Security for Mac  Kaspersky Security for Virtualization Light Agent  Kaspersky Embedded Systems Security for Windows  Kaspersky Embedded Systems Security für Linux  Kaspersky Industrial CyberSecurity for Nodes 
Aktivitätsmonitor	Kaspersky Security for Virtualization Light Agent 

In der folgenden Tabelle sind die Komponenten aufgeführt, die sich auf die Vollständigkeit der übertragenen Telemetriedaten auswirken.

Komponente	Dokumentation
Firewall	Kaspersky Endpoint Security für Windows  Kaspersky Security for Virtualization Light Agent  Kaspersky Embedded Systems Security for Windows  Kaspersky Industrial CyberSecurity for Nodes 
Schutz vor Netzwerkbedrohungen	Kaspersky Endpoint Security für Windows  Kaspersky Endpoint Security für Linux  Kaspersky Endpoint Security for Mac  Kaspersky Embedded Systems Security for Windows  Kaspersky Embedded Systems Security für Linux  Kaspersky Industrial CyberSecurity for Nodes 
Schutz vor E-Mail-Bedrohungen	Kaspersky Endpoint Security für Windows 
Schutz vor Web-Bedrohungen	Kaspersky Endpoint Security für Windows  Kaspersky Endpoint Security für Linux  Kaspersky Endpoint Security for Mac  Kaspersky Embedded Systems Security für Linux  Kaspersky Security for Virtualization Light Agent 
Selbstschutz	Kaspersky Endpoint Security für Windows  Kaspersky Security for Virtualization Light Agent  Kaspersky Embedded Systems Security for Windows  Kaspersky Industrial CyberSecurity for Nodes 

Integration mit Anwendungen und Lösungen von Kaspersky

Die folgende Tabelle beschreibt, wie Sie die Integration von Kaspersky Managed Detection and Response in andere Anwendungen und Lösungen von Kaspersky konfigurieren.

Lösung oder Anwendung	Version	Konfiguration
Kaspersky Endpoint Security für Windows Kaspersky Endpoint Security für Linux Kaspersky Endpoint Security for Mac Kaspersky Security for Virtualization Light Agent Kaspersky Industrial CyberSecurity for Nodes Windows Kaspersky Embedded Systems Security Windows Kaspersky Security für Windows Server mit Kaspersky Endpoint Agent für Windows		Lesen Sie den folgenden Artikel: MDR-Lösung in Kaspersky-Anwendungen aktivieren .

Lösung oder Anwendung	Version	Konfiguration
Kaspersky Endpoint Detection and Response Expert (on-premise)	8.0 oder höher, integriert in die Open Single Management Platform mit Kaspersky Next XDR 2.1 oder höher	Erfordert aktive Lizenzschlüssel für Kaspersky MDR Expert und Kaspersky EDR Expert. Für die Konfiguration der Integration wird die Rolle MDR-Administrator benötigt. 1. Konfigurieren Sie das MDR-Plug-in in der Konsole der Open Single Management Platform. 2. Klicken Sie in der Konsolenoberfläche von OSMP im MDR-Abschnitt auf die Registerkarte MDR-Nutzung. 3. Erweitern Sie den Block KPSN-Konfigurationsdatei für die Integration mit KEDR Expert. 4. Aktivieren Sie die Option KPSN-Vereinbarung akzeptieren und klicken Sie auf KPSN-Konfigurationsdatei für die Integration mit KEDR Expert anwenden. Die MDR-Lösung empfängt jetzt Telemetriedaten, einschließlich KEDR-Alarme, um diese zu analysieren.
Kaspersky Unified Monitoring and Analysis Platform	4.0 oder höher	Lesen Sie den folgenden Artikel: Integration von Kaspersky Managed Detection and Response .
Kaspersky Anti Targeted Attack (KATA) Platform	7.0–7.1	1. Laden Sie die MDR-Konfigurationsdatei herunter. 2. Aktivieren Sie die Integration von MDR. Nicht verfügbar in folgender Region: Königreich Saudi-Arabien.
	8.0 oder höher	Stellen Sie sicher, dass der Server, auf dem die Einrichtung der Integration mit der MDR-Lösung stattfindet, Netzwerkzugriff auf die folgenden Adressen besitzt: • *uis.kaspersky.com:443 • mdr.kaspersky.com:443 Stellen Sie sicher, dass die sekundären KATA-Server Netzwerkzugriff auf folgende Adresse besitzen: mdr.kaspersky.com:443. Lesen Sie den folgenden Artikel: Integration mit Kaspersky Managed Detection and Response konfigurieren. Nicht verfügbar in folgender Region: Königreich Saudi-Arabien.

Das MDR-Plug-ins konfigurieren

Um Kaspersky Managed Detection and Response mithilfe der MDR-Plug-in-Funktionalität zu verwalten, müssen Sie das MDR-Plug-in in der Lösung installieren, mit der Sie die Netzwerksicherheit zentral verwalten:

- Kaspersky Security Center Web Console
- Kaspersky Next Expert View
Das MDR-Plug-in ist in Kaspersky Next Expert View vorinstalliert.
- Open Single Management Platform

Voraussetzungen

Stellen Sie sicher, dass Sie Zugriff auf Kaspersky Security Center Web Console, Kaspersky Next Expert View oder Open Single Management Platform haben und mindestens über die folgenden Zugriffsrechte verfügen:

- Zugriffsrecht **Lesen** für den Funktionsbereich [Allgemeine Funktionen: Anwendungsintegration](#) 
- Die Zugriffsberechtigung für den Funktionsbereich [Zugriff auf Vorfälle](#) von Kaspersky Managed Detection and Response ist auf **Erlauben** gesetzt.

MDR-Plug-in in Kaspersky Security Center Web Console installieren

So installieren Sie das MDR-Plug-in in Kaspersky Security Center Web Console:

1. Gehen Sie im Hauptmenü von Kaspersky Security Center Web Console zu **Einstellungen** → **Web-Plug-ins**.
2. Klicken Sie im folgenden Fenster auf **Hinzufügen**.
Eine Liste der verfügbaren Plug-ins wird angezeigt.
3. Wählen Sie in der Liste der verfügbaren Plug-ins das MDR-Plug-in aus.
Eine Seite mit der Beschreibung des Plug-ins wird angezeigt.
4. Klicken Sie auf der Seite mit der Beschreibung des Plug-ins auf **Plug-in installieren**.
5. Klicken Sie nach Abschluss der Installation auf **OK**.

Das MDR-Plug-in wird mit der Standardkonfiguration heruntergeladen und in der Liste mit den Verwaltungs-Web-Plug-ins angezeigt.

MDR-Plug-in in Open Single Management Platform installieren

Wenn die Open Single Management Platform in einer geschlossenen Netzwerkumgebung betrieben wird, müssen Sie Proxy-Einstellungen angeben. Führen Sie auf dem Host der Open Single Management Platform den folgenden Befehl aus, um Umgebungsvariablen mit Proxy-Einstellungen hinzuzufügen:

```
kubectl set env deployment/plugin-mdr-proxy -n nwc \
  HTTP_PROXY=http://<proxy>:8080 \
  HTTPS_PROXY=http://<proxy>:8080 \
  NO_PROXY=localhost,127.0.0.1,.local,.cluster.local
```

Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Umgebungsvariablen konfiguriert wurden:

```
kubectl rollout status deployment/plugin-mdr-proxy -n nwc
```

So installieren Sie das MDR-Plug-in in OSMP:

1. Verschieben Sie das Web-Plug-in zur Verwaltung auf den Administrator-Host, auf dem sich das KDT-Tool befindet.
2. Führen Sie auf dem Administrator-Host, auf dem sich das KDT-Tool befindet, den folgenden Befehl aus, um das Plug-in zu installieren:

```
./kdt apply -k <Pfad zum Plug-in-Archiv>
```

3. Aktualisieren Sie die Benutzeroberfläche der OSMP-Konsole, um das hinzugefügte Plug-in anzuzeigen.

Das Web-Plug-in zur Verwaltung von MDR ist installiert und Sie können die MDR-Funktionen in der OSMP-Konsole aufrufen.

Sie können das KDT-Tool verwenden, um die Liste der installierten Web-Plug-ins anzuzeigen und sicherzustellen, dass das Web-Plug-in zur Verwaltung von MDR erfolgreich installiert wurde.

So zeigen Sie die Liste der Web-Plug-ins zur Verwaltung und weiterer OSMP-bezogener Komponenten an,

Führen Sie auf dem Administrator-Host, auf dem sich das KDT-Tool befindet, den folgenden Befehl aus:

```
./kdt state
```

Die Liste der in OSMP integrierten Komponenten wird im Befehlszeilenfenster angezeigt. Sie können die Liste prüfen, um sicherzustellen, dass das Web-Plug-in zur Verwaltung von MDR installiert wurde.

Ergebnisse

Nach Abschluss dieses Szenarios ist das MDR-Plug-in für die Arbeit mit Kaspersky Managed Detection and Response eingerichtet.

Aktivierung und Bereitstellung von MDR, wenn aktuelle Anwendungsversionen und ein einzelner Mandant verwendet werden

Die folgende Anleitung zur Aktivierung und Bereitstellung der MDR-Lösung eignet sich, wenn die unten genannten Bedingungen erfüllt sind:

- Auf allen Ihren Assets sind aktuelle Anwendungsversionen installiert:
 - Kaspersky Endpoint Security für Windows Version 12.10 oder höher
 - Kaspersky Endpoint Security für Linux Version 12.3 oder höher
 - Kaspersky Endpoint Security for Mac Version 12.2 oder höher

- Kaspersky Industrial CyberSecurity for Nodes Windows Version 4.5 oder höher
- Kaspersky Embedded Systems Security für Windows Version 4.0 oder höher
- Kaspersky Embedded Systems Security für Linux Version 4.0 oder höher
- Sie planen nicht, die [Mehrmandantenfähigkeit](#) sofort nach der Bereitstellung zu verwenden.
Die Mehrmandantenfähigkeit können Sie später konfigurieren, indem Sie MDR-Konfigurationsdateien (BLOB) zu Anwendungen hinzufügen.
- Sie besitzen eine der folgenden Lizenzen:
 - Kaspersky Next Complete Security
 - Kaspersky Optimum Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MDR Optimum
 - Kaspersky MDR
 - Kaspersky Managed Detection and Response

Voraussetzungen

Stellen Sie sicher, dass Ihre IT-Infrastruktur die [Hardware- und Softwareanforderungen von Kaspersky Managed Detection and Response](#) erfüllt.

Aktivierung und Bereitstellung

Gehen Sie folgendermaßen vor, um die MDR-Lösung zu aktivieren und bereitzustellen:

Schritt 1. Authentifizierung in der MDR Web Console

Führen Sie die folgenden Schritte aus:

1. Gehen Sie zur [MDR Web Console](#).
2. Klicken Sie auf **Benutzerkonto erstellen**. Erstellen Sie ein neues Benutzerkonto.
3. Melden Sie sich mit dem erstellten Benutzerkonto in der [MDR Web Console](#) an.
4. Wenn Sie dazu aufgefordert werden, geben Sie den Aktivierungscode ein. Der Aktivierungscode wurde an die E-Mail-Adresse gesendet, die Sie beim Erstellen des Benutzerkontos angegeben haben.

5. Wählen Sie die Region für die Datenverarbeitung aus und berücksichtigen Sie dabei den Standort, an dem die Lizenz genutzt wird.
6. Wenn Sie dazu aufgefordert werden, akzeptieren Sie die Vereinbarungen und bestätigen Sie die MDR-Aktivierung.

Schritt 2. Aktivierung der MDR-Lösung auf Ihren Assets

Wenn Sie die MDR-Lösung mit einer der folgenden Lizenzen verwenden, wird die MDR-Lösung automatisch auf Ihren Assets aktiviert, sodass Sie diesen Schritt überspringen und mit Phase 3 fortfahren können:

- Kaspersky Next Complete Security
- Kaspersky Symphony MDR
- Kaspersky Next MDR Optimum

Aktivieren Sie die MDR-Lizenz auf Ihren Assets:

Aktivierung in der Kaspersky Security Center Web Console

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Lizenzen für Kaspersky-Software**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Fügen Sie die Schlüsseldatei hinzu oder geben Sie den Aktivierungscode ein:
 - **Schlüsseldatei hinzufügen**
Klicken Sie auf die Schaltfläche **Schlüsseldatei auswählen** und suchen Sie die .key-Datei, die Sie hinzufügen möchten.
 - **Aktivierungscode eingeben**
Geben Sie den Aktivierungscode ein und klicken Sie auf die Schaltfläche **Senden**.
4. Klicken Sie auf **Schließen**.
5. Klicken Sie auf der Seite **Lizenzen für Kaspersky-Software** auf den Namen der aktuellen Lizenz.
Die Eigenschaften der Lizenz werden geöffnet.
6. Aktivieren Sie auf der Registerkarte **Allgemein** den Parameter **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.
7. Klicken Sie auf die Schaltfläche **Speichern**.

Der Lizenzschlüssel wird automatisch an die Assets verteilt. Wie ein Lizenzschlüssel mithilfe der Aufgabe zur Verteilung von Lizenzschlüsseln an Client-Geräte verteilt wird, erfahren Sie in der [Online-Hilfe zu Kaspersky Security Center](#).

Aktivierung in Open Single Management Platform

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
Das Eigenschaftensfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Lizenzschlüssel** aus.
3. Klicken Sie auf **Neuen Lizenzschlüssel hinzufügen** und geben Sie einen neuen Lizenzschlüssel an.
4. Klicken Sie auf die Schaltfläche **Speichern**.
5. Klicken Sie auf der Seite **Lizenzschlüssel** auf den Namen des hinzugefügten Lizenzschlüssels.
Die Eigenschaften des Lizenzschlüssels werden geöffnet.
6. Aktivieren Sie auf der Registerkarte **Allgemein** den Parameter **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.
7. Klicken Sie auf die Schaltfläche **Speichern**.

Der Lizenzschlüssel wird automatisch an die Assets verteilt.

Im folgenden Artikel wird beschrieben, wie Sie auf dem Administrationsserver verwendete Lizenzschlüssel und Aktivierungs-codes anzeigen: [Informationen über verwendete Lizenzschlüssel und Aktivierungs-codes anzeigen](#)^[4].

Schritt 3. Aktivieren der KSN-Nutzung

Gehen Sie in Kaspersky Security Center Web Console, Kaspersky Next Expert View oder Open Single Management Platform zum Abschnitt **Asset-Management** → **Richtlinien und Profile**. Aktivieren Sie die KSN-Nutzung in den Richtlinien für alle Anwendungen, die auf Ihren Assets verwendet werden:

Kaspersky Endpoint Security für Windows/Linux

1. Wählen Sie die Anwendungsrichtlinie aus. Wenn noch keine Anwendungsrichtlinie erstellt wurde, klicken Sie auf **Hinzufügen** und erstellen Sie die Richtlinie.
2. Gehen Sie in den Einstellungen der Anwendungsrichtlinie zu **Anwendungseinstellungen** → **Allgemeine Einstellungen** → **Kaspersky Security Network**.
3. Aktivieren Sie den Parameter **Nutzung von Kaspersky Security Network**.
4. Aktivieren Sie den Parameter **Erweiterten KSN-Modus verwenden**.
5. Wenn Sie den Administrationsserver als Proxy verwenden möchten, aktivieren Sie die folgenden Parameter:
 - **Administrationsserver als KSN-Proxyserver verwenden**, um Asset-Telemetriedaten über den KSN-Proxy zu senden.
 - **Kaspersky Security Network-Server verwenden, wenn der KSN-Proxyserver nicht verfügbar ist**, um Asset-Telemetriedaten über KSN zu senden, wenn der KSN-Proxy nicht verfügbar ist.
6. Klicken Sie auf **Speichern und schließen**.

Client-Geräte können Anfragen an KSN initiieren, Informationen von KSN beziehen und Informationen an KSN übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen. Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Kaspersky Endpoint Security for Mac

1. Wählen Sie die Anwendungsrichtlinie aus. Wenn noch keine Anwendungsrichtlinie erstellt wurde, klicken Sie auf **Hinzufügen** und erstellen Sie die Richtlinie.
2. Gehen Sie in den Einstellungen der Anwendungsrichtlinie zu **Anwendungseinstellungen** → **Erweiterter Schutz** → **Kaspersky Security Network**.
3. Aktivieren Sie den Parameter **Kaspersky Security Network**.
4. Aktivieren Sie den Parameter **Erweiterter KSN-Modus**.
5. Wenn Sie den Administrationsserver als Proxy verwenden möchten, aktivieren Sie die folgenden Parameter:
 - **Administrationsserver als KSN-Proxyserver verwenden**, um Asset-Telemetriedaten über den KSN-Proxy zu senden.
 - **Kaspersky Security Network-Server verwenden, wenn der KSN-Proxyserver nicht verfügbar ist**, um Asset-Telemetriedaten über KSN zu senden, wenn der KSN-Proxy nicht verfügbar ist.
6. Klicken Sie auf **Speichern und schließen**.

Client-Geräte können Anfragen an KSN initiieren, Informationen von KSN beziehen und Informationen an KSN übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen. Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Schritt 4. Netzwerkeinstellungen für Ihre Assets konfigurieren

Deaktivieren Sie für Assets mit Internetzugriff die Analyse des Datenverkehrs über die Ports 443 und 1443 und erlauben Sie ausgehenden Nicht-SSL-Verkehr an die folgenden Adressen:

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Konfigurieren Sie für Assets ohne Internetzugriff den KSN-Proxy für den Zugriff auf die KSN-Server. Erlauben Sie ausgehenden Nicht-SSL-Datenverkehr und deaktivieren Sie die Analyse des Datenverkehrs für die folgenden Varianten:

- Datenverkehr vom Asset zum KSN-Proxy über Port 13111 ([Standardport](#) .
- Datenverkehr von KSN-Proxy über die Ports 443 und 1443 an die folgenden Adressen:

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Es wird empfohlen, eine direkte Verbindung zwischen den Assets und den KSN-Servern zu konfigurieren. Dieser Ansatz hilft bei der Vermeidung von Telemetriedatenverlust, wenn der KSN-Proxy nicht verfügbar ist oder Laptops eine Remote-Verbindung verwenden.

Die MDR-Lösung wurde aktiviert und bereitgestellt. Assets, die von MDR verwaltet werden, werden nach der Synchronisierung in der MDR Web Console angezeigt (innerhalb von 24 Stunden): mdr.kaspersky.com/assets.

Jetzt können Sie mit der Konfiguration der MDR-Lösung fortfahren:

- [Laden Sie neue Benutzer in der MDR Web Console ein.](#)
- [Konfigurieren Sie regelmäßige Benachrichtigungen.](#)
- [Erweiterte Benachrichtigungen aktivieren](#)

Aktivierung und Bereitstellung von MDR, wenn aktuelle Anwendungsversionen und Mehrmandantenfähigkeit verwendet werden

Die folgende Anleitung zur Aktivierung und Bereitstellung der MDR-Lösung eignet sich, wenn die unten genannten Bedingungen erfüllt sind:

- Auf allen Ihren Assets sind aktuelle Anwendungsversionen installiert:
 - Kaspersky Endpoint Security für Windows Version 12.10 oder höher
 - Kaspersky Endpoint Security für Linux Version 12.3 oder höher
 - Kaspersky Endpoint Security for Mac Version 12.2 oder höher
 - Kaspersky Industrial CyberSecurity for Nodes Windows Version 4.5 oder höher
 - Kaspersky Embedded Systems Security für Windows Version 4.0 oder höher (kann nur dem Root-Mandanten zugewiesen werden)
 - Kaspersky Embedded Systems Security für Linux Version 4.0 oder höher (kann nur dem Root-Mandanten zugewiesen werden)
- Sie planen, die [Mehrmandantenfähigkeit](#) sofort nach der Bereitstellung zu verwenden.
- Sie besitzen eine der folgenden Lizenzen:
 - Kaspersky Next Complete Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MXDR Optimum
 - Kaspersky MDR

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

Voraussetzungen

Stellen Sie sicher, dass Ihre IT-Infrastruktur die [Hardware- und Softwareanforderungen von Kaspersky Managed Detection and Response](#) erfüllt.

Aktivierung und Bereitstellung

Gehen Sie folgendermaßen vor, um die MDR-Lösung zu aktivieren und bereitzustellen:

Schritt 1. Authentifizierung in der MDR Web Console

Führen Sie die folgenden Schritte aus:

1. Gehen Sie zur [MDR Web Console](#).
2. Klicken Sie auf **Benutzerkonto erstellen**. Erstellen Sie ein neues Benutzerkonto.
3. Melden Sie sich mit dem erstellten Benutzerkonto in der [MDR Web Console](#) an.
4. Wenn Sie dazu aufgefordert werden, geben Sie den Aktivierungscode ein. Der Aktivierungscode wurde an die E-Mail-Adresse gesendet, die Sie beim Erstellen des Benutzerkontos angegeben haben.
5. Wählen Sie die Region für die Datenverarbeitung aus und berücksichtigen Sie dabei den Standort, an dem die Lizenz genutzt wird.
6. Wenn Sie dazu aufgefordert werden, akzeptieren Sie die Vereinbarungen und bestätigen Sie die MDR-Aktivierung.

Schritt 2. Erstellen von Mandanten und Herunterladen von Konfigurationsdateien

Folgen Sie den nachstehenden Anweisungen:

1. [Erstellen Sie neue Mandanten in der MDR Web Console.](#)
2. Laden Sie für jeden erstellten Mandanten [die MDR-Konfigurationsdatei herunter und fügen Sie die BLOB-Datei \(P7\) zu den Anwendungsrichtlinien hinzu.](#)

Schritt 3. Aktivierung der MDR-Lösung auf Ihren Assets

Wenn Sie die MDR-Lösung mit einer der folgenden Lizenzen verwenden, wird die MDR-Lösung automatisch auf Ihren Assets aktiviert. Sie können diesen Schritt daher überspringen und mit Schritt 4 fortfahren:

- Kaspersky Next Complete Security
- Kaspersky Symphony MDR
- Kaspersky Next MDR Optimum

Aktivieren Sie die MDR-Lizenz auf Ihren Assets:

Aktivierung in der Kaspersky Security Center Web Console

1. Gehen Sie im Hauptmenü zu **Vorgänge → Lizenzen für Kaspersky-Software**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Fügen Sie die Schlüsseldatei hinzu oder geben Sie den Aktivierungscode ein:

- **Schlüsseldatei hinzufügen**

Klicken Sie auf die Schaltfläche **Schlüsseldatei auswählen** und suchen Sie die .key-Datei, die Sie hinzufügen möchten.

- **Aktivierungscode eingeben**

Geben Sie den Aktivierungscode ein und klicken Sie auf die Schaltfläche **Senden**.

4. Klicken Sie auf **Schließen**.
5. Klicken Sie auf der Seite **Lizenzen für Kaspersky-Software** auf den Namen der aktuellen Lizenz.
Die Eigenschaften der Lizenz werden geöffnet.
6. Aktivieren Sie auf der Registerkarte **Allgemein** den Parameter **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.
7. Klicken Sie auf die Schaltfläche **Speichern**.

Der Lizenzschlüssel wird automatisch an die Assets verteilt. Wie ein Lizenzschlüssel mithilfe der Aufgabe zur Verteilung von Lizenzschlüsseln an Client-Geräte verteilt wird, erfahren Sie in der [Online-Hilfe zu Kaspersky Security Center](#).

Aktivierung in Open Single Management Platform

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Lizenzschlüssel** aus.

3. Klicken Sie auf **Neuen Lizenzschlüssel hinzufügen** und geben Sie einen neuen Lizenzschlüssel an.

4. Klicken Sie auf die Schaltfläche **Speichern**.

5. Klicken Sie auf der Seite **Lizenzschlüssel** auf den Namen des hinzugefügten Lizenzschlüssels.

Die Eigenschaften des Lizenzschlüssels werden geöffnet.

6. Aktivieren Sie auf der Registerkarte **Allgemein** den Parameter **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.

7. Klicken Sie auf die Schaltfläche **Speichern**.

Der Lizenzschlüssel wird automatisch an die Assets verteilt.

Im folgenden Artikel wird beschrieben, wie Sie auf dem Administrationsserver verwendete Lizenzschlüssel und Aktivierungs-codes anzeigen: [Informationen über verwendete Lizenzschlüssel und Aktivierungs-codes anzeigen](#).

Schritt 4. Aktivieren der KSN-Nutzung

Gehen Sie in Kaspersky Security Center Web Console, Kaspersky Next Expert View oder Open Single Management Platform zum Abschnitt **Asset-Management** → **Richtlinien und Profile**. Aktivieren Sie die KSN-Nutzung in den Richtlinien für alle Anwendungen, die auf Ihren Assets verwendet werden:

Kaspersky Endpoint Security für Windows/Linux

1. Wählen Sie die Anwendungsrichtlinie aus. Wenn noch keine Anwendungsrichtlinie erstellt wurde, klicken Sie auf **Hinzufügen** und erstellen Sie die Richtlinie.

2. Gehen Sie in den Einstellungen der Anwendungsrichtlinie zu **Anwendungseinstellungen** → **Allgemeine Einstellungen** → **Kaspersky Security Network**.

3. Aktivieren Sie den Parameter **Nutzung von Kaspersky Security Network**.

4. Aktivieren Sie den Parameter **Erweiterten KSN-Modus verwenden**.

5. Wenn Sie den Administrationsserver als Proxy verwenden möchten, aktivieren Sie die folgenden Parameter:

- **Administrationsserver als KSN-Proxyserver verwenden**, um Asset-Telemetriedaten über den KSN-Proxy zu senden.
- **Kaspersky Security Network-Server verwenden, wenn der KSN-Proxyserver nicht verfügbar ist**, um Asset-Telemetriedaten über KSN zu senden, wenn der KSN-Proxy nicht verfügbar ist.

6. Klicken Sie auf **Speichern und schließen**.

Client-Geräte können Anfragen an KSN initiieren, Informationen von KSN beziehen und Informationen an KSN übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen. Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Kaspersky Endpoint Security for Mac

1. Wählen Sie die Anwendungsrichtlinie aus. Wenn noch keine Anwendungsrichtlinie erstellt wurde, klicken Sie auf **Hinzufügen** und erstellen Sie die Richtlinie.
2. Gehen Sie in den Einstellungen der Anwendungsrichtlinie zu **Anwendungseinstellungen → Erweiterter Schutz → Kaspersky Security Network**.
3. Aktivieren Sie den Parameter **Kaspersky Security Network**.
4. Aktivieren Sie den Parameter **Erweiterter KSN-Modus**.
5. Wenn Sie den Administrationsserver als Proxy verwenden möchten, aktivieren Sie die folgenden Parameter:

- **Administrationsserver als KSN-Proxyserver verwenden**, um Asset-Telemetriedaten über den KSN-Proxy zu senden.
- **Kaspersky Security Network-Server verwenden, wenn der KSN-Proxyserver nicht verfügbar ist**, um Asset-Telemetriedaten über KSN zu senden, wenn der KSN-Proxy nicht verfügbar ist.

6. Klicken Sie auf **Speichern und schließen**.

Client-Geräte können Anfragen an KSN initiieren, Informationen von KSN beziehen und Informationen an KSN übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen. Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Schritt 5. Netzwerkeinstellungen für Ihre Assets konfigurieren

Deaktivieren Sie für Assets mit Internetzugriff die Analyse des Datenverkehrs über die Ports 443 und 1443 und erlauben Sie ausgehenden Nicht-SSL-Verkehr an die folgenden Adressen:

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Konfigurieren Sie für Assets ohne Internetzugriff den KSN-Proxy für den Zugriff auf die KSN-Server. Erlauben Sie ausgehenden Nicht-SSL-Datenverkehr und deaktivieren Sie die Analyse des Datenverkehrs für die folgenden Varianten:

- Datenverkehr vom Asset zum KSN-Proxy über Port 13111 ([Standardport](#) )
- Datenverkehr von KSN-Proxy über die Ports 443 und 1443 an die folgenden Adressen:
 - *.ksn.kaspersky-labs.com
 - ksn-*.kaspersky-labs.com
 - ds.kaspersky.com

Es wird empfohlen, eine direkte Verbindung zwischen den Assets und den KSN-Servern zu konfigurieren. Dieser Ansatz hilft bei der Vermeidung von Telemetriedatenverlust, wenn der KSN-Proxy nicht verfügbar ist oder Laptops eine Remote-Verbindung verwenden.

Die MDR-Lösung wurde aktiviert und bereitgestellt. Assets, die von MDR verwaltet werden, werden nach der Synchronisierung in der MDR-Konsole angezeigt (innerhalb von 24 Stunden): mdr.kaspersky.com/assets.

Jetzt können Sie mit der Konfiguration der MDR-Lösung fortfahren:

- [Laden Sie neue Benutzer in MDR Console ein.](#)
- [Konfigurieren Sie regelmäßige Benachrichtigungen.](#)
- [Erweiterte Benachrichtigungen aktivieren](#)

Aktivierung und Bereitstellung von MDR, wenn ältere Anwendungsversionen verwendet werden

Verwenden Sie die folgende Anleitung, wenn Ihre Infrastruktur Assets mit älteren Anwendungsversionen enthält:

- Kaspersky Endpoint Security für Windows, Version 12.9 und älter
- Kaspersky Endpoint Security für Linux, Version 12.2 oder älter
- Kaspersky Endpoint Security for Mac, Version 12.1 und älter
- Kaspersky Security for Virtualization Light Agent, Version 5.2
- Kaspersky Security für Windows Server mit Kaspersky Endpoint Agent für Windows

Voraussetzungen

Stellen Sie sicher, dass Ihre IT-Infrastruktur die [Hardware- und Softwareanforderungen von Kaspersky Managed Detection and Response](#) erfüllt.

Aktivierung und Bereitstellung

Die Aktivierung und Bereitstellung der MDR-Lösung erfolgt in mehreren Schritten:

Schritt 1. Authentifizierung in der MDR Web Console

Führen Sie die folgenden Schritte aus:

1. Gehen Sie zur [MDR Web Console](#).
2. Klicken Sie auf **Benutzerkonto erstellen**. Erstellen Sie ein neues Benutzerkonto.
3. Melden Sie sich mit dem erstellten Benutzerkonto in der [MDR Web Console](#) an.
4. Wenn Sie dazu aufgefordert werden, geben Sie den Aktivierungscode ein. Der Aktivierungscode wurde an die E-Mail-Adresse gesendet, die Sie beim Erstellen des Benutzerkontos angegeben haben.
5. Wählen Sie die Region für die Datenverarbeitung aus und berücksichtigen Sie dabei den Standort, an dem die Lizenz genutzt wird.
6. Wenn Sie dazu aufgefordert werden, akzeptieren Sie die Vereinbarungen und bestätigen Sie die MDR-Aktivierung.

Schritt 2. Erstellen von Mandanten und Herunterladen von Konfigurationsdateien

Folgen Sie den nachstehenden Anweisungen:

1. Wenn Sie die Mehrmandantenfähigkeit benötigen, [erstellen Sie neue Mandanten in der MDR-Konsole](#).
2. Laden Sie für jeden erstellten Mandanten [die MDR-Konfigurationsdatei herunter und fügen Sie die BLOB-Datei \(P7\) zu den Anwendungsrichtlinien hinzu](#).

Schritt 3. Konfigurieren von KPSN

[Stellen Sie die KPSN-Konfigurationsdatei bereit.](#)

Schritt 4. Aktivieren der KSN-Nutzung

Gehen Sie in Kaspersky Security Center Web Console, Kaspersky Next Expert View oder Open Single Management Platform zum Abschnitt **Asset-Management** → **Richtlinien und Profile**. Aktivieren Sie die KSN-Nutzung in den Richtlinien für alle Anwendungen, die auf Ihren Assets verwendet werden:

1. Wählen Sie die Anwendungsrichtlinie aus. Wenn noch keine Anwendungsrichtlinie erstellt wurde, klicken Sie auf **Hinzufügen** und erstellen Sie die Richtlinie.
2. Gehen Sie in den Einstellungen der Anwendungsrichtlinie zu **Anwendungseinstellungen** → **Erweiterter Schutz** → **Kaspersky Security Network**.
3. Aktivieren Sie den Parameter **Kaspersky Security Network**.
4. Aktivieren Sie den Parameter **Erweiterter KSN-Modus**.
5. (Optional) Wenn der Administrationsserver als Proxy verwendet wird, aktivieren Sie die folgenden Parameter:
 - Aktivieren Sie **Administrationsserver als KSN-Proxyserver verwenden**, um Asset-Telemetriedaten über den KSN-Proxy zu senden.
 - Aktivieren Sie **Kaspersky Security Network-Server verwenden, wenn der KSN-Proxyserver nicht verfügbar ist**.
6. Klicken Sie auf **Speichern und schließen**.

Client-Geräte können Anfragen an KSN initiieren, Informationen von KSN beziehen und Informationen an KSN übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen. Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Schritt 5. Netzwerkeinstellungen für Ihre Assets konfigurieren

Deaktivieren Sie für Assets mit Internetzugang die Analyse des Datenverkehrs über die Ports 443 und 1443 und erlauben Sie ausgehenden Nicht-SSL-Verkehr an die folgenden Adressen:

*.ksn.kaspersky-labs.com

ksn-*.kaspersky-labs.com

ds.kaspersky.com

Konfigurieren Sie für Assets ohne Internetzugang den KSN-Proxy für den Zugriff auf die KSN-Server. Erlauben Sie ausgehenden Nicht-SSL-Datenverkehr und deaktivieren Sie die Analyse des Datenverkehrs für die folgenden Varianten:

- Datenverkehr vom Asset zum KSN-Proxy über Port 13111 ([Standardport](#) ).
- Datenverkehr von KSN-Proxy über die Ports 443 und 1443 an die folgenden Adressen:

*.ksn.kaspersky-labs.com
ksn-*.kaspersky-labs.com
ds.kaspersky.com

Es wird empfohlen, eine direkte Verbindung zwischen den Assets und den KSN-Servern zu konfigurieren. Dieser Ansatz hilft bei der Vermeidung von Telemetriedatenverlust, wenn der KSN-Proxy nicht verfügbar ist oder Laptops eine Remote-Verbindung verwenden.

Die MDR-Lösung wurde aktiviert und bereitgestellt. Assets, die von MDR verwaltet werden, werden nach der Synchronisierung in der MDR Console angezeigt (innerhalb von 24 Stunden): mdr.kaspersky.com/assets.

Jetzt können Sie mit der Konfiguration der MDR-Lösung fortfahren:

- [Laden Sie neue Benutzer in MDR Console ein.](#)
- [Konfigurieren Sie regelmäßige Benachrichtigungen.](#)
- [Erweiterte Benachrichtigungen aktivieren](#)

KPSN-Konfigurationsdatei bereitstellen

Sie müssen eine KPSN-Konfigurationsdatei bereitstellen, wenn auf mindestens einem Asset in Ihrer Infrastruktur eine ältere Anwendungsversion installiert ist:

- Kaspersky Endpoint Security für Windows 12.9 und älter
- Kaspersky Endpoint Security für Linux, Version 12.2 oder älter
- Kaspersky Endpoint Security for Mac, Version 12.1 und älter
- Kaspersky Security for Virtualization Light Agent, Version 5.2
- Kaspersky Security für Windows Server mit Kaspersky Endpoint Agent für Windows

Die Bereitstellung einer KPSN-Konfigurationsdatei erfolgt in zwei Schritten.

Schritt 1. Download der MDR-Konfigurationsdatei

Das Vorgehen für den Download der MDR-Konfigurationsdatei hängt davon ab, ob Sie zusätzliche Mandanten erstellt und das MDR-Plug-in für Kaspersky Security Center installiert haben.

Die MDR-Konfigurationsdatei ist ein ZIP-Archiv, das eine KPSN-Konfigurationsdatei (.pkcs7) für die Bereitstellung von EPP-Anwendungen enthält.

So laden Sie die MDR-Konfigurationsdatei in der MDR Web Console herunter:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Settings**.
2. Öffnen Sie die Registerkarte **Tenants**.
3. Klicken Sie auf die Zeile mit dem Mandanten, für den Sie die MDR-Konfigurationsdatei herunterladen möchten.
Der Block **Tenant settings** wird angezeigt.
4. Klicken Sie auf den Namen der Archivdatei, um das Archiv herunterzuladen.

So laden Sie die MDR-Konfigurationsdatei in der Kaspersky Security Center-Konsole herunter:

1. Klicken Sie im MDR-Abschnitt der Kaspersky Security Center Web Console oder in Kaspersky Next Expert View auf **Lizenzierung**.
2. Suchen Sie die Spalte **Archiv für die Asset-Konfiguration** und klicken Sie auf **Herunterladen**, um das Archiv herunterzuladen.

Schritt 2. KPSN-Konfigurationsdatei bereitstellen

Sie können die KPSN-Konfigurationsdatei in der Kaspersky Security Center Web Console bereitstellen. Wenn Sie das [MDR-Plug-in](#) installiert haben, können Sie die KPSN-Konfigurationsdatei auch im Menü des MDR-Plug-ins bereitstellen.

Entpacken Sie die MDR-Konfigurationsdatei und installieren Sie die KPSN-Konfigurationsdatei (.pkcs7).

So installieren Sie die KPSN-Konfigurationsdatei in der Kaspersky Security Center Web Console:

1. Wechseln Sie zu den Eigenschaften des Administrationsservers, indem Sie im Hauptmenü auf seinen Namen klicken.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** aus.
3. Aktivieren Sie den Parameter **KSN-Proxy auf dem Administrationsserver aktivieren**.
4. Aktivieren Sie den Parameter **Kaspersky Private Security Network verwenden**.
5. Klicken Sie auf **Datei mit KSN Proxy-Einstellungen wählen** und laden Sie die KPSN-Konfigurationsdatei (.pkcs7) hoch.
Die Details der KPSN-Konfigurationsdatei werden angezeigt.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die KPSN-Konfigurationsdatei wurde installiert.

So installieren Sie die KPSN-Konfigurationsdatei im Menü des MDR-Plug-ins von Kaspersky Security Center Web Console oder Open Single Management Platform:

1. Öffnen Sie im Hauptmenü den Abschnitt **MDR**.
2. Öffnen Sie die Registerkarte **MDR-Nutzung**.

3. Erweitern Sie den Block **KPSN-Konfigurationsdatei für die Integration in den KSC-Administrationsserver**.
4. Aktivieren Sie den Parameter **KPSN-Vereinbarung akzeptieren** und klicken Sie auf **KPSN-Konfigurationsdatei auf dem Administrationsserver anwenden**.

Die KPSN-Konfigurationsdatei wurde installiert.

MDR-Konfigurationsdatei (BLOB) bereitstellen

Sie können MDR-Konfigurationsdateien (BLOB) verwenden, um die MDR-Lösung in Anwendungen zu aktivieren, die die Integration in MDR über Kaspersky Security Center-Richtlinien unterstützen.

Wenn Sie andere Mandanten als den Root-Mandanten verwenden, müssen Sie die MDR-Konfigurationsdateien für jeden Mandanten herunterladen.

Für ältere Anwendungsversionen müssen MDR-Konfigurationsdateien (BLOB) verwendet werden:

- Kaspersky Endpoint Security für Windows 12.6 und älter
- Kaspersky Endpoint Security für Linux, Version 12.2 oder älter
- Kaspersky Endpoint Security for Mac, Version 12.1 und älter
- Kaspersky Security for Virtualization Light Agent, Version 5.2
- Kaspersky Security für Windows Server mit Kaspersky Endpoint Agent für Windows

Die Aktivierung der MDR-Lösung über die MDR-Konfigurationsdatei (BLOB) erfolgt in zwei Schritten.

Schritt 1. Download der MDR-Konfigurationsdatei

Das Vorgehen für den Download der MDR-Konfigurationsdatei hängt davon ab, ob Sie zusätzliche Mandanten erstellt und das MDR-Plug-in für Kaspersky Security Center installiert haben.

Die MDR-Konfigurationsdatei ist ein ZIP-Archiv, das eine BLOB-Datei (P7) zur Bereitstellung von EPP-Anwendungen enthält.

So laden Sie die MDR-Konfigurationsdatei in der MDR Web Console herunter:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Settings**.
2. Klicken Sie auf die Registerkarte **Tenants**.
3. Klicken Sie auf die Zeile mit dem Mandanten, für den Sie die MDR-Konfigurationsdatei herunterladen möchten.
Der Block **Tenant settings** wird angezeigt.
4. Klicken Sie auf den Namen der Archivdatei, um das Archiv herunterzuladen.

So laden Sie die MDR-Konfigurationsdatei in der Kaspersky Security Center-Konsole herunter:

1. Klicken Sie im MDR-Abschnitt der Kaspersky Security Center Web Console oder in Kaspersky Next Expert View auf **Lizenzierung**.
2. Suchen Sie die Spalte **Archiv für die Asset-Konfiguration** und klicken Sie auf **Herunterladen**, um das Archiv herunterzuladen.

Schritt 2. MDR-Konfigurationsdatei (BLOB) zu den Anwendungsrichtlinien hinzufügen

Entpacken Sie die MDR-Konfigurationsdatei und verwenden Sie die BLOB-Datei (P7), um die MDR-Lösung zu aktivieren.

So aktivieren Sie die MDR-Lösung in den folgenden Anwendungen:

- Kaspersky Endpoint Security für Windows
 - Kaspersky Endpoint Security für Linux
 - Kaspersky Endpoint Security for Mac
1. Gehen Sie in Kaspersky Security Center Web Console oder Open Single Management Platform zum Abschnitt **Asset-Management** → **Richtlinien und Profile**.
 2. Wählen Sie die Anwendungsrichtlinie aus. Wenn noch keine Anwendungsrichtlinie erstellt wurde, klicken Sie auf **Hinzufügen** und erstellen Sie die Richtlinie.
 3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
 4. Gehen Sie zu **Integrierte Agenten** → **Managed Detection and Response**.
 5. Aktivieren Sie den Parameter „Managed Detection and Response“.
 6. Klicken Sie auf **Hochladen** und wählen Sie die BLOB-Datei (P7) aus, die Sie aus der MDR-Konfigurationsdatei extrahiert haben.
 7. Schließen Sie das Schloss-Symbol (🔒), um die Einstellungen durchzusetzen.
 8. Klicken Sie auf **Speichern und schließen**.

Die MDR-Konfigurationsdatei (BLOB) wird hochgeladen und automatisch für Anwendungen bereitgestellt.

So aktivieren Sie die MDR-Lösung in Kaspersky Industrial CyberSecurity for Nodes Windows:

1. Gehen Sie in Kaspersky Security Center Web Console oder Open Single Management Platform zum Abschnitt **Asset-Management** → **Richtlinien und Profile**.
2. Wählen Sie die Richtlinie für Kaspersky Industrial CyberSecurity for Nodes Windows aus. Wenn noch keine Anwendungsrichtlinie erstellt wurde, klicken Sie auf **Hinzufügen** und erstellen Sie die Richtlinie.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zu **Telemetrie-Verbindungsserver**.
5. Klicken Sie im Abschnitt **Managed Detection and Response** auf **Konfigurieren**.
6. Aktivieren Sie den Parameter **Managed Detection and Response**.
7. Klicken Sie auf **Hochladen** und wählen Sie die BLOB-Datei (P7) aus, die Sie aus der MDR-Konfigurationsdatei extrahiert haben.
8. Klicken Sie auf **Speichern und schließen**.

Die MDR-Konfigurationsdatei (BLOB) wird hochgeladen und automatisch für Anwendungen bereitgestellt.

Bereitstellung durch Erfassen und Kopieren des Geräte-Images

Wenn Sie Anwendungen auf Assets installieren möchten, auf denen auch das Betriebssystem und sonstige Anwendungen installiert (oder neu installiert) werden müssen, können Sie das Image eines Referenz-Assets erfassen und kopieren.

Die Bereitstellung durch das Erfassen und Kopieren des Images eines Geräts erfolgt in zwei Schritten:

1. Bereiten Sie ein Referenz-Asset vor, auf dem die erforderliche Software installiert ist.
2. Erfassen Sie das Image des vorbereiteten Referenz-Assets und verteilen Sie es mithilfe der dafür vorgesehenen Kaspersky Security Center-Aufgabe an die Assets.

Wenn Ihre Lizenz für Kaspersky Security Center die Systemverwaltungsfunktion umfasst, können Sie [die Funktionalität von Kaspersky Security Center verwenden, um das Image zu erfassen und an die Assets zu verteilen](#)^[2]. Verwenden Sie andernfalls Drittanbieter-Tools, die in Ihrem Unternehmen verfügbar sind.

Referenz-Asset vorbereiten

So bereiten Sie ein Windows-basiertes Referenz-Asset vor:

1. Installieren und konfigurieren Sie das Betriebssystem und sonstige Anwendungen, die Sie verteilen möchten.
2. Gehen Sie auf dem Referenz-Asset zu den Windows-Einstellungen für Netzwerkverbindungen und trennen Sie die Verbindung des Referenz-Assets mit dem Netzwerk, in dem Kaspersky Security Center installiert ist.
3. Starten Sie auf dem Referenz-Asset die lokale Installation des Administrationsagenten. Führen Sie dazu die Datei setup.exe aus.
Der Installationsassistent für Kaspersky Security Center Administrationsagent wird gestartet. Folgen Sie den Anweisungen des Assistenten.
4. Geben Sie im Assistenten auf der Seite „Administrationsserver“ die IP-Adresse des Administrationsservers an.
Wenn Sie die genaue Adresse des Administrationsservers nicht kennen, geben Sie localhost ein. Sie können die IP-Adresse später ändern, indem Sie das [Dienstprogramm klmover](#)^[2] mit dem Schlüssel -address verwenden.

5. Deaktivieren Sie im Assistenten auf der Seite „Anwendung starten“ die Option „Anwendung im Installationsvorgang starten“.

6. Starten Sie das Asset nach Abschluss der Installation des Administrationsagenten nicht neu, bevor Sie ein Betriebssystem-Image erstellt haben.

Wenn Sie das Asset neu starten, müssen Sie die gesamte Vorbereitung eines Referenz-Assets zum Erstellen eines Betriebssystem-Images wiederholen.

7. Starten Sie auf dem Referenz-Asset in der Befehlszeile das Dienstprogramm sysprep und führen Sie den folgenden Befehl aus: `sysprep.exe /generalize /oobe /shutdown`.

Das Referenz-Asset ist bereit zum Erstellen eines Betriebssystem-Images.

So bereiten Sie ein Linux-basiertes Referenz-Asset vor:

1. Installieren und konfigurieren Sie das Betriebssystem und sonstige Anwendungen, die Sie verteilen möchten.

2. Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

- Kaspersky Endpoint Security für Linux ist nicht auf dem Referenz-Asset installiert.
- Das Referenz-Gerät wurde nicht mit Kaspersky Security Center verbunden.

Wenn eine dieser Bedingungen verletzt wird, kann die MDR-Lösung jene Assets, die durch die Verteilung eines Referenz-Asset-Images erstellt wurden, möglicherweise nicht richtig identifizieren. Um dieses Problem zu beheben, führen Sie für Assets, auf denen Kaspersky Endpoint Security für Linux installiert ist, die folgenden Schritte aus:

a. Führen Sie die folgenden Befehle aus, um eine neue UUID zu generieren:

```
uuidgen > /var/opt/kaspersky/kes1/common/pcid
```

```
uuidgen > /var/opt/kaspersky/epagent/install_id
```

b. Deinstallieren Sie Kaspersky Endpoint Security für Linux und installieren Sie es erneut.

Das Referenz-Asset ist bereit zum Erstellen eines Betriebssystem-Images.

Image eines Referenz-Assets erfassen und verteilen

Wenn Sie Drittanbieter-Tools verwenden, um das Image eines Assets mit installiertem Administrationsagenten zu erstellen, gibt es folgende Methoden:

- **Empfohlene Methode.** Wenn Sie den Administrationsagenten auf einem Referenz-Asset installieren, müssen Sie das Image des Assets vor dem ersten Start des Administrationsagenten-Dienstes erfassen (Dies ist erforderlich, da bei der ersten Verbindung des Administrationsagenten mit dem Administrationsserver eindeutige Informationen zur Asset-Identifizierung erstellt werden). Es wird empfohlen, den Administrationsagenten-Dienst danach erst wieder auszuführen, nachdem die Image-Erfassung abgeschlossen wurde.

Informationen zu Windows finden Sie im folgenden Artikel: [Vorbereitung eines Referenz-Assets mit installiertem Administrationsagenten zum Erfassen eines Betriebssystem-Images](#).

Informationen zu Linux finden Sie im folgenden Artikel: [Bereitstellung durch Erfassen und Kopieren des Asset-Images](#).

- Beenden Sie den Administrationsagenten auf dem Referenz-Asset und führen Sie das Dienstprogramm klmover mit dem Schlüssel -dupfix aus. Das Dienstprogramm klmover ist im Installationspaket des Administrationsagenten enthalten. Führen Sie den Administrationsagenten-Dienst nicht mehr aus, bis die Image-Erfassung abgeschlossen ist.

Stellen Sie sicher, dass das Tool "klmover" vor dem ersten Start des Dienstes des Administrationsagenten auf den Zielgeräten mit dem Schlüssel -dupfix ausgeführt wird. Dies ist eine zwingende Voraussetzung und muss beim ersten Start des Betriebssystems nach der Bereitstellung des Images durchgeführt werden.

- Verwenden Sie den Modus zum Klonen des Administrationsagenten-Datenträgers.

Informationen zu Windows finden Sie im folgenden Artikel: [Modus zum Klonen des Administrationsagenten-Datenträgers](#).

Informationen zu Linux finden Sie im folgenden Artikel: [Modus zum Klonen des Administrationsagenten-Datenträgers](#).

Sie können auch das Image eines Assets ohne installierten Administrationsagenten erfassen. Stellen Sie dazu auf den Ziel-Assets zuerst das Image und anschließend den Administrationsagenten bereit. Wenn Sie diese Methode verwenden, gewähren Sie Zugriff auf den Netzwerkordner mit den autonomen Installationspaketen aus dem Asset. Folgen Sie den Anweisungen:

- Informationen zu Windows finden Sie im folgenden Artikel: [Installation von Betriebssystem-Images](#).
- Informationen zu Linux finden Sie im folgenden Artikel: [Über Aufgaben zur Remote-Installation in Kaspersky Security Center Linux](#).

MDR-Lösung in Kaspersky-Anwendungen aktivieren

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Dieser Abschnitt enthält Referenzinformationen darüber, wie Sie die MDR-Lösung abhängig von Lizenz und Anwendungsversion aktivieren. Eine vollständige Anleitung zur Aktivierung der MDR-Lösung finden Sie im folgenden Artikel: [Kaspersky Managed Detection and Response aktivieren und bereitstellen](#).

In den folgenden Artikeln wird beschrieben, wie Sie Lizenzschlüssel und AktivierungsCodes auf dem Administrationsserver verwalten:

- [Automatische Verteilung von Lizenzschlüsseln und AktivierungsCodes](#)
- [Anzeigen von Informationen zu verwendeten Lizenzschlüsseln und AktivierungsCodes](#)

MDR-Lizenz	Unterstützte Anwendungen für die folgenden Methoden: Aktivierungscode BLOB-Datei	Unterstützte Anwendungen für die folgenden Methoden: BLOB-Datei
Kaspersky Symphony MDR Kaspersky Next Complete Security Kaspersky Optimum Security Kaspersky Next MXDR Optimum Siehe: Lizenzen für Kaspersky Symphony MDR und Kaspersky Next Complete Security	• Kaspersky Endpoint Security für Windows Version 12.6 oder höher • Kaspersky Endpoint Security für Windows, Version 12.8 oder höher im Light Agent-Modus • Kaspersky Endpoint Security für Windows Version 12.6 oder höher im Endpoint Detection and Response Agent-Modus • Kaspersky Endpoint Security für Linux Version 12.3 oder höher • Kaspersky Endpoint Security für Linux Version 12.3 oder höher im Light Agent-Modus • Kaspersky Endpoint Security for Mac Version 12.2 oder höher Die BLOB-Datei muss installiert werden, wenn Ihr Unternehmen über mehrere Mandanten verfügt. Die Aktivierung mit einer Schlüsseldatei wird nur eingeschränkt unterstützt. Es wird empfohlen, einen Aktivierungscode zu verwenden.	• Kaspersky Endpoint Security für Windows, Version 12.5 und älter • Kaspersky Endpoint Security für Windows, Version 5.2–6.1 im Light Agent-Modus • Kaspersky Endpoint Security für Windows, Version 12.3–12.5 im Endpoint Detection and Response Agent-Modus • Kaspersky Endpoint Security für Linux, Version 12.2 oder älter • Kaspersky Endpoint Security für Linux, Version 12.2 oder älter im Light Agent-Modus • Kaspersky Endpoint Security for Mac, Version 12.1 und älter Kaspersky Anti Targeted Attack Platform (einschließlich EDR) Version 4.0–7.1 unterstützt die Installation der MDR-Konfigurationsdatei, die die BLOB-Datei und die KPSN-Konfigurationsdatei enthält. Für Kaspersky Anti Targeted Attack Platform (einschließlich EDR) Version 8.0 ist die MDR-Konfigurationsdatei nicht erforderlich.
Kaspersky MDR Kaspersky Managed Detection and Response Siehe: Lizenzen für Kaspersky MDR	• Kaspersky Endpoint Security für Windows Version 12.6 oder höher • Kaspersky Endpoint Security für Windows, Version 12.8 oder höher im Light Agent-Modus • Kaspersky Endpoint Security für Windows Version 12.6 oder höher im Endpoint Detection and Response Agent-Modus • Kaspersky Endpoint Security für Linux Version 12.3 oder höher • Kaspersky Endpoint Security für Linux Version 12.3 oder höher im Light Agent-Modus • Kaspersky Endpoint Security for Mac Version 12.2 oder höher • Kaspersky Embedded Systems Security für Windows Version 4.0 oder höher • Kaspersky Embedded Systems Security für Linux Version 4.0 oder höher Die BLOB-Datei muss installiert werden, wenn Ihr Unternehmen über mehrere Mandanten verfügt. Die Aktivierung mit einer Schlüsseldatei wird nur eingeschränkt unterstützt. Es wird empfohlen, einen Aktivierungscode zu verwenden.	• Kaspersky Endpoint Security für Windows, Version 12.5 und älter • Kaspersky Endpoint Security für Windows, Version 5.2–6.1 im Light Agent-Modus • Kaspersky Endpoint Security für Windows, Version 12.3–12.5 im Endpoint Detection and Response Agent-Modus • Kaspersky Endpoint Security für Linux, Version 12.2 oder älter • Kaspersky Endpoint Security für Linux, Version 12.2 oder älter im Light Agent-Modus • Kaspersky Endpoint Security for Mac, Version 12.1 und älter Kaspersky Anti Targeted Attack Platform (einschließlich EDR) Version 4.0–7.1 unterstützt die Installation der MDR-Konfigurationsdatei, die die BLOB-Datei und die KPSN-Konfigurationsdatei enthält.
Kaspersky MDR Optimum Add-on Kaspersky MDR Expert Add-on Kaspersky Managed Detection and Response Basic Add-on Kaspersky Managed Detection and Response Advanced Add-on Kaspersky Managed Detection and Response Prime Add-on Siehe: Add-on-Lizenzen für Kaspersky MDR	• Kaspersky Endpoint Security für Windows Version 12.6 oder höher • Kaspersky Endpoint Security für Windows, Version 12.8 oder höher im Light Agent-Modus • Kaspersky Endpoint Security für Windows Version 12.6 oder höher im Endpoint Detection and Response Agent-Modus Die BLOB-Datei muss installiert werden, wenn Ihr Unternehmen über mehrere Mandanten verfügt. Die Aktivierung mit einer Schlüsseldatei wird nur eingeschränkt unterstützt. Es wird empfohlen, einen Aktivierungscode zu verwenden.	• Kaspersky Endpoint Security für Windows, Version 12.5 und älter • Kaspersky Endpoint Security für Windows, Version 5.2–6.1 im Light Agent-Modus • Kaspersky Endpoint Security für Windows, Version 12.3–12.5 im Endpoint Detection and Response Agent-Modus Kaspersky Anti Targeted Attack Platform (einschließlich EDR) Version 4.0–7.1 unterstützt die Installation der MDR-Konfigurationsdatei, die die BLOB-Datei und die KPSN-Konfigurationsdatei enthält.
Kaspersky Managed Detection And	Kaspersky Industrial CyberSecurity for	Die BLOB-Datei muss installiert werden, wenn Ihr

MDR-Lizenz	Unterstützte Anwendungen für die folgenden Methoden: Aktivierungscode BLOB-Datei	Unterstützte Anwendungen für die folgenden Methoden: BLOB-Datei
Response for Industrial CyberSecurity Siehe: Add-on-Lizenz für Kaspersky MDR for Industrial CyberSecurity	Nodes Windows, Version 4.5 oder höher. Die BLOB-Datei muss installiert werden, wenn Ihr Unternehmen über mehrere Mandanten verfügt.	Unternehmen über mehrere Mandanten verfügt. In diesem Szenario ist nach wie vor eine Schlüsseldatei oder ein Aktivierungscode erforderlich.

MDR-Lösung in Kaspersky-Anwendungen aktivieren. Lizenzen von Kaspersky MDR Add-ons

Die folgenden Tabellen beschreiben die Methoden zur Aktivierung der MDR-Lösung in Kaspersky-Anwendungen für die folgenden Lizenzen:

- Kaspersky MDR Expert Add-on
- Kaspersky MDR Optimum Add-on
- 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 für Windows

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.10 oder höher	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: • Sie verwenden derzeit MDR-Mandanten. • Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde. Um sowohl die Lösung "Endpoint Detection and Response Optimum" als auch die MDR-Lösung zu aktivieren, wenden Sie den Aktivierungscode für Endpoint Detection and Response Optimum und eine MDR-Konfigurationsdatei (BLOB) für die MDR-Lösung an.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: 1. Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. 2. Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.9	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde. Um sowohl die Lösung "Endpoint Detection and Response Optimum" als auch die MDR-Lösung zu aktivieren, wenden Sie den Aktivierungscode für Endpoint Detection and Response Optimum und eine MDR-Konfigurationsdatei (BLOB) für die MDR-Lösung an.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.6–12.8	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde. Um sowohl die Lösung "Endpoint Detection and Response Optimum" als auch die MDR-Lösung zu aktivieren, wenden Sie den Aktivierungscode für Endpoint Detection and Response Optimum und eine MDR-Konfigurationsdatei (BLOB) für die MDR-Lösung an.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.5 und niedriger	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Endpoint Security für Windows im Modus als Endpoint Detection and Response Agent

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.10 oder höher	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde. Um sowohl die Lösung "Endpoint Detection and Response Optimum" als auch die MDR-Lösung zu aktivieren, wenden Sie den Aktivierungscode für Endpoint Detection and Response Optimum und eine MDR-Konfigurationsdatei (BLOB) für die MDR-Lösung an.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.9	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben.
12.6–12.8	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben.
12.3–12.5	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Security for Virtualization Light Agent

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
6.3 oder höher Kaspersky Endpoint Security für Windows 12.10 oder höher im Light Agent-Modus	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde. Um sowohl die Lösung "Endpoint Detection and Response Optimum" als auch die MDR-Lösung zu aktivieren, wenden Sie den Aktivierungscode für Endpoint Detection and Response Optimum und eine MDR-Konfigurationsdatei (BLOB) für die MDR-Lösung an.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
6.2 Kaspersky Endpoint Security für Windows 12.8–12.9 im Light Agent-Modus	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscode installiert wurde. Um sowohl die Lösung "Endpoint Detection and Response Optimum" als auch die MDR-Lösung zu aktivieren, wenden Sie den Aktivierungscode für Endpoint Detection and Response Optimum und eine MDR-Konfigurationsdatei (BLOB) für die MDR-Lösung an.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
6.0–6.1 Kaspersky Security for Virtualization Light Agent	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.
5.2 Kaspersky Security for Virtualization Light Agent	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.
6.3 oder höher Kaspersky Endpoint Security für Linux 12.3 oder höher im Light Agent-Modus	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
6.2 Kaspersky Endpoint Security für Linux 12.2 im Light Agent-Modus	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

MDR-Lösung in Kaspersky-Anwendungen aktivieren. Lizenzen von Kaspersky MDR

Die folgenden Tabellen beschreiben die Methoden zur Aktivierung der MDR-Lösung in Kaspersky-Anwendungen für die folgenden Lizenzen:

- Kaspersky MDR
- Kaspersky Managed Detection and Response

Kaspersky Endpoint Security für Windows

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.10 oder höher	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.9	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.6–12.8	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde. Um sowohl die Lösung "Endpoint Detection and Response Optimum" als auch die MDR-Lösung zu aktivieren, wenden Sie den Aktivierungscode für Endpoint Detection and Response Optimum und eine MDR-Konfigurationsdatei (BLOB) für die MDR-Lösung an.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.5 und niedriger	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Endpoint Security für Windows im Modus als Endpoint Detection and Response Agent

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.10 oder höher	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.9	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben.
12.6–12.8	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben.
12.3–12.5	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Security for Virtualization Light Agent

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
6.3 oder höher Kaspersky Endpoint Security für Windows 12.10 oder höher im Light Agent-Modus	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
6.2 Kaspersky Endpoint Security für Windows 12.8–12.9 im Light Agent-Modus	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde. Um sowohl die Lösung "Endpoint Detection and Response Optimum" als auch die MDR-Lösung zu aktivieren, wenden Sie den Aktivierungscode für Endpoint Detection and Response Optimum und eine MDR-Konfigurationsdatei (BLOB) für die MDR-Lösung an.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
6.0–6.1 Kaspersky Security for Virtualization Light Agent	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.
5.2 Kaspersky Security for Virtualization Light Agent	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.
6.3 oder höher Kaspersky Endpoint Security für Linux 12.3 oder höher im Light Agent-Modus	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
6.2 Kaspersky Endpoint Security für Linux 12.2 im Light Agent-Modus	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Endpoint Security für Linux

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.3 oder höher	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.2 und niedriger	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Endpoint Security for Mac

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.2 oder höher	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Eine abgelaufene MDR-Konfiguration (BLOB) muss durch eine neue ersetzt werden.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.1 und niedriger	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Embedded Systems Security for Windows

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
4.0	Anwendung eines Aktivierungscodes oder einer Schlüsseldatei, um die MDR-Lösung zu aktivieren. Es ist nicht erforderlich, eine MDR-Konfigurationsdatei (BLOB) zu verwenden. Alle Assets sind standardmäßig dem Root-Mandanten zugewiesen.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei.

Kaspersky Embedded Systems Security für Linux

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
4.0	Anwendung eines Aktivierungscodes oder einer Schlüsseldatei, um die MDR-Lösung zu aktivieren. Es ist nicht erforderlich, eine MDR-Konfigurationsdatei (BLOB) zu verwenden. Alle Assets sind standardmäßig dem Root-Mandanten zugewiesen.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei.

MDR-Lösung in Kaspersky-Anwendungen aktivieren. Lizenzen für Kaspersky Symphony MDR, Kaspersky Next Complete Security, Kaspersky Optimum Security und Kaspersky Next MXDR Optimum

Die folgenden Tabellen beschreiben die Methoden zur Aktivierung der MDR-Lösung in Kaspersky-Anwendungen für die folgenden Lizenzen:

- Kaspersky Symphony MDR
- Kaspersky Next Complete Security
- Kaspersky Optimum Security
- Kaspersky Next MXDR Optimum

Kaspersky Endpoint Security für Windows

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.10 oder höher	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: • Sie verwenden derzeit MDR-Mandanten. • Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: 1. Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. 2. Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.9	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscode installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.6–12.8	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscode installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.5 und niedriger	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Security for Virtualization Light Agent

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
6.0–6.1 Kaspersky Security for Virtualization Light Agent	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.
5.2 Kaspersky Security for Virtualization Light Agent	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.
6.3 oder höher Kaspersky Endpoint Security für Windows 12.10 oder höher im Light Agent-Modus	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscode installiert wurde. Light Agent kann unter der Lizenz von NEXT Complete Security nicht aktiviert werden.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
6.2 Kaspersky Endpoint Security für Windows 12.8–12.9 im Light Agent-Modus	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde. Light Agent kann unter der Lizenz von NEXT Complete Security nicht aktiviert werden.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
6.3 oder höher Kaspersky Endpoint Security für Linux 12.3 oder höher im Light Agent-Modus	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
6.2 Kaspersky Endpoint Security für Linux 12.2 im Light Agent-Modus	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Endpoint Security für Linux

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.3 oder höher	In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode oder eine Schlüsseldatei anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscodes installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.2 und niedriger	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

Kaspersky Endpoint Security for Mac

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
12.2 oder höher	Das Aktivieren der MDR-Lösung mit einer Schlüsseldatei wird nicht unterstützt. In den folgenden Fällen müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, bevor Sie einen Aktivierungscode anwenden können: - Sie verwenden derzeit MDR-Mandanten. - Sie haben bereits MDR-Mandanten erstellt, selbst wenn weitere Mandanten gelöscht wurden. Es ist nicht erforderlich, eine abgelaufene MDR-Konfiguration (BLOB) zu ändern, die vor dem Anwenden eines Aktivierungscode installiert wurde.	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Um die MDR-Lösung ohne KPSN-Konfigurationsdatei zu verwenden, geben Sie den Aktivierungscode an, auch wenn Sie eine MDR-Konfigurationsdatei (BLOB) bereitgestellt haben. Wenn auf Ihren Assets bereits MDR-Konfigurationsdateien (BLOB) installiert sind und die MDR-Lösung vor Januar 2024 aktiviert wurde, müssen Sie die BLOB-Dateien erneut herunterladen und installieren: - Laden Sie die MDR-Konfigurationsdatei (BLOB) für den erforderlichen Mandanten in der MDR Web Console herunter. - Konfigurieren Sie die Richtlinie, um die BLOB-Datei auf Ihren Assets zu installieren.
12.1 und niedriger	Die MDR-Lösung kann mit einer MDR-Konfigurationsdatei (BLOB) aktiviert werden.	Die MDR-Lösung funktioniert nur, wenn die KPSN-Konfigurationsdatei in Kaspersky Security Center installiert ist.

MDR-Lösung in Kaspersky-Anwendungen aktivieren. Add-on-Lizenz für Kaspersky Managed Detection and Response for Industrial CyberSecurity

Die folgende Tabelle beschreibt die Methoden zur Aktivierung der MDR-Lösung in Kaspersky-Anwendungen für die Add-on-Lizenz von Kaspersky Managed Detection and Response for Industrial CyberSecurity.

Kaspersky Industrial CyberSecurity for Nodes Windows

Anwendungsversion	Aktivierungsmethode	Anforderungen an die KPSN-Konfigurationsdatei
4.5	Anwendung eines Aktivierungscode oder einer Schlüsseldatei, um die MDR-Lösung zu aktivieren: - Wenn Sie MDR-Mandanten weder verwenden noch erstellen, ist die Verwendung einer MDR-Konfigurationsdatei (BLOB) nicht erforderlich. Wenn Sie MDR-Mandanten verwenden, müssen Sie eine MDR-Konfigurationsdatei (BLOB) installieren, auch wenn diese abgelaufen ist. Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei. Verwenden Sie das MDR-Plug-in Version 3.0.0 oder höher, um mehrere Aktivierungscode für die Lizenz von Kaspersky Industrial CyberSecurity for Nodes anzuwenden. Wenn Sie nur einen Aktivierungscode für die Lizenz von Kaspersky Industrial CyberSecurity for Nodes besitzen, können Sie die MDR Web Console verwenden. Das Anwenden neuer Aktivierungscode für Kaspersky Industrial CyberSecurity for Nodes ist in der Region "Königreich Saudi-Arabien" nicht möglich, wenn Sie eine der folgenden Lizenzen besitzen: - Kaspersky Managed Detection and Response Basic Add-on - Kaspersky Managed Detection and Response Advanced Add-on - Kaspersky Managed Detection and Response Prime Add-on	Die Anwendung unterstützt die Verwendung von MDR mit und ohne KPSN-Konfigurationsdatei.

Lizenzierung

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für das Programm, welches Ihnen auf Basis der Nutzungsbedingungen überlassen wird.

Die MDR Web Console und das MDR-Plug-in können bis einschließlich Version 2.4.1 nur unter einer Lizenz verwendet werden. Wenn Sie einen neuen Aktivierungscode eingeben, ersetzt dieser den bisherigen.

Ab Version 2.4.2 des MDR-Plug-ins können Sie [mehrere MDR-Lizenzen gleichzeitig verwenden](#).

Eine Lizenz gewährt Ihnen folgende Arten von Dienstleistungen:

- Nutzung des Programms gemäß den Nutzungsbedingungen
- Erhalten von Technischem Support

Der Umfang und die Gültigkeitsdauer der Dienste hängen von dem Typ der Lizenz ab, unter der das Programm aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen:

- *Test* – Eine kostenlose Lizenz zum Ausprobieren des Programms.

Eine Testlizenz verfügt in der Regel über eine kurze Gültigkeitsdauer. Nach Ablauf der Testlizenz werden alle Funktionen von Kaspersky Managed Detection and Response deaktiviert. Um das Programm weiterhin verwenden zu können, müssen Sie eine kommerzielle Lizenz erwerben.

Das Programm kann nur ein einziges Mal mit einer Testlizenz aktiviert werden.

- *Kommerziell* – Eine kostenpflichtige Lizenz, die beim Kauf des Programms gewährt wird.

Nach Ablauf der kommerziellen Lizenz arbeitet das Programm mit einem eingeschränkten Funktionsumfang weiter (es werden keine Telemetriedaten bereitgestellt). Um weiterhin alle Funktionen von Kaspersky Managed Detection and Response nutzen zu können, müssen Sie Ihre kommerzielle Lizenz erneuern.

Um maximalen Schutz vor allen Sicherheitsbedrohungen zu gewährleisten, wird es empfohlen, die Lizenz vor ihrem Ablauf zu erneuern.

- *Abonnement* – Eine kostenpflichtige Lizenz, welche die Nutzung des Programms für einen monatlichen oder jährlichen Abrechnungszeitraum ermöglicht. Sie bietet eine automatische Verlängerung, bis sie gekündigt wird oder abgelaufen ist.

Es gibt zwei Arten von Abonnement-Lizenzen:

- *Befristet* – Wird solange am Ende jedes Abrechnungszeitraums automatisch verlängert, bis das festgelegte Ablaufdatum erreicht wird.
- *Unbefristet* – wird solange am Ende jedes Abrechnungszeitraums automatisch verlängert, bis es vom Kunden storniert wird.

Sie können die Abonnement-Lizenz über das Kaspersky License Management Portal (LMP) verwalten.

Wenn Sie den Gültigkeitsbereich Ihrer Lizenz ändern (indem Sie beispielsweise die Anzahl der Assets ändern) werden die Lizenzdetails innerhalb von 24 Stunden in der MDR Web Console aktualisiert.

Wenn die Abonnementlizenz gekündigt oder abgelaufen ist, arbeitet das Programm mit einem eingeschränkten Funktionsumfang weiter (es werden keine Telemetriedaten bereitgestellt). Um weiterhin alle Funktionen von Kaspersky Managed Detection and Response nutzen zu können, müssen Sie Ihre Abonnement-Lizenz verlängern.

Um maximalen Schutz vor allen Sicherheitsbedrohungen zu gewährleisten, wird es empfohlen, die Lizenz vor ihrem Ablauf zu erneuern.

Vergleich der kommerziellen Lizenzstufen

Welche Funktionen in Kaspersky Managed Detection and Response verfügbar sind, hängt von der Stufe Ihrer kommerziellen Lizenz ab (siehe Tabelle unten).

Vergleich der kommerziellen Lizenzstufen von Kaspersky Managed Detection and Response

Funktion	MDR / MDR Expert*	MDR Optimum* /MDR Basic*	MDR Advanced*	MDR Prime*
Überwachung, Vorfallerkennung und Vorfalldmanagement rund um die Uhr	✓	✓	✓	✓
Automatische Bedrohungssuche	✓	✓	✓	✓
Reaktions-Leitlinien und automatische Reaktion auf Vorfälle	✓	✓	✓	✓
Überprüfung von Asset-Status und Sichtbarkeit	✓	✓	✓	✓
MDR Web Console mit Dashboards und Berichten	✓	✓	✓	✓
Möglichkeit, erweiterte Informationen zu Vorfällen zu erhalten	✓	✓	✓	✓
Aufbewahrungsdauer des Ereignisverlaufs	1 Jahr	1 Jahr	1 Jahr	1 Jahr
Aufbewahrungsdauer für Rohdaten	3 Monate	1 Monat	3 Monate	3 Monate
Verwaltete Bedrohungssuche und Untersuchung von Ereignissen	✓	—	✓	✓
Erweiterter Expertensupport für das Vorfalldmanagement	✓	—	✓	✓
Zugriff auf das Kaspersky Threat Intelligence Portal (für Lizenzen mit Startdatum vor 12. Juli 2024)	✓	—	✓	✓
API für den Export von Kaspersky MDR-Daten	✓	—	✓	✓
Der Kunde kann einen benutzerdefinierten Vorfall für die Verarbeitung durch die Kaspersky MDR-Lösung erstellen**	✓	—	✓	✓
Lokalisierte Datenspeicherung*	✓	✓	✓	✓
Mehrmandantenfähigkeit	✓	✓	✓	✓
Hinzufügen und Bearbeiten von Kommentaren zu Vorfällen	✓	✓	✓	✓

Funktion	MDR / MDR Expert*	MDR Optimum* /MDR Basic*	MDR Advanced*	MDR Prime*
Hinzufügen und Bearbeiten von Anhängen für Vorfälle	✓	✓	✓	✓
Erweiterte Untersuchung von Vorfällen: Analyse zum Ermitteln von Hintergrund, Umständen und detaillierten Angriffsmechanismen	—	—	✓ Der Kunde kann die Vorfälle nicht für die erweiterte Untersuchung auswählen und es gibt keine garantierte Reaktionszeit für Vorfälle	✓ Der Kunde kann die Vorfälle für die erweiterte Untersuchung auswählen (innerhalb des erkauften Zeitfensters) und es gibt eine garantierte Reaktionszeit für Vorfälle

*Diese Stufe oder Funktion ist nur für bestimmte Regionen verfügbar und kann von Neukunden möglicherweise nicht erworben werden. Weitere Informationen zu den verfügbaren Stufen der kommerziellen Lizenz erhalten Sie von Ihrem Lösungsanbieter für Kaspersky Managed Detection and Response.

**Die Kaspersky Managed Detection and Response Lösung gewährleistet die Verarbeitung von drei Anfragen pro Woche gemäß den [Leistungszielen der Bereitstellung der Lösung](#). Die Anzahl der zu bearbeitenden Anfragen gemäß den Leistungszielen der Bereitstellung der Lösung wird proportional erhöht: pro 10.000 angeschlossenen Endpunkten wird die Anzahl der Anfragen um 1 erhöht.

Über den Aktivierungscode

Ein *Aktivierungscode* ist eine einmalige Folge aus 20 Buchstaben und Zahlen. Sie müssen einen Aktivierungscode eingeben, um [Kaspersky Managed Detection and Response zu aktivieren](#). Der Aktivierungscode wird Ihnen an die E-Mail-Adresse zugesandt, die Sie beim Erwerb von Kaspersky Managed Detection and Response angegeben haben.

Um die Lösung unter Verwendung eines Aktivierungscodes zu aktivieren, ist ein Internetzugang für die Verbindung mit den Aktivierungsservern von Kaspersky erforderlich.

Wenn Sie Ihren Aktivierungscode verloren haben, wenden Sie sich bitte an den Kaspersky-Partner, von dem Sie die Lizenz erworben haben.

Einen neuen Aktivierungscode angeben

Kaspersky Managed Detection and Response erstmals aktivieren

Weiterführende Artikel:

- Kaspersky Managed Detection and Response in Kaspersky Security Center aktivieren (empfohlen)
- Kaspersky Managed Detection and Response in der MDR Web Console aktivieren

Eingeben eines neuen Aktivierungscode

Sie müssen für Kaspersky Managed Detection and Response einen neuen Aktivierungscode angeben, wenn Sie beispielsweise die Lösung aktualisieren oder Ihre ablaufende Lizenz erneuern möchten.

Diese Funktion ist nur verfügbar, wenn Sie in der [Kaspersky Security Center Web Console](#) oder in [Kaspersky Next Expert View](#) das Zugriffsrecht **Integration von Anwendungen** festgelegt haben.

Weitere Informationen über die Verwaltung mehrerer Lizenzen in Kaspersky Managed Detection and Response in Kaspersky Security Center mit MDR-Plug-in Version 2.4.2 oder höher erhalten Sie in diesem Artikel: [Lizenzen in Kaspersky Security Center verwalten](#).

Wenn Sie eine einzelne Lizenz für die MDR-Lösung verwenden, können Sie diese Lizenz in der MDR Web Console verlängern. Dies erfordert die Rolle des **MDR-Administrators**.

Wenn Ihre Organisation über mehrere aktuelle Lizenzen verfügt, können Sie diese nur in Kaspersky Security Center verwalten. Wenn Sie stattdessen die MDR Web Console zur Verlängerung der Lizenz verwenden, stellen die Assets die Übertragung von Telemetriedaten ein.

Es wird empfohlen, das MDR-Plug-in für Kaspersky Security Center zu verwenden, um einen neuen Aktivierungscode einzugeben.

So geben Sie in Kaspersky Security Center mit MDR-Plug-in einen neuen Aktivierungscode für Kaspersky Managed Detection and Response ein:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **Lizenzierung**.
2. Klicken Sie auf die Schaltfläche **Lösung aktivieren** und geben Sie den Aktivierungscode im aufgerufenen Bereich ein.
3. Wählen Sie die Mandanten aus, auf welche die Benutzer dieses Administrationsservers Zugriff bekommen sollen.

Der neue Aktivierungscode wird angewendet. Kaspersky Managed Detection and Response wird unter der bereitgestellten Lizenz ausgeführt.

So ersetzen Sie in der MDR Web Console den aktuellen Aktivierungscode mit einem neuen:

1. Klicken Sie auf die Registerkarte **Licensing**.
2. Klicken Sie auf den Link **Enter a new activation code**.
3. Geben Sie einen neuen Aktivierungscode ein und klicken Sie auf **Continue**.
4. Wählen Sie Ihre Region aus und klicken Sie auf **Confirm and activate**.

Lizenzen in Kaspersky Security Center verwalten

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Wenn Ihre Organisation über mehrere aktuelle Lizenzen verfügt, können Sie diese nur in Kaspersky Security Center verwalten.

Für die Verwaltung der Lizenzen wird die Rolle **MDR-Administrator** benötigt.

So zeigen Sie die Lizenzen an:

Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **Lizenzierung**.

Die Liste **Lizenzen in Ihrem Unternehmen** wird angezeigt. Der obere Bereich enthält die folgenden allgemeinen Informationen über die Lizenzen:

- Region
- [Stufe der kommerziellen Lizenz](#)
- Gesamtanzahl und Obergrenze der verbundenen Assets

Auf der Registerkarte **Aktuell** werden nur aktuelle Lizenzen angezeigt. Klicken Sie auf die Registerkarte **Alle**, um alle Lizenzen in Ihrer Organisation anzuzeigen.

In der Tabelle werden folgende Informationen über Lizenzen angezeigt:

Lizenzname

Lizenzname, der Informationen wie die Lizenzstufe und die Obergrenze für die Anzahl der Assets enthält.

Verbundene Assets / Limit

Die Anzahl der Assets, von denen die Lizenz verwendet wird, und die Obergrenze.

Die Asset-Obergrenze für die Lizenz wird bei Überschreitung rot hervorgehoben.

Diese Zahl beinhaltet keine Hosts mit BLOB-Konfigurationsdateien, die vor dem 1. Januar 2024 erstellt wurden. Um dieses Problem zu beheben, aktualisieren Sie die BLOB-Datei in den Mandanteneinstellungen und wenden Sie diese auf die Assets des Mandanten an. Weitere Informationen dazu finde Sie in dem Thema [Über die MDR-Konfigurationsdatei](#).

ID

Die ID der Lizenz.

Ablaufdatum

Das Ablaufdatum der Lizenz wird rot hervorgehoben, wenn die Lizenz abgelaufen ist oder innerhalb der nächsten 14 Tagen abläuft.

Status

Einer der folgenden Statuswerte:

- Aktuell
- Abgelaufen
- Abgelehnt
- Nicht verwendet
- Ersetzt

Client-Name

Standardmäßig ausgeblendet. Sie können diese Spalte im Tabellenmenü aktivieren.

So laden Sie eine csv-Datei herunter, welche die Lizenzen nach Mandanten enthält (MDR-Plug-in Version 2.4.2):

Klicken Sie auf der Registerkarte **Aktuell** auf **Mandanten in CSV-Datei exportieren**.

Die csv-Datei enthält für jede Lizenz die Verteilung der Assets nach Mandanten.

So zeigen Sie Lizenzen nach Mandanten an (MDR-Plug-in ab Version 2.5.0):

Klicken Sie auf der Registerkarte **Aktuell** auf **Lizenznutzung durch Mandanten anzeigen**.

Die Tabelle zeigt für jede Lizenz die Verteilung der Assets nach Mandanten an.

So laden Sie die [MDR-Konfigurationsdatei](#) für eine Lizenz herunter:

Wählen Sie die Spalte **Archiv für die Asset-Konfiguration** und klicken Sie auf **Download**.

So geben Sie einen neuen Aktivierungscode ein:

Klicken Sie auf die Schaltfläche **Enter a new activation code** und geben Sie den Aktivierungscode im neuen Bereich ein.

Die [Lizenz-Stufe](#) und die Region der neuen Lizenz müssen mit der Lizenz-Stufe und Region der weiteren Aktivierungscode in Ihrer Organisation übereinstimmen.

So löschen Sie einen Aktivierungscode:

1. Aktivieren Sie das Optionsfeld neben dem Aktivierungscode, den Sie löschen möchten, und klicken Sie auf Symbol .
2. Bestätigen Sie im neuen Fenster das Löschen des Aktivierungscode.

Der Lizenzstatus ändert sich auf **Not used**. Ein gelöschter Aktivierungscode kann erneut eingegeben werden.

Fehlerbehebung bei Lizenzproblemen

Wenn Sie die MDR-Lösung für Ihre Assets aktiviert haben, im Abschnitt **Lizenzierung** in der MDR Web Console jedoch weniger Assets angezeigt werden, als mit der MDR-Lösung verbunden sind, sehen Sie in der folgenden Liste mit möglichen Ursachen und passenden Lösungen nach.

Die MDR-Lösung wird unter mehreren Lizenzen aktiviert

Lösung:

Aktivieren Sie alle Lizenzschlüssel im MDR-Plug-in. Die MDR Web Console unterstützt die Aktivierung mehrerer Lizenzschlüssel nicht.

Die MDR-Lösung wurde auf den Assets vor dem 01.01.2024 mithilfe der MDR-Konfigurationsdatei (BLOB) aktiviert

Lösung 1:

1. [Laden Sie eine neue MDR-Konfigurationsdatei \(BLOB\) herunter](#).
2. Wenden Sie die neue MDR-Konfigurationsdatei (BLOB) auf Ihre Assets an.

Lösung 2:

[Verwenden Sie einen Aktivierungscode](#) , um die MDR-Lösung auf Ihren Assets zu aktivieren.

Einige Ihrer Assets verwenden Kaspersky Endpoint Security für Windows Version 12.9 oder älter, und die MDR-Lösung wurde auf diesen Assets mit einer Schlüsseldatei aktiviert

Lösung:

[Verwenden Sie einen Aktivierungscode](#) , um die MDR-Lösung auf Ihren Assets zu aktivieren. Auf solchen Assets wird die Aktivierung mit einer Schlüsseldatei nur eingeschränkt unterstützt und wird nicht empfohlen.

Sie haben eine Schlüsseldatei für die Lizenz von Kaspersky Next Complete Security, Kaspersky Optimum Security, Kaspersky Next MXDR Optimum oder Kaspersky Symphony MDR verwendet, um Kaspersky Endpoint Security für Windows Version 12.9 oder niedriger zu aktivieren.

Lösung:

[Verwenden Sie einen Aktivierungscode](#) , um die MDR-Lösung auf Ihren Assets zu aktivieren.

Über die MDR-Erklärung

Die *MDR-Erklärung* stellt eine verbindliche Vereinbarung zwischen Ihnen und AO Kaspersky Lab dar, welche die Bedingungen vorgibt, unter denen Sie die Lösung verwenden können.

Lesen Sie die MDR-Erklärung sorgfältig, bevor Sie die Lösung benutzen.

Die MDR-Erklärung kann auf dem Bildschirm angezeigt werden:

- Während der Aktivierung von Kaspersky Managed Detection and Response.
- Durch Anklicken des Links **Nutzungsbedingungen für die MDR-Lösung** im Block **Nutzungsbedingungen für die MDR-Lösung** (Abschnitt **MDR** in Kaspersky Security Center → **MDR-Nutzung** → **Nutzungsbedingungen für die MDR-Lösung**).

Sie akzeptieren die Bedingungen der MDR-Erklärung, indem Sie bei der Aktivierung der Lösung bestätigen, dass Sie der MDR-Erklärung zustimmen. Wenn Sie die MDR-Erklärung nicht akzeptieren, brechen Sie die Aktivierung von Kaspersky Managed Detection and Response ab und verwenden Sie die Lösung nicht.

Über die Bereitstellung von Daten

Um zu gewährleisten, dass einige Komponenten von Kaspersky Managed Detection and Response funktionieren, muss Kaspersky die Daten des Benutzers verarbeiten. Die Komponenten senden keine Daten ohne die Erlaubnis des Administrators von Kaspersky Managed Detection and Response.

Die Liste der Benutzerdaten hängt von der Region ab, in der die Lösung verwendet wird. Für Ihre Region kann die Liste der Benutzerdaten von der Liste in diesem Abschnitt abweichen.

Kaspersky schützt alle erhaltenen Informationen in Übereinstimmung mit dem Gesetz und den geltenden Kaspersky-Regeln. Die Daten werden über einen sicheren Kanal übertragen.

Liste der Daten zu Ereignissen, die auf Benutzergeräten eintreten

Zur Erkennung neuer und fortschrittlicher Bedrohungen der Datensicherheit und deren Quellen sowie von eindringenden Bedrohungen, und um umgehend Maßnahmen zur Erhöhung des Schutzes der vom Kunden auf einem Computer gespeicherten und verarbeiteten Daten ergreifen zu können, verpflichtet sich der Kunde, folgende Informationen automatisch bereitzustellen, um den Dienst verwenden zu können:

- Das Datum der Softwareinstallation und -aktivierung, der vollständige Name und die Version der Software, einschließlich Informationen über installierte Updates und Sprachlokalisierung der Software.
- Informationen über die auf dem Computer installierte Software, einschließlich der Version des Betriebssystems, des Datums, an dem es heruntergeladen wurde, und der installierten Updates, und Informationen über Kernel-Objekte, Treiber, Dienste, Autostart-Einträge, Programme, die bei verschiedenen Systemereignissen (z. B. Betriebssystemstart, Benutzeranmeldung usw.) automatisch gestartet werden, und deren Konfigurationen, Browser-Erweiterungen, Microsoft-Internet-Explorer-Erweiterungen, Drucksystem-Erweiterungen, Windows-Explorer-Erweiterungen, Betriebssystem-Shell-Erweiterungen, geladene Objekt-Prüfsummen (MD5), aktive Setup-Elemente, Anwendungen der Systemsteuerung, Browser- und Mail-Client-Versionen.
- Informationen über Dateisystemberechtigungen, das für Dateisystemberechtigungen wirksame Bit, Versionen von Dateisystemberechtigungen, Umgebungsvariablen und Namen von Systemaufrufen.
- Informationen über vererbte Berechtigungen in Bezug auf eine Systemdatei.
- Informationen über den Namen des Computers, IP-Adressen, Standard-Gateways, MAC-Adressen und Hardware, einschließlich einer Prüfsumme der Seriennummer der Festplatte, die letzten zwölf Bytes der Computer-Sicherheitskennung (SID) und die im NTFS-Datenstrom enthaltene Sicherheitszonen-Kennung, Active Directory-Attribute des Computerkontos, einschließlich des Inhalts von msDS-AllowedToActOnBehalfOfOtherIdentity, dNSHostName, distinguishedName, sAMAccountName und userAccountControl.
- Informationen über verwendete Software-Tools zur Behebung von Problemen mit der auf dem Computer des Benutzers installierten Software oder zur Änderung deren Funktionalität sowie über die Return-Codes, die nach der Installation der jeweiligen Software erhalten wurden.

- Informationen über den Zustand des Antivirenschutzes des Computers, einschließlich der Versionen und Release-Daten und Release-Zeiten der verwendeten Antiviren-Datenbanken, Statistiken über Updates und Verbindungen zu Diensten von Kaspersky Lab, Auftragskennungen sowie die Kennungen und Versionen der Software-Komponenten, die die Virensuche unterstützen, Flags, die die interne Kaspersky-Testumgebung bezeichnen, die Primärfehlercodes für ein bestimmtes Ereignis, die Sekundärfehlercodes für ein bestimmtes Ereignis und die Ordnungszahlen der Ereignisse.
- Lizenzschlüssel und Seriennummer der Produkte von Kaspersky Lab, Namen und Versionen dieser Produkte. Kennung von Produktinstallationen von Kaspersky Lab und die Client-Beschreibung aus der Lizenzinformationsdatei.
- Informationen über Kundenbenutzerkonten: Benutzerkontoname, Name des Benutzers, Betriebssystemkennung, Anmeldeinformationen, Berechtigungen, Gruppenmitgliedschaften, Arten von Anmeldesitzungen im System, Name des Authentifizierungspakets, Domänennamen, DNS-Namen, die für Anmeldesitzungen im Authentifizierungssystem verwendet werden, der für die Authentifizierung verwendete Servername, der Benutzerprinzipalname (UPN) für das Konto, die SID, Active Directory-Attribute des Kontos, einschließlich Mail, altSecurityIdentities und sAMAccountName.
- Gesamter Inhalt der Betriebssystemprotokolle.
- Informationen über Aufrufsysteme.
- Informationen über erkannte Vorfälle aus Programmen von Kaspersky Lab, welche Kaspersky Managed Detection and Response unterstützen.
- Informationen über empfangene E-Mails, einschließlich: E-Mail-Adressen der Absender und Empfänger, Betreff, Informationen zum Anhang: Dateiname des Anhangs, Größe, Hash (MD5), Ergebnisse der Dateiformatanalyse.
- Informationen über Koordinaten des Bildschirmbereichs, in dem der Screenshot aufgenommen wurde.
- Informationen über Netzwerkverbindungen, einschließlich IP-Adressen und -Ports von Absender und Empfänger, IPv6-Zonenindizes, Informationen über die Richtung der Netzwerkverbindung (eingehend/ausgehend), die Typen und Masken der durchgeführten DNS-Abfragen, Fehlercodes für eine DNS-Abfrage, Antwort auf eine DNS-Abfrage und Informationen über den angeforderten DNS-Server.
- HTTP-Verbindungsdaten und -Methoden, einschließlich besuchter Webadressen, Referrer-URLs, Benutzer-Agenten, Informationen über TLS-Handshake: Version des TLS-Protokolls, verschlüsselter Servername aus der SNI-Erweiterung, MD5-Hash und SHA1-Hash des Zertifikats, gemeinsamer Name des Haupt-Subjekts und Liste der DNS-Namen der zusätzlichen Subjekte, Name der Zertifizierungsstelle, Seriennummer des von der Zertifizierungsstelle ausgestellten Zertifikats, Ergebnis der Zertifikatsüberprüfung, verwendete Cipher-Suite, Gültigkeitsdauer des Zertifikats, JA3-Dezimalwerte von Client- und Server-Helo-Paketen und deren MD5-Hashes und Daten des Netzwerk-Authentifizierungsprotokolls: MD5-Hash der Daten für die Kerberos-Authentifizierung, Konto- oder Computernamen, der Name des Kerberos-Realms, zu dem der Servername gehört, die Domain, zu der der Client-Name gehört, die UPN für das Konto, das Kryptografiepaket, das für das ausgestellte Kerberos-Ticket verwendet wurde, die Flaggenmaske für das Kerberos-Ticket im Hexadezimalformat, die Ausstellungszeit des Kerberos-Tickets, die Ablaufzeit des Kerberos-Tickets, das Ablaufdatum des Tickets (nach dem das Ticket nicht mehr erneuert werden kann) und der Name des Domaincontrollers, der zur Ausstellung des Kerberos-Tickets verwendet wurde.
- Informationen zu Protokollen auf Programmebene: Größe der LDAP-Suchanfrage, Filter der LDAP-Suchanfrage, eindeutiger Name der LDAP-Suchanfrage, Liste der Attribute für die LDAP-Suchanfrage.
- .Net-Informationen: vollständiger Name des heruntergeladenen .NET-Builds, Assembly-Flags für das heruntergeladene .NET-Build, Modul-Flags für das heruntergeladene .NET-Modul, der Domänenname für das heruntergeladene .NET-Build, Module für den generierten MSIL-Stub, Informationen über die verwaltete Methode: der Namespace der verwalteten Interaktionsmethode, der Name der verwalteten Interaktionsmethode, die Signatur der nativen Methode und die Signatur des Methoden-Stubs.

- Informationen über die im Betriebssystem verarbeiteten Dateien: Dateiname und Dateipfad, Größe, Attribute, Datei- und Objekttypen, Ergebnisse der Dateiformatanalyse, Prüfsumme (MD5), Webadresse, von der die Datei heruntergeladen wurde, E-Mail-Adresse des Absenders, von dem die Datei empfangen wurde und der Betreff der E-Mail, der Inhalt des Dateisystems der VERSIONINFO-Struktur aus den Metadaten der Datei, Informationen über den Herausgeber, wenn die Datei signiert ist, die Benutzerkennung des Dateieigentümers, die Gruppenkennung des Dateieigentümers, der Zeitstempel des letzten Zugriffs auf die Datei, der Zeitstempel der letzten Änderung der Datei-Metadaten, die Erstellung der Datei, die Markierungsmasken für die Überprüfung der digitalen Signatur, die Zeitstempel und Codes von Operationen mit den Dateien und Objekten, die Anzahl der Starts der ausführbaren Datei, die Dateiformatkennung, der vollständige Pfad zum Objekt und der Pfad zum Objekt-Container, der Inhalt der Autorun-Datei, Dateiname und Dateipfad der Datei auf der Remote-Netzwerkressource, auf die zugegriffen wird.
- Inhalt des Verzeichnisses \etc\.
- Befehlsausgabedaten.
- Audit-Daten: Aktionsergebnis, Aktionsbeschreibung, Ereignistyp, Benutzer der Aktion.
- Informationen über den Prozess: Prozesskennung (PID), Ablaufverfolgung von Prozessaufrufen, Informationen über die ausführbare Datei des Prozesses und ihre Kommandozeile, Informationen über den übergeordneten Prozess, MD5-Hash des Fehlercodes aus der Berechnung der ausführbaren Datei, Primärfehlercodes, Informationen zur Prozessintegrität, Informationen zur Sitzungsanmeldung, Kommandozeile, Kommandozeilenargumente für den Prozess, Umgebungsvariablen für den Zielprozess, eindeutige Kennung des Prozessaktivitätsprotokolls, Name und/oder Adresse der Code-Injektionsstelle, Informationen über Zugriffsrechte für den Prozess, Fehlercodes aus der Berechnung des MD5-Hash für ein Objekt aus der Kommandozeile des Prozesses, eine Liste von Datei-Wrappern des Objekts, das anfängliche Arbeitsverzeichnis für den Zielprozess, das Array von Prozesskennungen (PIDs) für abgeschlossene Prozesse.
- Registry-Informationen: Namen, Abschnitte und Werte.
- Informationen über Remote-Vorgänge: Name des Remote-Computers und der Fully Qualified Name (FQDN) des Remote-Computers, auf dem der Remote-Vorgang ausgeführt wurde, der Name des Benutzerkontos, das den Remote-Vorgang initiiert hat, die vom System bereitgestellte Kennung des Remote-Prozesses, der den Remote-Vorgang initiiert hat, die Startzeit des Remote-Prozesses, der den Remote-Vorgang initiiert hat, der Name des Namespace für den Benutzer der WMI-Ereignisse, der Name des WMI-Ereignisfilters des Benutzers, der Name des erstellten Benutzers der WMI-Ereignisse und der Quellcode des Benutzers der WMI-Ereignisse.
- Fehlerinformationen: Fehlercode für die MD5-Berechnung, Dateizugriffsfehlercode, Primärfehlercodes und Sekundärfehlercodes.

- Informationen über Reaktionsereignis-Aufgaben, die von Kaspersky Lab-Spezialisten und Benutzerspezialisten erstellt wurden: Ereignisname und -typ, Datum und Uhrzeit des Eintretens des Ereignisses, Einstellungen und Ergebnisse der Antwortaufgabe (Informationen über das Objekt [Pfad zum Objekt, Objektname und -größe, MD5- und SHA256-Prüfsummen], Informationen über die Quarantäne des Objekts, Informationen über die Löschung des Objekts, Informationen über die Prozessbeendigung, Informationen über die Löschung eines Registrierungsschlüssels/einer Registrierungsteilstruktur, Informationen über den Prozessstart, Informationen über Objekte, die von Kaspersky Lab-Spezialisten zur detaillierten Analyse mit der Zustimmung des Benutzers angefordert werden [Name, Pfad, Größe und Typ des Objekts, MD5- und SHA256-Prüfsummen, Objektbeschreibung, Datum und Uhrzeit der Verarbeitung der Dateianforderung, Dateiinhalte], Informationen über die Installation und das Entfernen der Netzwerkisolation des Gerätes, Informationen über Fehler, die sich aus der Antwortaufgabe ergeben), Ergebnisse der IOC-Untersuchungsaufgabe: IP-Adresse und physische Adresse aus der ARP-Tabelle, Name und Typ des DNS-Ressourcen-Datensatzes, IP-Adresse, Verlauf und Browserinformationen, Datensatz-ID und Name der Datenquelle im Ereignisprotokoll, Name des Ereignisprotokolls, Benutzername, Uhrzeit des Ereignisses, Hash, Vollständiger Name und Größe der Datei, Remote-IP-Adresse und Port mit Verbindung zum Zeitpunkt des Scans, IP-Adresse des lokalen Adapters, Auf lokalem Adapter offener Port, Protokoll als Nummer, Prozessname, Prozess-Argumente, Pfad zur Prozessdatei, Windows PID des Prozesses und des übergeordneten Prozesses, Datum und Uhrzeit des Prozessbeginns, Name und Beschreibung des Dienstes, Pfad und Name der Dienst-DLL (für svchost), Pfad und Name der ausführbaren Datei des Dienstes, Windows-PID, Typ, Status und Ausführungsmodus des Dienstes, Datenträgeretikett, Buchstabe und Typ, Wert der Windows-Registry, Wert des Registry-Hive, Pfad zum Registry-Schlüssel, Registry-Parameter, Physische Adresse des Geräts, Name und Version des Betriebssystems, Netzwerkname des Geräts, Domäne oder Arbeitsgruppe.
- Daten über Skripte, die auf dem Computer ausgeführt werden: Befehlszeilenargumente, Inhalte des Skripts oder Teil des auf dem Computer ausgeführten Skripts, Inhalte des Objekts oder Teil des von AMSI empfangenen Objekts.
- Daten über Befehle, die von der Konsolenanwendung, einschließlich der Befehlszeileninterpreter, durch eine Eingabeumleitung über eine Pipe oder Datei empfangen wurden, sowie Befehle, die vom Benutzer in Konsolenanwendungen, einschließlich der Befehlszeileninterpreter, ausgeführt wurden.

Wenn die MDR-Lösung in Kaspersky Endpoint Detection and Response Expert integriert ist, sind die zusätzlichen Daten nachfolgend aufgeführt:

- Informationen zu gescannten Dateien:
- Prüfsumme (MD5) des verarbeiteten Objekts; Prüfsumme (SHA256) des verarbeiteten Objekts; Name des verarbeiteten Objekts; Größe des verarbeiteten Objekts; Zeitpunkt (Datum und Uhrzeit), zu dem ein verarbeitetes Objekt erstellt wurde; Indikator, der anzeigt, dass die digitale Signatur des geladenen Moduls vorhanden und gültig ist; Informationen darüber, wer die verarbeitete Datei signiert hat; Vertrauensindikator des verarbeiteten Objekts nach KSN; Format des verarbeiteten Objekts; Informationen über die Ergebnisse der Dateisignaturprüfung; Vertrauensindikator des Moduls, dessen Integrität von der Software überprüft wird.
- Informationen zu Alarmen und Erkennungstechnologien:
- Veröffentlichungsdatum und -uhrzeit der Software-Datenbanken; Verdikt der Software für das verarbeitete Objekt; Debugging-Erkennungsanzeige; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Schwachstellen-Gefahrenkategorie; Erkennungs-ID, die von der Software für den Benutzer generiert wurde; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; ID des Abbilds des Gastbetriebssystems von Kaspersky Sandbox; Daten des internen Protokolls, das vom Anti-Virus-Softwaremodul für ein verarbeitetes Objekt erstellt wurde; MD5-Hash der Knoten-IP-Adresse für Kaspersky Sandbox; Ordnungszahl eines Objekts, das erneut untersucht wird; ID des Software-Datenbankeintrags; Wert des Levels der erkannten Schadsoftware oder legitimen Software, mit der der Computer oder die Benutzerdaten beschädigt werden können; Betriebsstatus der Softwarekomponente; Datum und Uhrzeit des Fundes.
- Informationen zu den Ergebnissen der Überprüfung der Telemetriedaten, nachdem die Regel für Angriffsindikatoren (IOA) ausgelöst wurde:

- Funktionen, die einem verarbeiteten Objekt zugewiesen wurden (für Unix-basierte Betriebssysteme); Informationen zu Systemprotokollereignissen: Ereigniszeit, Name des Protokolls, in dem das Ereignis erkannt wurde, Typ und Kategorie des Ereignisses, Name der Ereignisquelle und Ereignisbeschreibung; ID des im Windows-Ereignisprotokoll aufgezeichneten Ereignisses; Zeitstempel der Software-Datenbanken; Größe des verarbeiteten Objekts; Informationen zur Benutzergruppe; Zeitpunkt (Datum und Uhrzeit), zu dem ein verarbeitetes Objekt erstellt wurde; Name des verarbeiteten Objekts; Prüfsumme (MD5) des verarbeiteten Objekts; binäre Maske der Parameter für das verarbeitete Objekt; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; einmalige ID der Anmeldesitzung; Indikator, der anzeigt, dass die digitale Signatur des verarbeiteten Objekts vorhanden und gültig ist; Attribute des Prozesses, der den Selbstschutz der Software angegriffen hat; aktuelle Software-Einstellungen; Name des Softwareherstellers; Name der Software; ID des Gerätes, das die Remote-Verbindung zum System hergestellt hat; Speicherpfad des verarbeiteten Objekts; Wert des Windows-Registrierungselements; Typ des von der Software erkannten Objekts; ID des Benutzerkontos, unter dem der kontrollierte Prozess gestartet wurde; System-ID des Prozesses (PID); Controller-Typ des USB-Gerätes; Typ der Systemfunktion, die widerrufen wurde, um einen neuen Prozess zu verzweigen (für UNIX-basierte Betriebssysteme); Starttyp des Windows-Dienstes; Prüfsumme (SHA256) des verarbeiteten Objekts; Datum und Uhrzeit der letzten Änderung des verarbeiteten Objekts; Webadresse, die verarbeitet wird; Absender-E-Mail-Adresse oder Teile der E-Mail-Adresse, die verarbeitet wird; Code des Dateivorgangs; Name des Benutzergerätes; Attribute der ausführbaren Datei, die verarbeitet wird; Version des Betriebssystems, Build-Nummer des Betriebssystems, Update-Nummer des Betriebssystems, Edition des Betriebssystems, erweiterte Informationen über die Edition des Betriebssystems; Betriebssystemfamilie; Befehlszeile; Informationen darüber, wer die verarbeitete Datei signiert hat; http-Anforderungsmethode; Verdikt der Software für das verarbeitete Objekt; Befehlszeilenargumente für den Prozess; IP-Adressen oder Prüfsummen der IP-Adressen der Quelle und des Zieles der verarbeiteten Netzwerkverbindung; Name der MITRE-Angriffstechnik; Veröffentlichungsdatum und -uhrzeit der Software-Datenbanken; Format des verarbeiteten Objekts; Beschreibung eines verarbeiteten Objekts, wie in den Objekteigenschaften festgelegt; HTTP-Referer; Name und Version des Betriebssystems; Datum und Uhrzeit der Signierung der Datei; DNS-Server-Antwort; Volumen des ausgehenden Datenverkehrs; Typ des Volume-Dateisystems; Zugriffsrechte für das verarbeitete Objekt; offene Flags für ein verarbeitetes Objekt; Typ des Benutzerkontos, unter dem das potentiell schädliche Objekt gestartet wurde; Datum und Uhrzeit des Empfangs; Prüfsumme (SHA1) eines verarbeiteten Objekts; Ergebnis der Aktion mit dem verarbeiteten Objekt; Typ der Anmeldesitzung; Sicherheitszonen-ID, die aus dem NTFS-Datenstrom extrahiert wird; ID der E-Mail-Nachricht; erkannte Dateivorgänge mit dem verarbeiteten Objekt; DNS-Adresse des Webdienstes, auf den zugegriffen wird; Distinguished Name des Objekts; Integritätsebene für das verarbeitete Objekt; Kopfzeile der verarbeiteten http-Anfrage; Daten über ein Drittanbieter-Programm, das einen Fehler verursacht hat: Dateiname und -pfad des Programmabbilds, Programmabbild-Dateigröße und -Prüfsumme (MD5, SHA256, SHA-1), Programm-Prozess-ID (PID), Datum und Uhrzeit der Kompilierung und Erstellung der Programmprozessabbild-Datei, Programmprozess-Speicher-Stack und -Speicheradresse, an der ein Fehler aufgetreten ist, Verfügbarkeit des Programms, bevor der Fehler aufgetreten ist, Namen, Versionen und Prüfsummen (MD5, SHA256, SHA-1) der Dateien der Programmkomponenten; Indikatoren für HTTP-/HTTPS-Netzwerkanfragen: Anfrage-URL, Open-Source-Bibliothekstyp, Anfrage-Domänenname, CND-Anbieter, Anfragemethode, Anfragestartzeit, Anfragepaketgröße, gesamte Anfragedauer, Status-Code, Antwortpaketgröße, Antwortinhaltstyp, Anfrage-Header-Startzeit, Anfrage-Header-Endzeit, Anfrageinhalts-Startzeit, Anfrageinhalts-Endzeit, Antwort-Header-Startzeit, Antwort-Header-Endzeit, Antwortinhalts-Startzeit, Antwortinhalts-Endzeit, Anzahl der Umleitungen, Anzahl fehlgeschlagener DNS-Auflösungen, Gesamtanzahl der DNS-Auflösungen, Anzahl gleichzeitiger Host-Auflösungen, Ergebnis einer einzelnen Auflösung, Startzeit einer einzelnen Auflösung, Endzeit einer einzelnen Auflösung, Erfolgsstatus der Auflösung, Anzahl fehlgeschlagener Socket-Verbindungen, Gesamtanzahl der Socket-Verbindungen, Zieladresse einer einzelnen Verbindung, Startzeit einer einzelnen Verbindung, Endzeit einer einzelnen Verbindung, Startzeit eines einzelnen Handshakes, Endzeit eines einzelnen Handshakes, HTTP-Typ, HTTP-Version, SSL-Typ, Cipher-Suite-Typ, Erfolgsstatus der Verbindungsherstellung, Verbindungsfehler-Informationen, Anfrage-Ausnahmeinformationen, Stack-Informationen im Falle einer nicht normalen Antwort; Zeitpunkt (Datum und Uhrzeit), an dem das Zertifikat abläuft; Vollversion der Software; Anzahl der übertragenen Objekte; Datenträgertyp; Parameter von Aufgaben der Betriebssystem-Aufgabenplanung; gesamter Speicherplatz und derzeit genutzter Platz; Portnummern der Quelle und des Zieles der verarbeiteten Netzwerkverbindung; Wert der Zuverlässigkeit der Erkennung der Schadsoftware oder legitimen Software, mit der der Computer oder die Benutzerdaten beschädigt werden können; Zeitpunkt (Datum und Uhrzeit), an dem das Zertifikat ausgestellt wurde; ID der MITRE-Angriffstechnik; Dienst-ID; Name des Windows-Registrierungsschlüssels; Betreff der verarbeiteten E-Mail-Nachricht; Zeitpunkt (Datum und Uhrzeit), an dem der verarbeitete Prozess endete; Namespace-Name für den WMI-Ereignisempfänger;

Ereigniszeit; Name des Filters, der vom WMI-Ereignisempfänger verwendet wird; Betriebsmodus der Software-Schutzkomponente; Name des Zertifikatausstellers; Umgebungsvariablen, die einem verarbeiteten Objekt zugewiesen wurden (für Unix-basierte Betriebssysteme); Typ der Benachrichtigung, die das Senden der Statistik ausgelöst hat; WMI-Ereignisempfänger; Inhalt von Fragmenten des verarbeiteten Objekts; Parameter der Aufgabe zur Objektübertragung; Name des Netzwerkprotokolls, das im erkannten Netzwerkangriff verwendet wurde; Version des verarbeiteten Objekts; Name und Pfad des Windows-Registrierungselements; Ereigniszähler; ID der Aufgabe zur Objektübertragung; binäre Maske für Optionen der DNS-Abfrage; binäre Maske für Optionen der DNS-Abfrage; Name des Angriffsindikators (IOA); Dringlichkeit des Fensters, das zur Benutzeraktion auffordert; lokale IP-Adresse; Suchbereich der Abfrage; verkürzte Seriennummer der Festplatte; Zeichenfolge der Abfrage; verwendeter Proxyserver; Quelle des verarbeiteten Objekts; Name des erstellten WMI-Ereignisempfängers; Seriennummer des Zertifikats; Version des Angriffsindikators (IOA); ID des Controller-Modus für das USB-Gerät; Empfänger-E-Mail-Adresse oder Teile der E-Mail-Adresse, die verarbeitet wird; ID des Angriffsindikators (IOA); Geräte-ID; Richtung der Netzwerkverbindung; Quelle des verarbeiteten Web-Datenverkehrs; lokaler Host oder Remote-Host; IP-Adresse des DNS-Servers; Typ des Windows-Registrierungswertes; ID der MITRE-ATT&CK-Taktik; Pfad, an dem Code in den Prozess injiziert wurde; Fehler, der bei der Erkennungsverarbeitung aufgetreten ist; der Host, mit dem eine Verbindung hergestellt wurde, um Objekte zu übertragen.

- Dateiattribut eines verarbeiteten Objekts; Sicherheitsparameter aus Ereignissen des Windows-Ereignisprotokolls; Grund für das Verschieben der Datei in die Kategorie; Name der Domäne, die zur Authentifizierung des Besitzers der Anmeldesitzung verwendet wurde; Parameter des Active Directory-Objekts; Vorgangsparameter aus Ereignissen des Windows-Ereignisprotokolls; Benutzersitzungs-Parameter aus Ereignissen des Windows-Ereignisprotokolls; Objekttypcode; Version der Software-Komponente; Einstellungen und Eigenschaften des Smartcard-Geräts; Version der gesendeten Statistiken; System-ID des übergeordneten Prozesses (PID); lokale IP-Adresse; Aufgabenparameter, die in Ereignissen des Windows-Ereignisprotokolls aufgezeichnet wurden; DNS-Adresse des Webdienstes, auf den zugegriffen wird; Webadresse, die verarbeitet wird; Netzwerkverbindungs-Parameter aus Ereignissen des Windows-Ereignisprotokolls; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; Parameter des Active Directory-Objekts; Vorgangsparameter aus Ereignissen des Windows-Ereignisprotokolls; zusätzliche Parameter aus Ereignissen des Windows-Ereignisprotokolls; Benutzersitzungs-Parameter aus Ereignissen des Windows-Ereignisprotokolls; Name der Domäne, die zur Authentifizierung des Besitzers der Anmeldesitzung verwendet wurde; Sicherheits-ID des Benutzerkontos (SID); Fehlertyp; Text der Fehlermeldung.

Liste von Daten über Ereignisse, die als Ergebnis von Analysen des Netzwerkdatenverkehrs erkannt werden

Zur Erkennung neuer und fortschrittlicher Ereignisse der Datensicherheit und deren Quellen sowie von eindringenden Bedrohungen, und um umgehend Maßnahmen zur Erhöhung des Schutzes der vom Kunden auf einem Computer gespeicherten und verarbeiteten Daten ergreifen zu können, verpflichtet sich der Kunde, folgende Informationen automatisch bereitzustellen, um den Dienst verwenden zu können:

- Informationen zu gescannten Dateien:
Prüfsumme (MD5) des verarbeiteten Objekts; Prüfsumme (SHA256) des verarbeiteten Objekts; Name des verarbeiteten Objekts; Größe des verarbeiteten Objekts; Zeitpunkt (Datum und Uhrzeit), zu dem ein verarbeitetes Objekt erstellt wurde; Indikator, der anzeigt, dass die digitale Signatur des geladenen Moduls vorhanden und gültig ist; Informationen darüber, wer die verarbeitete Datei signiert hat; Vertrauensindikator des verarbeiteten Objekts nach KSN; Format des verarbeiteten Objekts; Informationen über die Ergebnisse der Dateisignaturprüfung; Vertrauensindikator des Moduls, dessen Integrität von der Software überprüft wird.

- Informationen zu Alarmen und Erkennungstechnologien:
Veröffentlichungsdatum und -uhrzeit der Software-Datenbanken; Verdikt der Software für das verarbeitete Objekt; Debugging-Erkennungsanzeige; ID des ausgelösten Eintrags in den Antiviren-Datenbanken der Software; Schwachstellen-Gefahrenkategorie; Erkennungs-ID, die von der Software für den Benutzer generiert wurde; Name der erkannten Schadsoftware oder legitimen Software, mit der das Gerät oder die Daten des Benutzers beschädigt werden können; ID des Abbilds des Gastbetriebssystems von Kaspersky Sandbox; Daten des internen Protokolls, das vom Anti-Virus-Softwaremodul für ein verarbeitetes Objekt erstellt wurde; MD5-Hash der Knoten-IP-Adresse für Kaspersky Sandbox; Ordnungszahl eines Objekts, das erneut untersucht wird; ID des Software-Datenbankeintrags; Wert des Levels der erkannten Schadsoftware oder legitimen Software, mit der der Computer oder die Benutzerdaten beschädigt werden können; Betriebsstatus der Softwarekomponente; Datum und Uhrzeit des Fundes.
- Informationen zur Quelle verarbeiteter Objekte und Netzwerkverbindungen:
Quelle des verarbeiteten Objekts; Webadresse, die verarbeitet wird; aufgerufene IPv4-Adresse des Webdienstes; Webadresse der Quelle der Webdienst-Anfrage (Referenz); Host-Quelle; Name der Domäne, die zur Authentifizierung des Besitzers der Anmeldesitzung verwendet wurde; lokale IP-Adresse; Informationen über den Client, der ein Netzwerkprotokoll verwendet (Benutzer-Agent); Absender-E-Mail-Adresse oder Teile der E-Mail-Adresse, die verarbeitet wird; Empfänger-E-Mail-Adresse oder Teile der E-Mail-Adresse, die verarbeitet wird; Betreff der verarbeiteten E-Mail-Nachricht; IP-Adressen oder Prüfsummen der IP-Adressen der Quelle und des Zieles der verarbeiteten Netzwerkverbindung; Portnummern der Quelle und des Zieles der verarbeiteten Netzwerkverbindung; Name des Netzwerkprotokolls, das im erkannten Netzwerkangriff verwendet wurde; Name des Netzwerkprotokolls, das im erkannten Netzwerkangriff verwendet wurde.
- Daten, die an den technischen Support gesendet werden:
Wenn auf der Benutzerseite ein Problem festgestellt wird, das die Qualität der Lösung beeinträchtigt und das Eingreifen des technischen Supports erforderlich macht, werden Informationen wie der Name der Organisation und die Kontakt-E-Mail-Adresse, eine Beschreibung des Problems sowie begleitende Unterlagen, die zum Verständnis und zur Lösung des Problems beitragen können, an das technische Support-Team weitergeleitet. Die Kontakt-E-Mail-Adresse kann sein: die Adresse, auf die Lösung registriert ist, oder die Adresse eines bestimmten Mitarbeiters des Benutzers, falls dieser Mitarbeiter die Unterstützung von den Experten angefordert hat, die Lösungen liefern.
Falls zuvor noch kein Konto mit der von den Experten übermittelten E-Mail-Adresse verknüpft war, legt der technische Support automatisch ein Konto in den technischen Support-Systemen an.
Dieses Konto für den Mitarbeiter des Benutzers ist erforderlich, um die Kommunikation zwischen dem Benutzer und dem technischen Support zu gewährleisten und Probleme, die im Zusammenhang mit der Lösung auftreten, zu beheben.
Dieses Konto wird ausschließlich vom technischen Support verwendet, um Probleme im Zusammenhang mit dem Dienst zu beheben, und so lange verwendet, bis der Kontoinhaber eine Anfrage erstellt, die nichts mit dem Dienst zu tun hat.
- Daten, die beim Versand von Benachrichtigungen und Vorfallberichten gesendet werden:
Der Benutzer kann den Dienst nutzen, um Benachrichtigungen im Fall von Informationssicherheitsvorfällen und zusammenfassende Berichte über Informationssicherheitsvorfälle an die vom Benutzer vorgegebenen Empfänger zu senden.
Wenn der Dienst für den Versand von Benachrichtigungen und Berichten per E-Mail konfiguriert ist, verarbeitet der Auftragsverarbeiter die folgenden Daten: die Benutzer-ID und die E-Mail-Adresse des Empfängers.
Wenn der Dienst für den Versand von Benachrichtigungen über den Telegram-Bot konfiguriert ist, verarbeitet der Auftragsverarbeiter die folgenden Daten: die Benutzer-ID, die ID des Empfängers der Benachrichtigung, eine Markierung, die anzeigt, ob der Empfänger der Benachrichtigung den Telegram-Bot abonniert hat, ein Link zum Chat des Empfängers der Benachrichtigung mit dem Telegram-Bot.

Die Bereitstellung von Daten im Rahmen der Verwendung von Kaspersky Endpoint Agent

Einzelheiten zur Bereitstellung von Daten im Rahmen der Verwendung von Kaspersky Endpoint Agent finden Sie in [Kaspersky Endpoint Agent für Windows](#).

Regionen der Datenverarbeitung

Die folgende Tabelle enthält die Regionen, in denen die Benutzerdaten gemäß der Erklärung zur Datenverarbeitung von Kaspersky Managed Detection and Response verarbeitet werden.

Regionen der Datenverarbeitung

Region der genutzten Lizenz	Regionen der Datenverarbeitung
Europa, Kanada	Europa
Königreich Saudi-Arabien	Königreich Saudi-Arabien
Russland und weitere Regionen mit Ausnahme der oben aufgeführten	Russland

Die Region der Datenverarbeitung ist abhängig von der Region, die Sie während der [Aktivierung](#) von Managed Detection and Response auswählen, um die Einhaltung der gesetzlichen Anforderungen bezüglich der Verarbeitung von Benutzerdaten zu gewährleisten.

Über die Erklärung zur Datenverarbeitung

Die *Vereinbarung zur Datenverarbeitung* (VDV) ist ein wesentlicher Bestandteil der Vereinbarung zu Kaspersky Managed Detection and Response. Diese Vereinbarung zur Datenverarbeitung gilt für die Verarbeitung von Benutzerdaten durch AO Kaspersky Lab im Auftrag des Benutzers.

Der Inhalt der *Vereinbarung zur Datenverarbeitung* (VDV), ihre Verfügbarkeit in den Benutzeroberflächen der Lösung und die Liste der Benutzerdaten hängen von der Region ab, in der die Lösung verwendet wird.

Die Vereinbarung zur Datenverarbeitung kann wie folgt auf dem Bildschirm angezeigt werden:

- Während der Aktivierung von Kaspersky Managed Detection and Response (nur in einigen Regionen).
- Im Abschnitt **Über** der MDR Web Console: <https://mdr.kaspersky.com/about> (nur in einigen Regionen).

Der Abschnitt **Über** ist nur für angemeldete Benutzer verfügbar.

- In der Zusammenstellung von Dokumenten, die Sie beim Kauf von Kaspersky Managed Detection and Response erhalten (nur in einigen Regionen).

Lesen Sie die Vereinbarung zur Datenverarbeitung sorgfältig durch, bevor Sie die Lösung benutzen.

Sie bestätigen, dass Sie die Vereinbarung zur Datenverarbeitung vollständig gelesen und verstanden haben, wenn Sie die Lösung aktivieren oder die Lösung Kaspersky Managed Detection and Response erwerben. Wenn Sie mit der Verarbeitung Ihrer Daten, wie sie in der Vereinbarung zur Datenverarbeitung beschrieben ist, nicht einverstanden sind, brechen Sie die Aktivierung von Kaspersky Managed Detection and Response ab und verwenden Sie die Lösung nicht.

Benutzeroberflächen von Kaspersky Managed Detection and Response

Dieser Abschnitt enthält Informationen zu den Benutzeroberflächen von Kaspersky Managed Detection and Response.

Sie können für die Arbeit mit Kaspersky Managed Detection and Response die folgenden Schnittstellen verwenden:

- Das Portal von Kaspersky Managed Detection and Response (im Weiteren auch als MDR Web Console bezeichnet).

Die MDR Web Console ist verfügbar unter <https://mdr.kaspersky.com/> nachdem Sie sich dort angemeldet haben. Verwenden Sie zum Anmelden die E-Mail-Adresse und das Kennwort des Benutzerkontos von der [Kaspersky-Website](#), welches [bei der Aktivierung](#) von Kaspersky Managed Detection and Response erstellt wurde.

- Den Abschnitt **MDR** in der [Kaspersky Security Center Web Console](#) oder in Kaspersky Next Expert View.

Um Kaspersky Security Center Web Console mit Kaspersky Managed Detection and Response zu verwenden, müssen Sie das MDR-Plug-in [herunterladen und in der Kaspersky Security Center Web Console konfigurieren](#). In Kaspersky Next Expert View ist das MDR-Plug-in vorinstalliert.

Um auf die Funktionen von Kaspersky Managed Detection and Response zuzugreifen, klicken Sie in der Kaspersky Security Center Web Console oder in Kaspersky Next Expert View auf **Überwachung und Berichterstattung** → **MDR**.

Die Möglichkeiten und verfügbaren Funktionen dieser Schnittstellen sind im Wesentlichen identisch, es wird jedoch gelegentlich empfohlen, für einige Aufgaben eine bestimmte der beiden Schnittstellen zu verwenden. Dies hängt damit zusammen, dass in der empfohlenen Schnittstelle eine größere Auswahl an Funktionen oder Daten zur Verfügung steht. Die jeweils empfohlene Schnittstelle ist in der Beschreibung der Aufgaben und Verwendungsszenarien angegeben.

Die Benutzeroberfläche von Kaspersky Security Center ist hauptsächlich für die folgenden Aufgaben vorgesehen:

- [Kaspersky Managed Detection and Response aktivieren](#)
- Statuswerte der Assets prüfen

Die Benutzeroberfläche der MDR Web Console ist hauptsächlich für die folgenden Aufgaben vorgesehen:

- Aufgaben des Security Officers wahrnehmen: Vorfällen verwalten
- Aufgaben des Administrators wahrnehmen: MDR-Benutzer verwalten
- Assets anzeigen und verwalten

MDR-Abschnitt in Kaspersky Security Center

Sie können mit Kaspersky Managed Detection and Response arbeiten, indem Sie den Abschnitt **MDR** in der [Kaspersky Security Center Web Console](#) oder in Kaspersky Next Expert View verwenden. Um auf die Funktionen von Kaspersky Managed Detection and Response zuzugreifen, klicken Sie in Kaspersky Security Center auf **Überwachung und Berichterstattung** → **MDR**.

Der Abschnitt **MDR** in der Weboberfläche von [Kaspersky Security Center](#) enthält die folgenden Registerkarten:

- **Vorfälle.** Enthält den Link zur MDR Web Console, in der Sie Ihre Vorfälle verwalten können.
- **Einstellungen.** Ermöglicht das Aktivieren erweiterter Benachrichtigungen und das Ändern der Sprache für Vorfallsdaten, Benachrichtigungen und Berichte.
- **Lizenzierung.** Ermöglicht die Verwaltung von MDR-Lizenzen.
- **API.** Enthält eine Liste mit den API-Verbindungen und die Funktionen, um diese zu verwalten.
- **Mandanten.** Enthält eine Liste mit den Mandanten und die Funktionen, um diese zu verwalten.
- **Status der MDR-Assets.** Enthält Listen mit fehlerhaften Assets und mit allen Assets, die mindestens einmal gesehen wurden.
- **Erste Schritte** (Getting Started). Umfasst eine Anleitung zur Einrichtung der MDR-Lösung.
- **MDR-Nutzung.** Enthält Informationen zum Aktivierungsstatus der Lösung, zur Lizenz, zur Region für die Speicherung von Telemetriedaten, zur KPSN-Konfigurationsdatei und darüber, ob die Nutzungsbedingungen akzeptiert wurden.

Sie können in Kaspersky Security Center im Abschnitt **Überwachung und Berichterstattung** → **Dashboard** das Widget **MDR-Assets nach Status** [hinzufügen](#).

MDR-Plug-in in Kaspersky Security Center einrichten

Dieser Abschnitt enthält Informationen zur Erstkonfiguration des MDR-Plug-ins in Kaspersky Security Center für die Arbeit mit Kaspersky Managed Detection and Response.

Zugriffsrechte in Kaspersky Security Center konfigurieren

Sie müssen die Zugriffsrechte für jeden Benutzer von Kaspersky Security Center Web Console oder Kaspersky Next Expert View konfigurieren, der MDR-Funktionen in Kaspersky Security Center verwendet. Die Zugriffsrechte hängen von den ausführbaren Vorgängen ab, die Sie für die Benutzer vorgesehen haben.

Sie können die MDR Rollen mit vordefinierten Zugriffsrechten automatisch erstellen, indem Sie in Kaspersky Security Center im Abschnitt **MDR** den Link im ersten Schritt auf die Registerkarte **Erste Schritte** (Getting Started) anklicken.

So konfigurieren Sie die Zugriffsrechte:

1. Wechseln Sie in der Kaspersky Security Center zum Abschnitt **Benutzer und Rollen** → **Rollen** und erstellen Sie anschließend eine neue Rolle. Ausführliche Informationen zum Erstellen von Rollen finden Sie in der [Hilfe zu Kaspersky Security Center für Windows](#), der [Hilfe zu Kaspersky Security Center für Linux](#) oder der [Hilfe zu Kaspersky Next Expert View](#).

2. Gewähren Sie auf der Registerkarte **Zugriffsrechte** einer neuen Rolle das Recht **Zulassen** für die folgenden Funktionsbereiche:

- **Kaspersky Security Center Administrationsserver** → **Allgemeine Funktionen** → **Programmintegration**
Kaspersky Security Center Administrationsserver → **Allgemeine Funktionen** → **Basisfunktionen**
Kaspersky Security Center Administrationsserver → **Allgemeine Funktionen** → **Auf Objekte unabhängig von ihren ACLs zugreifen**

Diese Zugriffsrechte ermöglichen Benutzern, Kaspersky Managed Detection and Response zu aktivieren, zu konfigurieren, zu verwenden und die Verwendung zu beenden

- **Kaspersky Managed Detection and Response** → **Zugriff auf Vorfälle**

Damit Benutzer Zugriff auf den Abschnitt **MDR** in Kaspersky Security Center haben, muss das Recht **Zulassen** für den Funktionsbereich **Zugriff auf Vorfälle** festgelegt werden. Wenn für den Funktionsbereich **Zugriff auf Vorfälle** das Recht **Verbieten** festgelegt ist, kann der Benutzer in Kaspersky Security Center nur die Registerkarte **Erste Schritte** (Getting Started) des Abschnitts **MDR** anzeigen.

- **Kaspersky Managed Detection and Response** → **Verwaltung von Mandanten**

Ermöglicht es Benutzern, Mandanten zu erstellen, anzuzeigen und zu bearbeiten.

- **Kaspersky Managed Detection and Response** → **Zugriff auf REST-API**

Ermöglicht es Benutzern, Kaspersky Managed Detection and Response über die REST-API zu verwalten.

3. Weisen Sie die erstellte Rolle allen Benutzern zu, welche die MDR-Funktionen in Kaspersky Security Center verwenden.

Die folgende Tabelle zeigt den Mindestsatz an Zugriffsrechten.

Mindestsatz an Zugriffsrechten

Funktionsbereich	Erlauben	Verweigern
Integration von Programmen	—	✓
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	—	✓
Verwaltung von Reaktionen	—	✓
Verwaltung von Mandanten	—	✓
Planung einer Zusammenfassung des Vorfalls	—	✓
Zugriff auf REST-API	—	✓

Die Zugriffsrechte sind konfiguriert.

MDR-Einstellungen in Kaspersky Security Center anzeigen und bearbeiten

Sie können die Einstellungen des in Kaspersky Security Center installierten MDR-Plug-ins anzeigen und bearbeiten.

So zeigen Sie Einstellungen an und bearbeiten sie:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **Einstellungen**.
2. Wenn Sie [die erweiterten Benachrichtigungen](#) per E-Mail aktivieren möchten, aktivieren Sie zunächst die Option **Erweiterte Benachrichtigungen per E-Mail aktivieren** und anschließend das Kontrollkästchen, um zu bestätigen, dass Sie die Bedingungen für den Versand von erweiterten Benachrichtigungen gelesen und verstanden haben.
3. Mit der Einstellung **Sprache** können Sie für die angezeigten Berichte und Benachrichtigungen zwischen englischer oder russischer Sprache auswählen.
4. Klicken Sie im unteren Bereich des Fensters auf die Schaltfläche **Speichern**, um die Einstellungen zu speichern. Die Schaltfläche **Speichern** wird erst aktiv, wenn Sie Einstellungen geändert haben.

Funktionen des MDR-Plug-ins auf einem virtuellen Administrationsserver verwenden

So verwenden Sie die MDR-Funktionen in Kaspersky Security Center auf einem virtuellen Administrationsserver:

- Wenn Sie Kaspersky Security Center für Windows verwenden:
 1. Laden Sie die [MDR-Konfigurationsdatei](#) in der Kaspersky Security Center Web Console oder in der [MDR Web Console](#) herunter.
 2. Wählen Sie in Kaspersky Security Center Web Console den (physischen) Haupt-Administrationsserver aus, auf dem sich Ihr virtueller Administrationsserver befindet.
 3. Aktivieren Sie den Schalter [Kaspersky Private Security Network](#) in den Eigenschaften des Haupt-Administrationsservers (physisch).
 4. Klicken Sie auf die Schaltfläche **Datei mit KSN-Proxy-Einstellungen auswählen** und wählen Sie die heruntergeladene MDR-Konfigurationsdatei aus.
- Wenn Sie Kaspersky Next Expert View verwenden:
 1. Aktivieren Sie Kaspersky Managed Detection and Response auf dem Haupt-Administrationsserver (physischer Server).
 2. Klicken Sie auf dem Haupt-Administrationsserver (physisch) auf **Überwachung und Berichterstattung** → **MDR**, öffnen Sie die Registerkarte **MDR-Nutzung** und vergewissern Sie sich, dass im Abschnitt **KPSN-Konfigurationsdatei für die Integration in den KSC-Administrationsserver** der korrekte Status angezeigt wird und die richtige Version der KPSN-Konfigurationsdatei enthalten ist. Beispiel für den korrekten Status und die richtige Version:

Um Telemetriedaten an die Kaspersky MDR-Infrastruktur zu übertragen, wird die KPSN-Konfigurationsdatei der Version verwendet

Wenn der Dateistatus oder die Version nicht korrekt sein sollten, [wenden Sie sich bitte an den Technischen Support](#).

Verwendung der MDR-Funktionen in Kaspersky Security Center über einen Proxyserver

Wenn in dem Netzwerk, in dem Kaspersky Security Center ausgeführt wird, ein Proxyserver verwendet wird, müssen Sie für das HTTP- und das HTTPS-Protokoll zwei Umgebungsvariablen mit Proxyserver-Einstellungen festlegen. Das ist notwendig, damit die MDR-Funktionen in Kaspersky Security Center ordnungsgemäß funktionieren. Diese Umgebungsvariablen müssen auf dem Host festgelegt werden, auf dem Kaspersky Security Center Web Console installiert ist.

Die Umgebungsvariablen haben das folgende Format:

`HTTP_PROXY=<Protokoll>://<Proxy-Benutzername>:<Proxy-Kennwort>@<Host>:<Port>`

wobei:

- <Protokoll> – http oder https
- <Proxy-Benutzername> – Benutzername für die Autorisierung auf dem Proxyserver
- <Proxy-Kennwort> – Kennwort für die Autorisierung auf dem Proxyserver
- <Host>:<Port> – Name oder IP-Adresse des Proxyservers und dessen Portnummer

Beispiel für die Umgebungsvariablen:

```
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
```

Sie können die Umgebungsvariablen auf zwei Arten festlegen:

- Wenn Sie die Proxy-Einstellungen für alle Programme auf dem Host anwenden möchten, auf dem Kaspersky Security Center Web Console installiert ist, fügen Sie diese Umgebungsvariablen mithilfe der Komponente **Umgebungsvariablen des Systems bearbeiten** des Windows-Betriebssystems hinzu. Informationen zur Verwendung dieser Komponente finden Sie in der Dokumentation Ihres verwendeten Betriebssystems.
- Wenn Sie diese Proxy-Einstellungen nur auf Kaspersky Security Center Web Console anwenden möchten, fügen Sie diese Umgebungsvariablen zur .env-Datei hinzu. Diese Datei befindet sich im Installationsordner von Kaspersky Security Center Web Console (Standardpfad: C:\Programme\Kaspersky Lab\Kaspersky Security Center Web Console\). Sollte die .env-Datei nicht im Installationsordner vorhanden sein, erstellen Sie sie.

Nachdem Sie die Umgebungsvariablen festgelegt haben, müssen Sie den Host, auf dem Kaspersky Security Center Web Console installiert ist, neu starten. Dadurch werden die Änderungen übernommen.

Änderung der Zertifikate zur Verwendung der MDR-Funktionen in Kaspersky Security Center mit einem Proxyserver oder einer Antiviren-Software

In folgenden Fällen müssen Sie die Zertifikatskette für die Verbindung zwischen Kaspersky Security Center Web Console mit dem MDR-Plug-in und der Infrastruktur der MDR-Lösung neu definieren:

- Im Netzwerk, in dem Kaspersky Security Center ausgeführt wird, wird ein Proxyserver mit TLS-Verbindung verwendet.
- Auf einem Host, auf dem Kaspersky Security Center Web Console installiert ist, wird eine Antiviren-Software mit TLS-Datenverkehrsverschlüsselung ausgeführt.

So definieren Sie die Zertifikatskette neu:

1. Speichern Sie die erforderlichen Zertifikate als Dateien auf Ihrem Computer.

- So speichern Sie die Zertifikatsdatei der Software, die den Datenverkehr verschlüsselt: Öffnen Sie auf dem Host mit Kaspersky Security Center Web Console die Seite <https://mdr-ksc.kaspersky.com/> im Chrome-Browser und klicken Sie in der Adressleiste auf das Schloss-Symbol neben der Website-Adresse. Klicken Sie jetzt auf **Verbindung ist sicher** und anschließend auf **Zertifikat ist gültig**. Wechseln Sie zur Registerkarte **Details** und klicken Sie dort auf die Schaltfläche **Exportieren**. Die Anweisungen für andere Browser finden Sie in der Dokumentation der jeweiligen Browser.
- Das Zertifikat für die Verbindung mit dem Proxyserver können Sie bei Ihrem Netzwerkadministrator anfordern.

2. Fügen Sie die gespeicherten Zertifikate der Datei mit der Erweiterung .PEM hinzu (z. B. KL_Root.pem).

3. Legen Sie die erstellte .PEM-Datei im Installationsordner von Kaspersky Security Center Web Console ab (Standardpfad: C:\Programme\Kaspersky Lab\Kaspersky Security Center Web Console\).

4. Fügen Sie die Umgebungsvariable NODE_EXTRA_CA_CERTS zu der .env-Datei hinzu, die sich im Installationsordner von Kaspersky Security Center Web Console befindet. Sollte die .env-Datei nicht im Installationsordner vorhanden sein, erstellen Sie sie.

Beispiel für die Variable:

```
NODE_EXTRA_CA_CERTS="C:\Programme\ Kaspersky Lab\ Kaspersky Security Center Web Console\KL_Root.pem"
```

Um nach dem Festlegen der Umgebungsvariable diese Änderungen zu übernehmen, starten Sie den Host mit der installierten Kaspersky Security Center Web Console neu.

MDR-Funktionen in Kaspersky Security Center ein- und ausblenden

Die Bedienelemente von Kaspersky Managed Detection and Response werden standardmäßig in der Benutzeroberfläche der Kaspersky Security Center angezeigt. Wenn Sie Kaspersky Managed Detection and Response nicht verwenden, können Sie dessen Funktionen aus der Benutzeroberfläche ausblenden. Sie können später die [die Einstellungen der Benutzeroberfläche ändern](#), um die ausgeblendeten Elemente wieder anzuzeigen.

So verbergen Sie die MDR-Funktionen in Kaspersky Next Expert View:

1. Bewegen Sie in Kaspersky Security Center Web Console oder Kaspersky Next Expert View den Mauszeiger auf Ihren Benutzernamen, der sich im linken unteren Bereich befindet. Das Menü mit den Einstellungen der Benutzeroberfläche wird angezeigt.
2. Klicken Sie auf **Einstellungen der Benutzeroberfläche**.
3. Deaktivieren oder aktivieren Sie die Option **MDR-Funktionen anzeigen**.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Kaspersky Security Center speichert den Wert dieser Option nur für Ihr Benutzerkonto. Andere Benutzer können einen anderen Wert festlegen.

Der **MDR**-Bereich wird ausgeblendet oder angezeigt.

MDR Web Console

Sie können mit Kaspersky Managed Detection and Response über die Weboberfläche namens [MDR Web Console](#)  arbeiten.

Das Fenster der MDR Web Console enthält die folgenden Elemente:

- Hauptmenü im linken Fensterbereich
- Arbeitsbereich im rechten Fensterbereich

Hauptmenü

Das Hauptmenü enthält die folgenden Abschnitte:

- **Monitoring.** Enthält die Widgets mit zusammenfassenden Informationen zu aktiven Vorfällen, Assets und Reaktionen.
- **Incidents.** Enthält detaillierte Informationen über Ihre Vorfälle und die Tools, um diese zu verwalten.
- **Assets.** Enthält detaillierte Informationen über Assets und die Tools, um diese zu verwalten.
- **Settings.** Enthält Registerkarten für das Arbeiten mit Benutzerkonten, Benachrichtigungen, Vorfalleinstellungen, zusammenfassenden Berichten, API, Mandanten und allgemeinen Einstellungen.
- **About.** Enthält neben Informationen über die Lösung auch die Links zur MDR-Erklärung, zur Vereinbarung zur Datenverarbeitung, zu dieser Online-Hilfe und zur Website des Technischen Supports.

Im unteren Bereich der linken Leiste befindet sich das Steuerelement **Account settings**. Damit können Sie in MDR Web Console auf die *Seite „Erste Schritte“* zugreifen, die Sprache der Benutzeroberfläche ändern, die Seite Ihres Benutzerprofils öffnen und sich von MDR Web Console abmelden.

Arbeitsbereich

Im Arbeitsbereich werden die Informationen angezeigt, die Sie in der MDR Web Console anzeigen möchten. Zudem enthält der Bereich Steuerelemente, mit denen Sie die Darstellung der Informationen anpassen können.

Sprache der Benutzeroberfläche in Kaspersky Security Center ändern

Die MDR-Benutzeroberfläche ist in Kaspersky Security Center in den folgenden Sprachen verfügbar:

- Englisch
- Russisch
- Deutsch
- Spanisch
- Französisch
- Italienisch

So ändern Sie die Sprache der Benutzeroberfläche in Kaspersky Security Center:

1. Wechseln Sie in Kaspersky Security Center Web Console oder Kaspersky Next Expert View im Hauptmenü zu **Einstellungen** → **Sprache**.
2. Wählen Sie eine der unterstützten Lokalisierungssprachen aus.

Die Sprache wird umgeschaltet.

Sie können jederzeit zu einer anderen Sprache wechseln.

Sprache der Benachrichtigungen und Berichte in Kaspersky Security Center ändern

In Kaspersky Security Center können für die angezeigten Vorfalldaten, Benachrichtigungen und Berichte zwischen den Sprachen Englisch oder Russisch auswählen.

So ändern Sie Sprache für Benachrichtigungen und Berichte in Kaspersky Security Center:

1. Klicken Sie in der Kaspersky Security Center Web Console oder in Kaspersky Next Expert View auf **MDR** → **Einstellungen**.
2. Wählen Sie im Bereich **Sprache** entweder **Russisch** oder **Englisch** aus.
3. Klicken Sie auf die Schaltfläche **Speichern**.

Die Sprache wird umgeschaltet.

Sie können jederzeit zu einer anderen Sprache wechseln.

Das Ändern der Sprache wirkt sich nur auf neue Benachrichtigungen und Berichte aus. Benachrichtigungen und Berichte, die bereits erstellt wurden, behalten die alte Spracheinstellung bei.

Sprache der Benutzeroberfläche in der MDR Web Console ändern

Die Benutzeroberfläche der MDR Web Console ist in den folgenden Sprachen verfügbar:

- Englisch
- Russisch

So ändern Sie die Sprache der Benutzeroberfläche der MDR Web Console:

1. Wechseln Sie in der MDR Web Console zum Abschnitt **Account settings**, der sich auf der linken Seite am unteren Rand befindet. Dieser Abschnitt enthält den Bereich **Language**.
2. Klicken Sie im Bereich **Language** auf die Sprache, die Sie für die Oberfläche der MDR Console übernehmen möchten.

Die Sprache wird geändert. Sie können die Sprache im Anschluss jederzeit ändern.

Über die MDR-Konfigurationsdatei

Für die auf den [Assets](#) installierten EPP-Anwendungen für Workstations von Kaspersky (wie Kaspersky Endpoint Security für Windows) verwendet Kaspersky Managed Detection and Response eine MDR-Konfigurationsdatei, um die Lösung auf diesen Assets zu aktivieren.

Die MDR-Konfigurationsdatei wird von Kaspersky Managed Detection and Response automatisch generiert, wenn Sie die Lösung mittels eines Aktivierungscodes aktivieren. Die MDR-Konfigurationsdatei ist ein zip-Archiv mit folgenden Dateien:

- [KPSN](#)-Konfigurationsdatei
- BLOB-Datei (P7) für die Bereitstellung von EPP-Anwendungen, welche die Integration mit MDR über Richtlinien von Kaspersky Security Center unterstützen.

Die BLOB-Datei läuft 5 Jahre nach ihrer Erstellung ab. Dies gilt auch, wenn die Lizenz unbefristet ist oder für einen längeren Zeitraum ausgestellt wurde.

Unter den folgenden Bedingungen benötigen Sie die BLOB (P7)-Datei möglicherweise nicht:

Hinweis: Sie müssen die Lösung auch dann über die MDR Web Console oder das MDR-Plug-in in Kaspersky Security Center aktivieren, wenn Sie die MDR-Konfigurationsdatei nicht verwenden.

- Sie verwenden nur die folgenden EPP-Anwendungen:
 - Kaspersky Endpoint Security für Windows 12.6 oder höher
 - Kaspersky Endpoint Security für Windows 12.8 oder höher im Light Agent-Modus
 - Kaspersky Endpoint Security für Linux Version 12.3 oder höher
 - Kaspersky Endpoint Security for Mac 12.2 oder höher
- Ihr Unternehmen verwendet nur den Root-Mandanten und erstellt keine zusätzlichen Mandanten.
- Sie verwenden die Lösung Kaspersky Endpoint Detection and Response Optimum nicht gleichzeitig mit der Lösung Kaspersky MDR. Details finden Sie unter [MDR-Lösungen in Kaspersky-Anwendungen aktivieren](#).

In diesem Fall wendet Kaspersky Endpoint Security für Windows die Lizenz aus Kaspersky Security Center an. Wenn Sie andere Mandanten als den Root-Mandanten verwenden, müssen Sie die MDR-Konfigurationsdatei für jeden Mandanten herunterladen.

[Laden Sie die MDR-Konfigurationsdatei herunter](#) und verwenden Sie diese gemäß den Anweisungen der EPP-Anwendungen, die auf Ihren Assets installiert sind:

- [Kaspersky Endpoint Security für Windows](#)
- [Kaspersky Endpoint Security für Linux](#)
- [Kaspersky Endpoint Security for Mac](#)

Über Kaspersky Security Network

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Die MDR-Lösung verwendet Kaspersky Security Network (KSN) für die folgenden Aufgaben:

- Senden von Telemetriedaten von den Assets.
- Integration in den Server von Kaspersky Anti Targeted Attack Platform (EDR).
- Integration in Kaspersky Endpoint Detection and Response Expert innerhalb der Open Single Management Platform.

Eine KPSN-Konfigurationsdatei wird installiert, wenn Sie die Integration in Kaspersky Anti Targeted Attack Platform (EDR) oder in Kaspersky Endpoint Detection and Response Expert innerhalb der Open Single Management Platform konfigurieren.

Empfehlung: Verwenden Sie keine KPSN-Konfigurationsdatei, um Telemetriedaten von den Assets zu senden. Sollte Ihre Konfiguration [die Voraussetzungen für den Betrieb ohne KPSN-Konfigurationsdateien](#) jedoch nicht erfüllen, müssen Sie eine KPSN-Konfigurationsdatei auf dem Administrationsserver installieren. Weitere Informationen zur Konfiguration von KSN finden Sie in der [Dokumentation zu Kaspersky Security Center](#). Um eine sichere Übertragung der Telemetriedaten vom Kunden an Kaspersky Managed Detection and Response zu gewährleisten, aktualisiert Kaspersky regelmäßig die Chiffrierschlüssel für MDR-Telemetriedaten. Weitere Informationen dazu finden Sie im folgenden Artikel: [KPSN-Konfigurationsdateien regelmäßig aktualisieren](#).

Wenn Sie eine KPSN-Konfigurationsdatei auf dem Kaspersky Security Center Administrationsserver installieren, wird KSN automatisch deaktiviert, falls Sie [Ihre Zustimmung zu den Nutzungsbedingungen der MDR-Lösung widerrufen](#).

Wenn Sie auf dem Administrationsserver manuell eine KPSN-Konfigurationsdatei hinzugefügt und das MDR-Plug-in für Kaspersky Security Center nicht aktiviert haben, müssen Sie die KPSN-Konfigurationsdatei manuell ersetzen oder vom Administrationsserver entfernen.

KPSN-Konfigurationsdateien regelmäßig aktualisieren

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Es wird empfohlen, die MDR-Lösung auf den Betrieb ohne KPSN-Konfigurationsdateien umzustellen. Weitere Informationen dazu finden Sie in diesem Artikel: [MDR-Lösung auf den Betrieb ohne KPSN-Konfigurationsdateien umstellen](#). Wenn Sie Assets betreiben, die KPSN-Konfigurationsdateien verwenden, müssen Sie die Konfigurationsdateien jährlich aktualisieren. Andernfalls stellen diese Assets die Übertragung ihrer Telemetriedaten an Kaspersky Managed Detection and Response ein.

Wenn Sie derzeit nicht auf den Betrieb ohne KPSN-Konfigurationsdateien umstellen können, lesen Sie die folgenden Informationen und befolgen Sie die Anweisungen.

Warum die Aktualisierung der Konfigurationsdateien erforderlich ist

Um eine sichere Übertragung der Telemetriedaten vom Kunden an Kaspersky Managed Detection and Response zu gewährleisten, aktualisiert Kaspersky regelmäßig die Chiffrierschlüssel für MDR-Telemetriedaten. Der öffentliche Schlüssel wird als Teil der KPSN-Konfigurationsdatei übertragen.

Wenn Sie das MDR-Plug-in für Kaspersky Next Expert View oder ein lokal bereitgestelltes Kaspersky Security Center verwenden, wird die KPSN-Konfigurationsdatei in einigen Fällen automatisch aktualisiert (siehe dazu Details in der folgenden Tabelle). In vielen Fällen müssen Sie jedoch die installierte KPSN-Konfigurationsdatei manuell ersetzen.

Spätestens einen Monat vor Ablauf der aktuellen KPSN-Konfigurationsdatei benachrichtigt Kaspersky Sie über den bevorstehenden Ablauf der KPSN-Konfigurationsdatei. Es stehen zwei Benachrichtigungsoptionen zur Verfügung:

- Es wird ein Vorfall erstellt, der Sie über den bevorstehenden Ablauf der aktuellen KPSN-Konfigurationsdatei informiert.
- In der MDR Web Console wird eine Benachrichtigung über den bevorstehenden Ablauf der aktuellen KPSN-Konfigurationsdatei veröffentlicht. Diese Benachrichtigung wird jedem Benutzer, der sich an der MDR Web Console anmeldet, angezeigt.

Erforderliche Maßnahmen zum Aktualisieren der KPSN-Konfigurationsdatei

Lösung für die Verwaltung Ihrer Assets	Schnittstelle, die Ihre SOC-Analysten verwenden	Erforderliche Maßnahmen
Kaspersky Next Expert View	MDR-Plug-in in Kaspersky Next Expert View installiert	Melden Sie sich bei Kaspersky Next Expert View an. Wenn Sie sich anmelden, fordert das MDR-Plug-in Sie auf, die neue KPSN-Vereinbarung zu akzeptieren. Die KPSN-Konfigurationsdatei wird automatisch aktualisiert, nachdem der Administrator die KPSN-Vereinbarung akzeptiert hat. Wenn das MDR-Plug-in die Datei erfolgreich aktualisiert, erhalten Sie eine Benachrichtigung über die Änderung der KPSN-Konfigurationsdatei. Wenn das MDR-Plug-in die KPSN-Konfigurationsdatei nicht aktualisieren kann, erhalten Sie eine Benachrichtigung zur Ursache des Problems: • Ihr Konto verfügt nicht über ausreichende Zugriffsrechte, um die Datei zu aktualisieren. • Beim Aktualisieren der KPSN-Konfigurationsdatei ist ein unerwarteter Fehler aufgetreten. Wenn keine Benachrichtigungen angezeigt werden, wurde die KPSN-Konfigurationsdatei wahrscheinlich bereits erfolgreich aktualisiert, als sich ein anderer Spezialist mit Kaspersky Next Expert View verbunden hat. Wenn Sie eine Benachrichtigung über unzureichende Zugriffsrechte zum Aktualisieren der KPSN-Konfigurationsdatei sehen, wenden Sie sich an Ihren Administrator von Kaspersky Next Expert View (Rolle Hauptadministrator), um Hilfe zu erhalten: Bitten Sie den Administrator, sich mit Kaspersky Next Expert View zu verbinden. Wenn der Administrator eine Verbindung herstellt, wird die KPSN-Konfigurationsdatei aktualisiert. Sie können jederzeit überprüfen, ob die KPSN-Konfigurationsdatei aktuell ist. Klicken Sie dazu in Kaspersky Security Center im Abschnitt MDR auf die Registerkarte MDR-Nutzung. Es werden Informationen über die aktuelle Version der KPSN-Konfigurationsdatei angezeigt. Sobald eine neue Version der KPSN-Konfigurationsdatei verfügbar wird, können Sie die KPSN-Konfigurationsdatei über eine Schaltfläche aktualisieren. Wenn beim Aktualisieren ein unerwarteter Fehler auftritt, wenden Sie sich an den Technischen Support von Kaspersky.

Lösung für die Verwaltung Ihrer Assets	Schnittstelle, die Ihre SOC-Analysten verwenden	Erforderliche Maßnahmen
Kaspersky Next Expert View	MDR Web Console ODER Verwendung der API, um die Vorfälle herunterzuladen und sie anschließend im eigenen System zu verarbeiten	Melden Sie sich bei Kaspersky Next Expert View an. Starten Sie den Assistenten für die Erstkonfiguration, um das MDR-Plug-in zu aktivieren. Wenn Ihr Konto nicht über ausreichende Zugriffsrechte zum Aktivieren des MDR-Plug-ins verfügt, wenden Sie sich an den Administrator Ihres Kaspersky Next Expert View-Servers, um Hilfe zu erhalten. Folgen Sie anschließend den obigen Anweisungen für den Kaspersky Next Expert View-Server und das MDR-Plug-in. Wenn beim Aktualisieren ein unerwarteter Fehler auftritt, wenden Sie sich an den Technischen Support von Kaspersky.
Open Single Management Platform	In Open Single Management Platform installiertes MDR-Plug-in	Wenn sich ein MDR-Administrator bei der Open Single Management Platform anmeldet, muss er die neue KPSN-Vereinbarung akzeptieren. Die KPSN-Konfigurationsdatei wird automatisch aktualisiert, nachdem der Administrator die KPSN-Vereinbarung akzeptiert hat. Wenn die Vereinbarung nicht akzeptiert wurde, können Benutzer mit der Rolle MDR-Administrator sie später in der OSMP-Konsole akzeptieren. <i>So akzeptieren Sie die Vereinbarung und führen ein Update der KPSN-Konfigurationsdatei durch:</i> 1. Klicken Sie in der Konsolenoberfläche von OSMP im MDR-Abschnitt auf die Registerkarte MDR-Nutzung. 2. Erweitern Sie den Block KPSN-Konfigurationsdatei für die Integration mit dem KSC-Administrationsserver. 3. Aktivieren Sie die Option KPSN-Vereinbarung akzeptieren und klicken Sie auf KPSN-Konfigurationsdatei auf dem Administrationsserver anwenden. 4. Wenn Sie zusätzlich die Integration mit Kaspersky Endpoint Detection and Response Expert (lokal) konfiguriert haben, gehen Sie wie folgt vor: a. Erweitern Sie den Block KPSN-Konfigurationsdatei für die Integration mit KEDR Expert. b. Aktivieren Sie die Option KPSN-Vereinbarung akzeptieren und klicken Sie auf KPSN-Konfigurationsdatei für die Integration mit KEDR Expert anwenden.

Lösung für die Verwaltung Ihrer Assets	Schnittstelle, die Ihre SOC-Analysten verwenden	Erforderliche Maßnahmen
Lokal ausgeführtes Kaspersky Security Center ab Version 14	Im lokal ausgeführten Kaspersky Security Center installiertes MDR-Plug-in	Melden Sie sich bei Kaspersky Security Center an. Wenn Sie sich anmelden, wird je nach Version des MDR-Plug-ins entweder automatisch oder nachdem ein Benutzer mit der Rolle MDR-Administrator die neue KPSN-Vereinbarung akzeptiert hat ein Update der KPSN-Konfigurationsdatei durchgeführt. Wenn das MDR-Plug-in die Datei erfolgreich aktualisiert, erhalten Sie eine Benachrichtigung über die Änderung der KPSN-Konfigurationsdatei. Wenn das MDR-Plug-in die KPSN-Konfigurationsdatei nicht aktualisieren kann, erhalten Sie eine Benachrichtigung zur Ursache des Problems: - Ihr Konto verfügt nicht über ausreichende Zugriffsrechte, um die Datei zu aktualisieren. - Beim Aktualisieren der KPSN-Konfigurationsdatei ist ein unerwarteter Fehler aufgetreten. Wenn keine Benachrichtigungen angezeigt werden, wurde die KPSN-Konfigurationsdatei wahrscheinlich bereits erfolgreich aktualisiert, als sich ein anderer Spezialist mit Kaspersky Next Expert View verbunden hat. Wenn Sie eine Benachrichtigung über fehlende Zugriffsrechte zum Aktualisieren der KPSN-Konfigurationsdatei sehen, wenden Sie sich an Ihren Serveradministrator für Kaspersky Security Center, um Hilfe zu erhalten: Bitten Sie den Administrator, sich mit dem Server von Kaspersky Security Center zu verbinden. Wenn der Administrator eine Verbindung herstellt, wird die KPSN-Konfigurationsdatei aktualisiert. Wenn der Administrator die Benachrichtigung über die Änderung der KPSN-Konfigurationsdatei nicht erhält, sollte er die Version des installierten MDR-Plug-ins überprüfen und es gegebenenfalls auf die aktuelle Version aktualisieren (es ist MDR-Plug-in ab Version 2.1.17 erforderlich). Sie können jederzeit überprüfen, ob die KPSN-Konfigurationsdatei aktuell ist. Klicken Sie dazu in Kaspersky Security Center im Abschnitt MDR auf die Registerkarte MDR-Nutzung. Es werden Informationen zur aktuellen Version der KPSN-Konfigurationsdatei angezeigt. Wenn eine neue Version der KPSN-Konfigurationsdatei verfügbar ist, wird eine Schaltfläche zum Aktualisieren der KPSN-Konfigurationsdatei angezeigt. Wenn beim Aktualisieren ein unerwarteter Fehler auftritt, wenden Sie sich an den Technischen Support von Kaspersky.
Lokal ausgeführtes Kaspersky Security Center ab Version 14	MDR Web Console (MDR-Plug-in ist nicht im lokal ausgeführten Kaspersky Security Center installiert) ODER Sie verwenden die API, um die Vorfälle herunterzuladen und sie anschließend in Ihrem eigenen System zu verarbeiten	Bitten Sie den Administrator der MDR Web Console Folgendes zu tun: - Herunterladen des ZIP-Archivs von der Seite Lizenzierung. - Extrahieren der KPSN-Konfigurationsdatei aus dem zip-Archiv. - Versenden der Datei an den Administrator des Kaspersky Security Center Administrationsservers.
Lokal ausgeführtes Kaspersky Security Center bis einschließlich Version 13.*	Im lokal ausgeführten Kaspersky Security Center installiertes MDR-Plug-in ODER Sie verwenden die API, um die Vorfälle herunterzuladen und sie anschließend in Ihrem eigenen System zu verarbeiten	Bitten Sie den Serveradministrator von Kaspersky Security Center, die KPSN-Konfigurationsdatei hochzuladen, indem er auf Eigenschaften des Administrationsservers → Einstellungen des KSN-Proxyservers → Datei mit Einstellungen des KSN-Proxyservers klickt. Wenn beim Aktualisieren ein unerwarteter Fehler auftritt, wenden Sie sich an den Technischen Support von Kaspersky.

Wenn sich in Ihrem Netzwerk mehrere Server mit Kaspersky Security Center befinden, müssen Sie die KPSN-Konfigurationsdatei auf jedem der Server aktualisieren.

Aktualisieren der KPSN-Konfigurationsdatei auf KATA-Servern

Wenn sich in Ihrem Netzwerk KATA-Server befinden, die mit Kaspersky Managed Detection and Response verbunden sind, müssen Sie die MDR-Konfigurationsdatei auf diesen KATA-Servern aktualisieren.

Die Schritte zum Aktualisieren der MDR-Konfigurationsdatei hängen von der KATA-Version ab.

So aktualisieren Sie die MDR-Konfigurationsdatei auf KATA-Servern der Version 8.0–8.1:

1. Melden Sie sich mit dem Administratorkonto bei der KATA-Webschnittstelle an.
2. Wählen Sie den Abschnitt **Einstellungen** und den Unterabschnitt **KSN/KPSN und MDR** aus.
3. Klicken Sie unter **MDR-Integration** auf **Erneut anmelden**.
4. Geben Sie im folgenden Fenster Ihre Anmeldeinformationen für Kaspersky Account ein.

Nach erfolgreicher Überprüfung der Anmeldeinformationen wird die MDR-Konfigurationsdatei automatisch auf dem Server aktualisiert.

So aktualisieren Sie die MDR-Konfigurationsdatei auf KATA-Servern der Version 7.1 und älter:

1. Melden Sie sich mit dem MDR-Administratorkonto an der MDR-Konsole an.
2. Laden Sie das ZIP-Archiv mit der MDR-Konfiguration von der Seite **Getting Started** herunter:
<https://mdr.kaspersky.com/guide>.
3. Melden Sie sich mit dem Administratorkonto bei der KATA-Webschnittstelle an.
4. Wählen Sie den Abschnitt **Einstellungen** und den Unterabschnitt **KSN/KPSN und MDR** aus.
5. Klicken Sie im Bereich **MDR-Integration** auf **Hochladen**, um die Konfigurationsdatei hochzuladen.
Daraufhin wird das Fenster zur Dateiauswahl geöffnet.
6. Wählen Sie das von der MDR Web Console heruntergeladene Archiv aus und klicken Sie auf **Öffnen**.

Die MDR-Konfigurationsdatei wird auf dem Server aktualisiert.

Falls beim Update der MDR-Konfigurationsdatei Probleme auftreten, kann sich der Administrator des KATA-Servers an den Technischen Support von Kaspersky wenden, um eine Anleitung zum Aktualisieren der MDR-Konfigurationsdatei auf dem KATA-Server zu erhalten.

MDR-Lösung auf den Betrieb ohne KPSN-Konfigurationsdateien umstellen

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Die MDR-Lösung muss in den folgenden Szenarien die KPSN-Konfiguration verwenden:

- Um sicherzustellen, dass KSN-Abfrage- und Statistikdaten nie in eine andere Region übertragen werden. Ohne KPSN-Konfiguration stellt Kaspersky nur sicher, dass die Daten in die angegebene Region übertragen werden. Weitere Informationen dazu finden Sie in diesem Artikel: [KPSN-Konfigurationsdateien regelmäßig aktualisieren](#).
- Um die Ausführung der MDR-Lösung sicherzustellen, wenn auf einem Ihrer Geräte eine veraltete EPP-Anwendung installiert ist.

Sie können die MDR-Lösung auf die Ausführung ohne KPSN-Konfigurationsdateien umstellen, wenn folgende Voraussetzungen erfüllt sind:

1. Auf allen Ihren Assets sind EPP-Anwendungen in den Versionen installiert, die eine KPSN-freie Ausführung unterstützen:

- Kaspersky Endpoint Security für Windows Version 12.6 oder höher
- Kaspersky Endpoint Security für Windows Version 12.6 oder höher in der Konfiguration als Endpoint Detection and Response Agent
- Kaspersky Endpoint Security für Windows Light Agent Version 12.8 oder höher
- Kaspersky Endpoint Security für Linux Version 12.3 oder höher
- Kaspersky Endpoint Security for Mac 12.2 oder höher
- Kaspersky Embedded Systems Security für Windows Version 4.0 oder höher
- Kaspersky Embedded Systems Security für Linux Version 4.0 oder höher
- Kaspersky Industrial CyberSecurity for Nodes Windows 4.5

2. Die MDR-Lösung wird auf allen Ihren Assets mit einem Aktivierungscode oder einer BLOB-Datei aktiviert, die nicht vor dem 1. Januar 2024 erstellt wurde.

BLOB-Dateien, die ab dem 01.01.2024 erstellt wurden, enthalten Daten, die für die KPSN-freie Ausführung notwendig sind.

Es wird empfohlen, zur Aktivierung der MDR-Lösung für EPP-Anwendungen, welche dies unterstützen, einen Aktivierungscode zu verwenden. Einige EPP-Anwendungen unterstützen die Ausführung ohne KPSN nicht, wenn Sie die MDR-Lösung mit einer Schlüsseldatei aktivieren. Details finden Sie im folgenden Artikel: [Hardware- und Softwareanforderungen](#).

So stellen Sie die MDR-Lösung auf die KPSN-freie Ausführung um:

1. [Erstellen und überprüfen Sie in Kaspersky Security Center einen Bericht über Versionen der Kaspersky-Programme](#).

2. Aktualisieren Sie EPP-Anwendungen entsprechend den Anforderungen:

- Kaspersky Endpoint Security für Windows Version 12.6 oder höher
- Kaspersky Endpoint Security für Windows Version 12.6 oder höher, im Modus als Endpoint Detection and Response Agent (erfordert die Installation einer BLOB-Datei)

- Kaspersky Endpoint Security für Windows Light Agent Version 12.8 oder höher
- Kaspersky Endpoint Security für Linux Version 12.3 oder höher
- Kaspersky Endpoint Security for Mac 12.2 oder höher
- Kaspersky Embedded Systems Security für Windows Version 4.0 oder höher
- Kaspersky Industrial CyberSecurity for Nodes Windows 4.5

3. Deaktivieren Sie im Administrationsserver die Verwendung von KPSN.

- In Kaspersky Security Center mit verwendetem MDR-Plug-in:

1. Stellen Sie sicher, dass das MDR-Plug-in auf Version 2.5.1 aktualisiert ist.
2. Klicken Sie im Fenster von Kaspersky Security Center im Abschnitt MDR auf die Registerkarte **MDR-Nutzung**.
3. Erweitern Sie den Block **KPSN** und klicken Sie auf **KPSN deaktivieren**.

- In Kaspersky Security Center ohne verwendetem MDR-Plug-in:

1. Klicken Sie im Hauptmenü, neben dem Namen des gewünschten Administrationsservers, auf das Einstellungen-Symbol ()
 2. Das Eigenschaftfenster des Administrationsservers wird geöffnet.
 3. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt "KSN Proxy-Einstellungen" aus.
 4. Deaktivieren Sie die Option **Kaspersky Private Security Network verwenden**.
 5. Aktivieren Sie die Option **KSN Proxy auf dem Administrationsserver aktivieren**.
4. Wenn Sie Assets aus einem Betriebssystem-Image bereitstellen, aktualisieren Sie das Image, sodass die EPP-Anwendung keine KPSN-Konfiguration verwendet.
5. Bearbeiten Sie die Richtlinien für EPP-Anwendungen (erforderlich sowohl für die Verwendung des Aktivierungscodes als auch für die Verwendung der BLOB-Datei).
1. Deaktivieren Sie die Verwendung von Kaspersky Security Network und speichern Sie die Richtlinie. Weitere Informationen finden Sie in diesem Artikel: [Kaspersky Security Network konfigurieren](#) ².
 2. Wenn die EPP-Anwendung nur mit einer BLOB-Datei aktiviert werden kann, [laden Sie die MDR-Konfigurationsdatei herunter](#) und laden Sie die BLOB-Datei in die Richtlinie hoch.
 3. Aktivieren Sie wieder die Verwendung von Kaspersky Security Network und akzeptieren Sie die KSN-Vereinbarung. Stellen Sie sicher, dass in den Richtlinieneinstellungen die Option "Erzwingen" aktiviert ist.

Dashboards für die Überwachung in der MDR Web Console

Die MDR Web Console bietet Dashboards zur Überwachung, mit denen zusammenfassende Informationen angezeigt werden können.

So zeigen Sie Dashboards an:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Monitoring**.

Die Seite **Summary** wird geöffnet.

2. Die folgenden Dashboards sind auf der Seite **Summary** vorhanden:

- **Number of connected assets**

Dieser Abschnitt zeigt die Anzahl der verbundenen Assets im Vergleich zur Zielanzahl der Assets.

- **Assets by status**

Dies ist ein Kreisdiagramm, das die Verteilung der Assets nach ihrem Status zeigt.

- **Active incidents**

Dies ist ein Kreisdiagramm, das die Verteilung der aktiven Vorfälle nach ihrem Status zeigt.

- **Responses**

Dies ist ein Kreisdiagramm, das die Verteilung der Reaktionen nach ihrem Status zeigt.

Die Anzahl der verbundenen Assets stellt die Assets dar, die innerhalb der letzten 7 Tagen von der MDR Web Console gesehen wurden. Wenn Sie die Anzahl der verbundenen **Assets** für den bestimmten Zeitraum abrufen möchten, navigieren Sie zum Menüpunkt Assets der MDR Web Console.

- **Telemetry statistics**

Dieses Dashboard zeigt die Telemetrie-Statistiken der MDR-Lösung für einen Client, inklusive Statistiken nach bestimmten Mandanten, an. Sie können die Daten für 1, 7, 30, 90 oder 180 Tage, für 1 Jahr oder für den gesamten zusammenhängenden Nutzungszeitraum der MDR-Lösung auf einem Client anzeigen.

Das Dashboard zeigt die Anzahl für jedes der folgenden Objekte an:

- *Telemetry events** sind alle Ereignisse, die von den Assets eines Clients an Kaspersky Managed Detection and Response gesendet werden.
- *Suspicious events* sind Telemetrie-Ereignisse, die von Kaspersky Managed Detection and Response als Ereignisse eingestuft werden, die eine zusätzliche Überprüfung erfordern.
- *Security events* sind Telemetrie-Ereignisse, die von Erkennungsregeln als potenzielle Vorfälle eingestuft werden.

- *Incidents* sind Vorgänge, die von der Erkennungstechnologie als „Kritisch“ eingestuft werden. Vorfälle erfordern eine sofortige Reaktion (Reaktionsmaßnahme) von Kaspersky Managed Detection and Response.
- *Detection rules triggered* zeigen die Anzahl eindeutiger Erkennungsregeln, die bei bestimmten Telemetrie-Ereignissen innerhalb einem bestimmten Zeitraum ausgelöst wurden.

Dashboards werden bei jeder Aktualisierung der Seite **Summary** aktualisiert.

So zeigen Sie in Dashboards die Statistiken für bestimmte Mandanten an:

1. Klicken Sie im oberen Bereich der Seite **Summary** auf **Filter**.
2. Wählen Sie im neuen Menü mindestens einen Mandanten aus.
3. Klicken Sie auf die Schaltfläche **Save**.

Die Statistiken für bestimmte Mandanten sind in den folgenden Widgets verfügbar:

- **Assets limit for this license**
- **Assets by status**
- **Active incidents**
- **Incidents**
- **Responses**
- **Telemetry statistics**

Zusammenfassende Informationen erhalten

Kaspersky Managed Detection and Response bietet verschiedene Arten von zusammenfassenden Informationen, die Sie per E-Mail erhalten können. In diesem Abschnitt wird beschrieben, wie Sie das Erhalten von zusammenfassenden Informationen konfigurieren.

Zusammenfassung aller Assets als CSV-Datei abrufen (MDR Web Console)

Sie können eine Zusammenfassung als CSV-Datei abrufen, die alle Assets Ihres Benutzerkontos umfasst. Auf die Zusammenfassung werden keine Filter angewendet, d. h. die Anzahl der Assets in dieser Zusammenfassung stellt alle Assets dar, die in der MDR Web Console angezeigt wurden.

Sie können Assets mit dem Status **Abwesend** in der Zusammenfassung ausblenden, indem Sie das entsprechende Kontrollkästchen in den **Einstellungen** aktivieren.

So erhalten Sie eine csv-Zusammenfassung:

1. Navigieren Sie im Fenster der MDR Web Console zum Menüpunkt **Assets**.

Die Asset-Liste wird geöffnet.

2. Klicken Sie im oberen Teil des Fensters auf die Schaltfläche **Receive a CSV summary by email**.

Die Zusammenfassung wird an die E-Mail-Adresse gesendet, die im Rahmen der Aktivierung von Kaspersky Managed Detection and Response angegeben wurde.

Informationen zu Vorfällen als PDF abrufen (MDR Web Console)

Sie können zusammenfassende Informationen über einen bestimmten Vorfall als PDF abrufen.

So rufen Sie eine pdf-Zusammenfassung ab:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Incidents**.

Die Vorfall-Liste wird geöffnet.

2. Klicken Sie auf den Vorfall dessen Zusammenfassung Sie abrufen möchten.

Die Vorfall-Karte wird angezeigt.

3. Klicken Sie im oberen Teil des Fensters auf den Link **Receive a PDF by email** erhalten.

Die Zusammenfassung wird an die E-Mail-Adresse gesendet, die im Rahmen der Aktivierung von Kaspersky Managed Detection and Response angegeben wurde.

Regelmäßige Zustellung von Berichten in der MDR Web Console einrichten

Diese Funktion steht nur in der MDR Web Console zur Verfügung.

Für zusammenfassende Berichte, die Daten über offene Vorfälle enthalten, können Sie die Zustellungen planen. Dabei wird für jede konfigurierte Zustellung ein Zeitplan gespeichert. Sie können für eine Organisation maximal 50 und für jeden Mandanten maximal 10 Zeitpläne erstellen.

Um Zeitpläne für die Zustellung von Berichten zu erstellen oder zu bearbeiten, müssen Sie über die Benutzerrolle [MDR-Administrator](#) verfügen.

Der Bericht wird nach dem festgelegten Zeitplan per E-Mail als offene, unverschlüsselte pdf-Datei an die angegebenen Adressen gesendet.

Der Bericht enthält immer die Daten der letzten sieben Tage, wobei der Tag der Berichtserstellung nicht berücksichtigt wird. Wenn Sie den Zeitplan z. B. so einrichten, dass Sie den zusammenfassenden Bericht jeden Tag erhalten, enthält der tägliche Bericht die Daten für die letzten sieben Tage, ohne den aktuellen Tag. Wenn Sie den Zeitplan so einrichten, dass Sie den zusammenfassenden Bericht jeden Mittwoch erhalten, enthält Ihr Bericht die Daten vom Mittwoch letzter Woche bis zum Dienstag der aktuellen Woche.

So richten Sie die Zustellung des zusammenfassenden Berichts als PDF-Datei ein:

1. Klicken Sie in der MDR Web Console im Abschnitt **Settings** auf die Registerkarte **Schedules**.
2. Klicken Sie auf die Schaltfläche **Add**.
Das Fenster **Add new schedule** wird geöffnet.
3. Setzen Sie den Umschalter auf die Position **Enabled**.
4. Lesen Sie sorgfältig den unten stehenden Hinweis mit den Bedingungen für den Versand von zusammenfassenden Berichten. Aktivieren Sie anschließend das Kontrollkästchen, um zu bestätigen, dass Sie die Nutzungsbedingungen gelesen und verstanden haben. Wenn das Kontrollkästchen nicht aktiviert ist, können Sie die vorgenommenen Änderungen nicht speichern.
5. Legen Sie die folgenden Einstellungen fest:
 - Geben Sie im Feld **Schedule name** einen beliebigen, lesbaren Namen für den zusammenfassenden Bericht an. Der Name kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten und darf höchstens 1000 Zeichen lang sein.
 - Wählen Sie im Feld **Tenant** den Mandanten aus, für den Sie einen zusammenfassenden Bericht zustellen möchten. Der Bericht enthält nur die Daten des ausgewählten Mandanten. Wenn Sie alternativ einen zusammenfassenden Bericht über alle Mandanten zustellen möchten, wählen Sie **All tenants**.

- Geben Sie im Feld **To emails** eine E-Mail-Adresse oder eine durch Kommas getrennte Liste mit E-Mail-Adressen der Benutzer an, welche die Zusammenfassung erhalten sollen.

Vergewissern Sie sich, dass die eingegebenen E-Mail-Adressen korrekt sind, da diese ohne weitere Bestätigung hinzugefügt werden. Die zusammenfassenden Berichte können vertrauliche Daten enthalten und werden im offenen und unverschlüsselten PDF-Format gesendet.

- Wählen Sie im Feld **Sending day** den Wochentag aus, an dem die Zusammenfassung an die angegebenen E-Mail-Adressen gesendet werden soll. Sie können einen bestimmten Tag oder **Every day** auswählen.
- Geben Sie im Feld **Time, UTC** eine Uhrzeit im 24-Stunden-UTC-Format an., Beispiel: 15:00.

Der Zeitplan bezieht sich nur auf den Zeitpunkt des Berichtsversands aus, nicht auf den Zeitraum der im Bericht enthaltenen Daten.

Der Bericht enthält immer die Daten der letzten sieben Tage, wobei der Tag der Berichtserstellung nicht berücksichtigt wird. Wenn Sie den Zeitplan z. B. so einrichten, dass Sie den zusammenfassenden Bericht jeden Tag erhalten, enthält der tägliche Bericht die Daten für die letzten sieben Tage, ohne den aktuellen Tag. Wenn Sie den Zeitplan so einrichten, dass Sie den zusammenfassenden Bericht jeden Mittwoch erhalten, enthält Ihr Bericht die Daten vom Mittwoch letzter Woche bis zum Dienstag der aktuellen Woche.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Der zusammenfassende Bericht wird wöchentlich oder täglich an die angegebenen E-Mail-Adressen gesendet.

Benachrichtigungen empfangen

Sie können die Zustellung von Ereignisbenachrichtigungen konfigurieren, die bei Vorfällen und Reaktionen während ihrer Verarbeitung in Kaspersky Managed Detection and Response auftreten.

Je nach den von Ihnen angegebenen Einstellung versendet Kaspersky Managed Detection and Response Benachrichtigungen per Telegram oder E-Mail an die Clients. Die Benachrichtigung beinhaltet eine Beschreibung des Ereignisses und einen Link zu dem Objekt, auf dem das Ereignis aufgetreten ist.

Die Benachrichtigungen können Sie in MDR Web Console konfigurieren.

Benachrichtigungen in der MDR Web Console einrichten

So konfigurieren Sie die Zustellung von Benachrichtigungen in der MDR Web Console:

1. Klicken Sie in der MDR Web Console im Abschnitt **Settings** auf die Registerkarte **Notification settings**.
2. Wählen Sie die Kontrollkästchen der Ereignisse aus, für die Sie Benachrichtigungen per E-Mail oder Telegram erhalten möchten.

Verfügbare Kontrollkästchen:

- **All** – Alle Ereignisse, für die Kaspersky Managed Detection and Response Benachrichtigungen versendet.
 - **Incidents** – Benachrichtigungen über das Erstellen, Aktualisieren, Beheben und Schließen von Vorfällen.
 - **Extended notifications** – Eine Beschreibung des als Vorfall erkannten Angriffs und die darauf empfohlene Reaktion. Dieses Kontrollkästchen ist verfügbar, wenn die Funktion für erweiterte Benachrichtigungen [auf der Registerkarte General settings aktiviert ist](#). Diese Benachrichtigungen können nur in der MDR Web Console aktiviert werden, nicht jedoch im MDR-Plug-in.
 - **Comments** – Benachrichtigungen über das Erstellen, Aktualisieren und Löschen von Kommentaren in Vorfällen.
 - **Responses** – Benachrichtigungen über das Erstellen, Annehmen und Ablehnen von Reaktionen.
 - **Information on license expiration** – Benachrichtigungen über die folgenden Ereignisse: die Lizenz läuft in weniger als 30 Tagen ab, die Lizenz ist abgelaufen. Kaspersky Managed Detection and Response sendet diese Benachrichtigungen täglich bis zum Ablauf oder einer Verlängerung der Lizenz.
3. Klicken Sie über den Kontrollkästchen auf die Schaltfläche **Subscribe**, um Benachrichtigungen von dem Telegram-Chatbot zu abonnieren. Durch das Klicken auf die Schaltfläche **Subscribe** wird vom Programm ein individueller Link generiert und angezeigt. Verwenden Sie diesen Link, um in Telegram den Chatbot zu aktivieren. Sie können diesen Link nur für ein einziges Telegram-Konto verwenden.

Verwenden Sie diesen Link nur auf einem Gerät (Desktop oder Mobilgerät), auf dem die Telegram-App installiert ist. In der Web-Version von Telegram kann der Link den Chatbot nicht aktivieren.

Wenn Sie Benachrichtigungen an ein weiteres Telegram-Konto erhalten möchten, klicken Sie auf die Schaltfläche **Unsubscribe** und wiederholen Sie den Abonnement-Vorgang, um einen neuen Link zu generieren und den Chatbot für ein weiteres Konto zu aktivieren.

4. Klicken Sie im unteren Bereich des Fensters auf die Schaltfläche **Save**, um die Einstellungen zu speichern. Die Schaltfläche **Save** wird erst aktiv, wenn Sie Einstellungen geändert haben.

Die Zustellung von Benachrichtigungen ist konfiguriert.

Benachrichtigungen zum Asset-Status

Sie können die Zustellung von Benachrichtigungen konfigurieren, wenn die Anzahl der Assets mit einem bestimmten Status einen Schwellenwert überschreitet.

Mit Benachrichtigungen zum Asset-Status können Sie zeitnah Informationen zu folgenden Problemen erhalten:

- Rückgang der MDR-Überwachungsabdeckung
- Probleme bei der Verbindung von Assets mit MDR
- Massenhafter Wechsel von Assets in den Warnstatus oder kritischen Status

Details zu Asset-Status finden Sie im folgenden Artikel: [Asset-Status](#).

Funktionsweise automatischer Benachrichtigungen

Für jeden der unten aufgeführten Status können Sie einen Schwellenwert als Prozentsatz der Gesamtzahl der Assets festlegen. Wenn der Schwellenwert überschritten wird, wird eine Benachrichtigung gesendet.

Status	Bedingung
OK	Die Anzahl der Assets liegt unter dem Schwellenwert.
Warnung	Die Anzahl der Assets liegt über dem Schwellenwert.
Kritisch	Die Anzahl der Assets liegt über dem Schwellenwert.
Autonom	Die Anzahl der Assets liegt über dem Schwellenwert.

Automatische Asset-Prüfungen werden in einem Intervall von 1 Stunde ausgeführt.

Benachrichtigungen werden separat für jeden Mandanten gesendet, der seine Schwellenwerte überschreitet. Eine Benachrichtigung für einen bestimmten Status wird pro Mandant höchstens einmal pro Tag gesendet.

Nur Benutzer, die Zugriff auf den Mandanten mit überschrittenen Schwellenwerten haben und Benachrichtigungen in ihren Benutzereinstellungen aktiviert haben, erhalten die Benachrichtigungen.

Konfigurieren von Benachrichtigungsregeln durch den MDR-Administrator

Zum Einrichten von Benachrichtigungen über den Asset-Status ist die Rolle des MDR-Administrators erforderlich.

So konfigurieren Sie Regeln für Asset-Status-Benachrichtigungen:

1. Wechseln Sie in der MDR-Konsole zu **Einstellungen** → **Allgemeine Einstellungen**.
2. Aktivieren Sie eine oder beide der folgenden Optionen:
 - **Erweiterte Benachrichtigungen per E-Mail erhalten**
 - **Erweiterte Benachrichtigungen per Telegram erhalten**
3. Aktivieren Sie den Parameter **Benachrichtigungen über Änderungen des Asset-Status aktivieren**.

Der Bereich **Basisregel** kann nun bearbeitet werden und enthält die Einstellungen der Benachrichtigungsregel. Sie können zusätzliche Regeln hinzufügen (z. B. für eine andere Gruppe von Mandanten), indem Sie unter dem Bereich **Basisregel** auf die Schaltfläche **Regel hinzufügen** klicken.
4. Wählen Sie im Bereich die Mandanten aus, für die die Regel gelten soll, oder aktivieren Sie **Auf alle Mandanten anwenden**.
5. Legen Sie Schwellenwerte für Asset-Status fest oder behalten Sie die Standardwerte bei.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Regel wurde nun erstellt und ist aktiv. Um Benachrichtigungen zu erhalten, müssen MDR-Benutzer Benachrichtigungen über den Asset-Status wie unten beschrieben konfigurieren.

Konfigurieren von Benachrichtigungen über den Asset-Status durch MDR-Benutzer

So erhalten Sie Benachrichtigungen über den Asset-Status:

1. Wechseln Sie in der MDR-Konsole zu **Einstellungen** → **Benachrichtigungseinstellungen**.
2. Aktivieren Sie **Benachrichtigungen über den Asset-Status**.
3. Klicken Sie auf die Schaltfläche **Speichern**.

Sie erhalten nun gemäß den konfigurierten Regeln Benachrichtigungen über den Asset-Status für die Mandanten, auf die Sie Zugriff haben.

Erweiterte Benachrichtigungen erhalten

Sie können die Zustellung von erweiterten Vorfallbenachrichtigungen an MDR-Benutzer per E-Mail oder Telegram konfigurieren. Die erweiterten Benachrichtigungen enthalten eine Beschreibung des als Vorfall erkannten Angriffs und Empfehlungen zur Reaktion. Die Beschreibung des Angriffs enthält Informationen, welche die MDR-Lösung im Rahmen der Telemetriedaten von den Geräten empfängt, die mit der MDR-Lösung verbunden sind. Die Beschreibung kann daher die folgenden vertraulichen Informationen enthalten:

- Hostnamen
- IP-Adressen der Hosts

- Namen von Benutzerkonten
- Kennwörter von Benutzerkonten (wenn auf einem Gerät ein Skript ausgeführt wurde, das ein Kennwort enthält)
- URLs von Diensten
- Dateinamen
- E-Mail-Adressen
- Namen von Abteilungen und Mandanten

Die vollständige Liste der von der MDR-Lösung empfangenen Daten finden Sie im Abschnitt [Bereitstellung von Daten](#).

Erweiterte Benachrichtigungen in der MDR Web Console aktivieren

So aktivieren Sie die Zustellung der erweiterten Benachrichtigungen:

1. Klicken Sie in der MDR Web Console im Abschnitt **Settings** auf die Registerkarte **General settings**.
2. Aktivieren Sie mindestens eine der beiden Optionen:
 - **Enable extended email notification**
 - **Enable extended Telegram notification**
3. Aktivieren Sie das Kontrollkästchen im unteren Bereich, um zu bestätigen, dass Sie die Bedingungen für den Versand erweiterter Benachrichtigungen gelesen und verstanden haben.
4. Klicken Sie auf **Save**.

Jetzt können Sie in den **Notification settings** der MDR Web Console die erweiterten Benachrichtigungen [abonnieren](#).

Benutzer verwalten

Die Benutzer von Kaspersky Managed Detection and Response können unterschiedliche Rollen innehaben, wobei für jede Rolle unterschiedliche Funktionen verfügbar sind. Das *Rollenmodell* ist ein Satz von Regeln, welche die Benutzerrollen festlegen.

Die folgenden Rollen sind in Kaspersky Managed Detection and Response verfügbar:

MDR Administrator

Der Superuser mit Zugriff auf alle Funktionen von Kaspersky Managed Detection and Response, die von der Lizenz gewährt werden. Der MDR-Administrator kann anderen Benutzern den Zugriff auf die Client-Datenquellen gewähren. Wenn Sie Kaspersky Managed Detection and Response aktivieren, werden Sie automatisch zum MDR-Administrator. Aus diesem Grund wird empfohlen, für den Aktivierungsprozess die E-Mail-Adresse des Unternehmens anstelle einer persönlichen E-Mail-Adresse zu verwenden. Wenn der MDR-Administrator mit einer persönlichen E-Mail-Adresse erstellt wird, kann dies ein Sicherheitsrisiko darstellen, z. B. falls das Konto des MDR-Administrators gestohlen wird.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	✓	—
Verwaltung von Reaktionen	✓	—
Verwaltung von Mandanten	✓	—
Planung einer Zusammenfassung des Vorfalls	✓	—
Zugriff auf REST-API	✓	—

Senior Security Officer

Ein Mitarbeiter, der Zugriff auf die durch die Lizenz gewährten Funktionen von Kaspersky Managed Detection and Response hat. Er hat jedoch keinen Zugriff auf die REST-API. Der Senior Security Officer hat das Recht, [Reaktionen](#) zu akzeptieren und abzulehnen.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	✓	—
Verwaltung von Reaktionen	✓	—
Verwaltung von Mandanten	—	✓
Planung einer Zusammenfassung des Vorfalls	—	✓
Zugriff auf REST-API	—	✓

Security Officer

Ein Mitarbeiter, der Zugriff auf die durch die Lizenz gewährten Funktionen von Kaspersky Managed Detection and Response hat. Er hat jedoch keinen Zugriff auf die REST-API. Der Security Officer kann [Reaktionen](#) weder akzeptieren noch ablehnen.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	—	✓
Verwaltung von Reaktionen	—	✓
Verwaltung von Mandanten	—	✓
Planung einer Zusammenfassung des Vorfalls	—	✓
Zugriff auf REST-API	—	✓

Neue Benutzer über die MDR Web Console einladen

So laden Sie einen neuen Benutzer zu Kaspersky Managed Detection and Response ein:

Sollte Ihr zuvor erstellter [Kaspersky Account](#) (d. h. Ihre E-Mail-Adresse) bereits für den Zugriff auf Kaspersky Managed Detection and Response verwendet wurden sein, ist er möglicherweise mit den MDR-Daten eines anderen Unternehmens verknüpft und für die Anwendung eines neuen Aktivierungscode nicht verfügbar. Um Ihren vorhandenen Kaspersky Account für die neue Aktivierung zu verwenden, wenden Sie sich an den [Technischen Support](#).

Bitte beachten Sie: Wenn der Technische Support die Verknüpfung Ihres bestehenden Kaspersky Accounts mit den MDR-Daten einer anderen Organisation aufhebt, kann Ihr vorhandener Kaspersky Account nicht mehr für den Zugriff auf die Daten der anderen Organisation verwendet werden, für die es zuvor verwendet wurde.

1. Navigieren Sie im Fenster der MDR Console zum Menüpunkt **Settings**.

Die Benutzerliste wird geöffnet.

2. Klicken Sie über der Benutzerliste auf die Schaltfläche **Add**.

Die Einladungskarte wird angezeigt.

3. Geben Sie im Feld **Email** eine E-Mail-Adresse an.

4. Geben Sie im Feld **User role** für den neuen Benutzer an.

Folgende Benutzerrollen stehen zur Verfügung:

MDR Administrator

Der Superuser mit Zugriff auf alle Funktionen von Kaspersky Managed Detection and Response, die von der Lizenz gewährt werden. Der MDR-Administrator kann anderen Benutzern den Zugriff auf die Client-Datenquellen gewähren. Wenn Sie Kaspersky Managed Detection and Response aktivieren, werden Sie automatisch zum MDR-Administrator. Aus diesem Grund wird empfohlen, für den Aktivierungsprozess die E-Mail-Adresse des Unternehmens anstelle einer persönlichen E-Mail-Adresse zu verwenden. Wenn der MDR-Administrator mit einer persönlichen E-Mail-Adresse erstellt wird, kann dies ein Sicherheitsrisiko darstellen, z. B. falls das Konto des MDR-Administrators gestohlen wird.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	✓	—
Verwaltung von Reaktionen	✓	—
Verwaltung von Mandanten	✓	—

Funktionsbereich	Erlauben	Verweigern
Planung einer Zusammenfassung des Vorfalls	✓	—
Zugriff auf REST-API	✓	—

Nur ein Benutzer, dem selbst die [Rolle](#) als **MDR Administrator** zugewiesen wurde, kann die Rolle **MDR Administrator** auch neuen Benutzern zuweisen.

Senior Security Officer

Ein Mitarbeiter, der Zugriff auf die durch die Lizenz gewährten Funktionen von Kaspersky Managed Detection and Response hat. Er hat jedoch keinen Zugriff auf die REST-API. Der Senior Security Officer hat das Recht, [Reaktionen](#) zu akzeptieren und abzulehnen.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	✓	—
Verwaltung von Reaktionen	✓	—
Verwaltung von Mandanten	—	✓
Planung einer Zusammenfassung des Vorfalls	—	✓
Zugriff auf REST-API	—	✓

Security Officer

Ein Mitarbeiter, der Zugriff auf die durch die Lizenz gewährten Funktionen von Kaspersky Managed Detection and Response hat. Er hat jedoch keinen Zugriff auf die REST-API. Der Security Officer kann [Reaktionen](#) weder akzeptieren noch ablehnen.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	—	✓
Verwaltung von Reaktionen	—	✓
Verwaltung von Mandanten	—	✓
Planung einer Zusammenfassung des Vorfalls	—	✓
Zugriff auf REST-API	—	✓

5. Wählen Sie bei Bedarf den Wert (oder die Werte) in der Dropdown-Liste **Tenant** aus.

Es werden bereits vorhandene Mandanten und der Wert **Root tenant** vorgeschlagen.

Der Benutzer kann nur die Assets und Vorfälle anzeigen, die sich auf die angegebenen Mandanten beziehen. Wenn Sie über Assets und Vorfälle verfügen, die keinem Mandanten zugewiesen sind, kann der Benutzer diese anzeigen, wenn Sie den Wert **Root tenant** auswählen.

Sie können den Wert **Root tenant** zusätzlich zu angegebenen Namen der Mandanten auswählen.

6. Klicken Sie auf **Invite**.

Die Einladungskarte wird ausgeblendet.

Geben Sie die E-Mail-Adresse ein. Die E-Mail-Adresse muss zunächst auf dem Web-Portal auth.hq.uis.kaspersky.com registriert und verifiziert werden.

Eine Nachricht mit dem Einladungslink wird von noreply@mail.account.uis.kaspersky.com an die angegebene E-Mail-Adresse gesendet.

Der eingeladene Benutzer muss seine E-Mail-Adresse bestätigen, indem er dem Link aus der Nachricht folgt. Der Benutzer kann sich erst dann anmelden und Kaspersky Managed Detection and Response verwenden, wenn seine E-Mail-Adresse überprüft wurde. Der Benutzerrolle entsprechende Berechtigungen werden nach der ersten Anmeldung des Benutzers erteilt.

Benutzerrollen in der MDR Web Console ändern

Sie können die Rolle für einen bestehenden Benutzer ändern. Beispielsweise kann ein Mitarbeiter mit der zugewiesenen Rolle "Security Officer" zusätzliche Verantwortlichkeiten bekommen, welche die Zuweisung der Rolle "Senior Security Officer" erfordern.

So ändern Sie eine Rolle für einen vorhandenen Benutzer:

1. Navigieren Sie im Fenster der MDR Console zum Menüpunkt **Settings**.

Die Benutzerliste wird geöffnet.

2. Klicken Sie auf die Zeichenfolge mit dem Benutzer, dessen Rolle Sie ändern möchten.

Die Benutzerkarte wird angezeigt.

3. Ändern Sie in der Benutzerkarte die Rolle für den vorhandenen Benutzer, indem Sie eine andere Rolle aus der Dropdown-Liste der Rollen auswählen.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Rolle für den bestehenden Benutzer wird geändert.

Methoden zur Benachrichtigung der Benutzer in der MDR Web Console bearbeiten

Das Bearbeiten der Methoden zur Benachrichtigung der Benutzer steht nur dem Benutzer zur Verfügung, dem die [Rolle](#) MDR-Administrators zugewiesen wurde. Der Benutzer mit dieser Rolle kann die Benachrichtigungseinstellungen für alle Benutzer mit dem Status „Aktiv“, einschließlich sich selbst, bearbeiten.

Benutzer mit dem Status "Aktiv" können Benachrichtigungen von Kaspersky Managed Detection and Response per E-Mail und/oder Telegram erhalten.

So bearbeiten Sie die Methoden zur Benachrichtigung für einen vorhandenen Benutzer:

1. Navigieren Sie im Fenster der MDR Console zum Menüpunkt **Settings**.

Die Benutzerliste wird geöffnet.

2. Klicken Sie auf die Zeichenfolge mit dem Benutzer, dessen Benachrichtigungsmethoden Sie ändern möchten.

Die Benutzerkarte wird angezeigt.

3. Geben Sie in der Benutzerkarte die folgenden Optionen an:

- **Email notifications enabled**

Der Benutzer erhält Benachrichtigungen an die E-Mail-Adresse, die bei der Einladung dieses Benutzers angegeben wurde.

- **Telegram notifications enabled**

Der Benutzer erhält Benachrichtigungen vom Telegram-Chatbot.

Wenn Benutzer ihren Zugriff auf das Telegram-Konto verloren haben, aktivieren Sie das Kontrollkästchen **Unsubscribe Telegram account from notifications**. Bitten Sie anschließend die Benutzer, sich an der MDR Web Console anzumelden, den Abschnitt **Settings** → **Notification settings** aufzurufen und anschließend den Abonnement-Vorgang zu wiederholen. Dadurch wird ein neuer Link generiert, mit dem das Telegram-Abonnement für ein anderes Telegram-Konto aktiviert wird.

4. Klicken Sie im unteren Teil der Benutzerkarte auf die Schaltfläche **Save**, um die Karte zu schließen.

Die Methoden zur Benachrichtigung des Benutzer werden bearbeitet und gespeichert.

Benutzerzugriff auf Mandanten in der MDR Web Console bearbeiten

Sie können den Benutzerzugriff auf die Mandanten in Ihrem Konto ändern. Das kann beispielsweise erforderlich sein, wenn Sie einen neuen Mandanten hinzufügen und möchten, dass ein vorhandener Benutzer darauf zugreifen kann.

So ändern Sie den Zugriff auf Mandanten:

1. Navigieren Sie im Fenster der MDR Console zum Menüpunkt **Settings**.

Die Benutzerliste wird geöffnet.

2. Klicken Sie auf die Zeichenfolge mit dem Benutzer, dessen Zugriffsrechte Sie ändern möchten.

Die Benutzerkarte wird angezeigt.

3. Ändern Sie den Wert (oder die Werte) auf der Benutzerkarte in der Dropdown-Liste **Tenant**.

4. Klicken Sie im unteren Teil der Benutzerkarte auf die Schaltfläche **Save**, um die Karte zu schließen.

Der Benutzerzugriff auf Mandanten wurde geändert.

Benutzerkonten löschen

Das Löschen von Benutzerkonten ist in der MDR-Konsole und auf der Kaspersky-Website verfügbar.

MDR-Benutzerkonten in der MDR-Konsole löschen

Das MDR-Administratorkonto ist erforderlich, um MDR-Benutzerkonten zu löschen.

Die mit einem gelöschten Konto verknüpfte E-Mail-Adresse erhält keine Benachrichtigungen und Berichte mehr. Um den Zugriff auf die MDR-Konsole wiederherzustellen, [muss eine neue Einladung an die E-Mail-Adresse gesendet werden](#).

Wenn Sie nur über ein einziges MDR-Administratorkonto verfügen, kann dieses Konto nicht gelöscht werden.

So löschen Sie ein MDR-Benutzerkonto:

1. Navigieren Sie im Fenster der MDR Console zum Menüpunkt **Settings**.

Die Benutzerliste wird geöffnet.

2. Bewegen Sie in der Benutzerliste den Mauszeiger über den Benutzer, den Sie löschen möchten, und klicken Sie rechts auf das Papierkorbsymbol.

Das Fenster **Confirm user deletion** wird geöffnet.

3. Klicken Sie auf die Schaltfläche **Delete**, um den Benutzer zu löschen.

Kaspersky Accounts löschen

Benutzer können ihren eigenen Kaspersky Account unabhängig von den zugewiesenen Benutzerrechten auf der Kaspersky-Website löschen.

Beim Löschen eines Kaspersky Accounts wird das entsprechende MDR-Benutzerkonto automatisch gelöscht. Die mit dem gelöschten Kaspersky Account verknüpfte E-Mail-Adresse erhält keine MDR-Benachrichtigungen und -Berichte mehr.

Wenn alle Benutzerkonten von MDR-Administratoren gelöscht werden, können keine neuen Benutzer mehr hinzugefügt und die MDR-Konsole kann nicht mehr konfiguriert werden. In diesem Fall [nehmen Sie Kontakt zum Technischen Support auf](#).

Wenn Sie den Kaspersky Account löschen, der zur Konfiguration des MDR-Plug-ins auf dem Administrationsserver oder in der Open Single Management Plattform verwendet wurde, muss das MDR-Plug-in neu konfiguriert werden.

Assets verwalten

Ein *Asset* ist ein Gerät, auf dem eine EPP-Anwendung von Kaspersky (z. B. Kaspersky Endpoint Security für Windows) installiert ist. Dieser Abschnitt enthält Informationen zum Anzeigen, Sortieren und Filtern von Assets.

Assets in der MDR Web Console anzeigen und durchsuchen

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Sie können verfügbare Assets anzeigen und durchsuchen, indem Sie die Asset-Liste verwenden.

So zeigen Sie Assets an:

1. Navigieren Sie im Fenster der MDR Web Console zum Menüpunkt **Assets**.

Die Asset-Liste wird geöffnet. Jede Zeile steht für ein Asset. Sie können auf eine beliebige Stelle in der Zeile klicken, um Informationen zu dem Asset anzuzeigen.

Die folgenden Asset-Attribute können über der Liste angezeigt werden:

Asset name

Netzwerkname eines Computers

Sie können auf den **Asset name** klicken, um die Asset-Informationen in der Kaspersky Security Center Web Console anzuzeigen.

Asset ID

Eine eindeutige Kennung eines Assets. Die Asset-ID wird von Kaspersky Managed Detection and Response automatisch generiert, bevor das Asset zum ersten Mal Telemetriedaten sendet.

Applications

Auf dem Asset installierte Endpoint Protection Plattform (EPP-Anwendung), die für die Verwendung mit Kaspersky Managed Detection and Response konfiguriert ist.

Interfaces

Anzahl aller Netzwerkschnittstellen, die auf dem Gerät verfügbar sind.

Operating system

Betriebssystem, das auf dem Asset installiert ist.

Domain

Netzwerkdomäne, der das Asset zugehörig ist.

Tenant

Name des [Mandanten](#), wenn das Asset zu einem Mandanten gehört. Wenn das Asset keinem Mandanten besitzt, ist dieses Feld leer.

Last seen

Anzahl der Tage, seit das Asset zuletzt in MDR Web Console gesehen wurde.

Assets werden nach diesem Attribut in absteigender Reihenfolge sortiert.

Standardmäßig werden die Assets angezeigt, die in den letzten 30 Tagen gesehen wurden. Sie können den Zeitraum erweitern, indem Sie Assets filtern.

Status

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Der Status spiegelt den aktuellen Asset-Status wider. Für Assets mit dem Status *OK*, *Warnung* oder *Kritisch* listet das Programm zusätzlich die Probleme (falls vorhanden) der letzten 72 Stunden auf.

Die Assets nehmen einen der folgenden Statuswerte an:

- **OK** (grün)

Telemetriedaten werden versandt und der Schutz ist voll funktionsfähig.

- **Warning** (gelb)

Mögliche Gründe für den Status **Warning**:

- Geringe Verluste von Telemetriedaten. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Antiviren-Datenbanken sind mehr als 7 Tage veraltet.
- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

Firewall.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) [↗]
- [Kaspersky Security for Virtualization Light Agent](#) [↗]
- [Kaspersky Embedded Systems Security for Windows](#) [↗]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [↗]

Schutz vor Netzwerkbedrohungen

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) [↗]
- [Kaspersky Endpoint Security für Linux](#) [↗]
- [Kaspersky Endpoint Security for Mac](#) [↗]
- [Kaspersky Embedded Systems Security for Windows](#) [↗]

- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Schutz vor E-Mail-Bedrohungen und Zusätzliche Erweiterung von Microsoft Office Outlook

Im folgenden Artikel wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:
[Kaspersky Endpoint Security für Windows](#) .

Schutz vor Web-Bedrohungen.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 

Selbstschutz des Produkts

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Diese Komponenten wirken sich auf die Vollständigkeit der gesendeten Telemetrie aus. Wenn eine Komponente deaktiviert ist oder fehlt, sendet Kaspersky Managed Detection and Response keine Telemetriedaten von Ereignissen, die sich auf diese Komponente beziehen. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft ab. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#). Wenn Sie mit der aktuellen Konfigurationsdatei weiterarbeiten, ändert sich der Status einige Tage vor dem Ablaufdatum in **Critical**.

Der Status **Warning** gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#)  wird dieser Status nicht angezeigt.

- **Critical** (rot)

Mögliche Gründe für den Status **Critical**:

- Große Verluste von Telemetriedaten. Die Daten sind unzureichend für eine Analyse. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

- **Aktivitätsmonitor oder Verhaltensanalyse**

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **Schutz vor bedrohlichen Dateien**

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Wenn eine dieser Komponenten deaktiviert ist oder fehlt, stellt Kaspersky Managed Detection and Response das Senden von Telemetriedaten von dem Asset ein. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft bald ab oder ist bereits abgelaufen. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#).

Dieser Status gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#)  wird dieser Status nicht angezeigt.

- **Offline** (schwarz)

Keine Telemetriedaten für mehr als 7 Tage (Standardwert). Im Abschnitt **Einstellungen** können Sie die Anzahl an Tagen ohne empfangene Telemetriedaten, nach denen für das Asset der Status **Offline** angezeigt soll, ändern. Der verfügbare Zeitraum beträgt 2–29 Tage.

Wenn für Ihre Assets der Status **Offline** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Der Status **Offline** gilt nicht für VDI-Assets (temporäre virtuelle Maschinen).

- **Absent** (schwarz)

Keine Telemetriedaten für mehr als 30 Tage für physische Assets oder für mehr als 24 Stunden für VDI-Assets (temporäre virtuelle Maschinen).

Wenn für Ihre Assets der Status **Absent** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Sie können Assets mit dem Status **Absent** in der [Asset-Liste](#), den [Berichten](#) und den Daten, die über [API-Schnittstelle](#) empfangenen werden, ausblenden.

Am Anfang der Vorfallsliste befinden sich die folgenden Schaltflächen:

- Die Schaltfläche **Columns** mit einem Zahnradsymbol, um auszuwählen, welche Spalten auf der Registerkarte **History** angezeigt werden sollen.
- Die Schaltfläche **Filter** mit einem Trichtersymbol, um nur die Änderungen anzuzeigen, die sich auf die ausgewählten Kontrollkästchen beziehen.
- Die Schaltfläche **Search** mit einem Lupensymbol, um nur die Änderungen anzuzeigen, die sich auf die eingegebenen Wörter oder Zeichen beziehen.

2. Wenn Sie die Anzahl der angezeigten Assets pro Listenseite ändern möchten, wählen Sie die Anzahl aus, indem Sie unten auf der Seite auf die Option **entries per page** klicken.

Sie können 10, 20 oder 50 Assets pro Seite auswählen.

Assets mit dem Status **Absent** können Sie in der Asset-Liste ausblenden. Aktivieren Sie dazu das Kontrollkästchen in den **Settings** → Registerkarte **General settings**.

Wenn Sie durch die Asset-Liste navigieren möchten, wählen Sie die gewünschte Seite unterhalb der Liste aus. Mit den Optionen **Previous** und **Next** können Sie zwischen benachbarten Seiten wechseln.

Die Asset-Liste enthält standardmäßig jene Assets, die in den letzten 30 Tagen in MDR Web Console gesehen wurden.

So ändern Sie diesen Zeitraum:

1. Klicken Sie auf das Trichter-Symbol über der Liste.
2. Wählen Sie im rechten Bereich **Filter** den Zeitraum im Feld **Last seen** aus.
3. Klicken Sie auf die Schaltfläche **Save**.

Sie können die Assets durchsuchen, indem Sie über der Asset-Liste neben dem Trichter-Symbol auf die Lupe klicken.

Assets in der MDR Web Console filtern

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Sie können Filter erstellen und auf die Asset-Liste anwenden.

So erstellen Sie einen Filter für die Asset-Liste:

1. Navigieren Sie im Fenster der MDR Web Console zum Menüpunkt **Assets**.

Die Asset-Liste wird geöffnet.

2. Klicken Sie über der Asset-Liste auf das Trichtersymbol.

Das Menü **Filter** wird angezeigt.

Für die Filterung sind folgende Parameter verfügbar:

- **Last seen**

Der Zeitpunkt, zu dem das Asset zuletzt in MDR Web Console gesehen wurde.

- **Asset name**

Verfügbare Asset-Namen.

Ein Asset-Name ist der Netzwerkname eines Computers.

- **Tenant**

Verfügbare Mandanten-Namen.

Sie können den Wert **Root tenant** auswählen, um Assets anzuzeigen, die keinem Ihrer Mandanten zugewiesen sind.

Sie können den Wert **Root tenant** zusätzlich zu angegebenen Namen der Mandanten auswählen.

- **Status**

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Der Status spiegelt den aktuellen Asset-Status wider. Für Assets mit dem Status *OK*, *Warnung* oder *Kritisch* listet das Programm zusätzlich die Probleme (falls vorhanden) der letzten 72 Stunden auf.

Die Assets nehmen einen der folgenden Statuswerte an:

- **OK** (grün)

Telemetriedaten werden versandt und der Schutz ist voll funktionsfähig.

- **Warning** (gelb)

Mögliche Gründe für den Status **Warning**:

- Geringe Verluste von Telemetriedaten. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Antiviren-Datenbanken sind mehr als 7 Tage veraltet.
- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

Firewall.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Schutz vor Netzwerkbedrohungen

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Schutz vor E-Mail-Bedrohungen und Zusätzliche Erweiterung von Microsoft Office Outlook

Im folgenden Artikel wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren: [Kaspersky Endpoint Security für Windows](#) .

Schutz vor Web-Bedrohungen.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 

- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 

Selbstschutz des Produkts

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Diese Komponenten wirken sich auf die Vollständigkeit der gesendeten Telemetrie aus. Wenn eine Komponente deaktiviert ist oder fehlt, sendet Kaspersky Managed Detection and Response keine Telemetriedaten von Ereignissen, die sich auf diese Komponente beziehen. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft ab. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#). Wenn Sie mit der aktuellen Konfigurationsdatei weiterarbeiten, ändert sich der Status einige Tage vor dem Ablaufdatum in **Critical**.

Der Status **Warning** gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#)  wird dieser Status nicht angezeigt.

• Critical (rot)

Mögliche Gründe für den Status **Critical**:

- Große Verluste von Telemetriedaten. Die Daten sind unzureichend für eine Analyse. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

• Aktivitätsmonitor oder Verhaltensanalyse

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **Schutz vor bedrohlichen Dateien**

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Wenn eine dieser Komponenten deaktiviert ist oder fehlt, stellt Kaspersky Managed Detection and Response das Senden von Telemetriedaten von dem Asset ein. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft bald ab oder ist bereits abgelaufen. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#).

Dieser Status gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#)  wird dieser Status nicht angezeigt.

- **Offline** (schwarz)

Keine Telemetriedaten für mehr als 7 Tage (Standardwert). Im Abschnitt **Einstellungen** können Sie die Anzahl an Tagen ohne empfangene Telemetriedaten, nach denen für das Asset der Status **Offline** angezeigt soll, ändern. Der verfügbare Zeitraum beträgt 2–29 Tage.

Wenn für Ihre Assets der Status **Offline** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Der Status **Offline** gilt nicht für VDI-Assets (temporäre virtuelle Maschinen).

- **Absent** (schwarz)

Keine Telemetriedaten für mehr als 30 Tage für physische Assets oder für mehr als 24 Stunden für VDI-Assets (temporäre virtuelle Maschinen).

Wenn für Ihre Assets der Status **Absent** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Sie können Assets mit dem Status **Absent** in der [Asset-Liste](#), den [Berichten](#) und den Daten, die über [API-Schnittstelle](#) empfangenen werden, ausblenden.

- **Isolation**

Gibt an, ob die Netzwerkisolation aktiviert ist oder nicht. Folgende Filterwerte sind möglich:

- **Isolated**

Die Netzwerkisolation ist aktiviert.

- **Not isolated**

Die Netzwerkisolation ist deaktiviert.

3. Klicken Sie auf **Save**, um den erstellten Filter zu übernehmen.

Nachdem der Filter angewendet wurde, werden in der Asset-Liste nur Assets angezeigt, die den ausgewählten Parameter des Filters entsprechen.

Assets mit dem Status **Absent** können Sie in der Asset-Liste ausblende. Aktivieren Sie dazu das Kontrollkästchen in den **Settings** → Registerkarte **General settings**.

Detaillierte Informationen zu Assets in der MDR Web Console anzeigen

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

So zeigen Sie detaillierte Informationen zu Assets an:

1. Navigieren Sie im Fenster der MDR Web Console zum Menüpunkt **Assets**.

Die Asset-Liste wird geöffnet.

2. Klicken Sie auf die Zeichenfolge des Assets, dessen Details Sie anzeigen möchten.

Die Asset-Karte wird angezeigt. Die Asset-Karte enthält zwei Registerkarten:

- **Properties** enthält allgemeine Informationen über das Asset
- **Incidents** enthält Informationen zu Vorfällen, die mit dem Asset aufgetreten sind

Die allgemeinen Informationen auf der Registerkarte **Properties** enthalten die folgenden Informationen:

- **Asset name**

Netzwerkname eines Computers

Sie können auf den **Asset name** klicken, um die Asset-Informationen in der Kaspersky Security Center Web Console anzuzeigen.

- **Status**

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Der Status spiegelt den aktuellen Asset-Status wider. Für Assets mit dem Status *OK*, *Warnung* oder *Kritisch* listet das Programm zusätzlich die Probleme (falls vorhanden) der letzten 72 Stunden auf.

Die Assets nehmen einen der folgenden Statuswerte an:

- **OK** (grün)

Telemetriedaten werden versandt und der Schutz ist voll funktionsfähig.

- **Warning** (gelb)

Mögliche Gründe für den Status **Warning**:

- Geringe Verluste von Telemetriedaten. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Antiviren-Datenbanken sind mehr als 7 Tage veraltet.
- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

Firewall.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) [↗]
- [Kaspersky Security for Virtualization Light Agent](#) [↗]
- [Kaspersky Embedded Systems Security for Windows](#) [↗]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [↗]

Schutz vor Netzwerkbedrohungen

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) [↗]
- [Kaspersky Endpoint Security für Linux](#) [↗]
- [Kaspersky Endpoint Security for Mac](#) [↗]
- [Kaspersky Embedded Systems Security for Windows](#) [↗]
- [Kaspersky Embedded Systems Security für Linux](#) [↗]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [↗]

Schutz vor E-Mail-Bedrohungen und Zusätzliche Erweiterung von Microsoft Office Outlook

Im folgenden Artikel wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren: [Kaspersky Endpoint Security für Windows](#) [↗].

Schutz vor Web-Bedrohungen.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 

Selbstschutz des Produkts

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Diese Komponenten wirken sich auf die Vollständigkeit der gesendeten Telemetrie aus. Wenn eine Komponente deaktiviert ist oder fehlt, sendet Kaspersky Managed Detection and Response keine Telemetriedaten von Ereignissen, die sich auf diese Komponente beziehen. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft ab. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#). Wenn Sie mit der aktuellen Konfigurationsdatei weiterarbeiten, ändert sich der Status einige Tage vor dem Ablaufdatum in **Critical**.

Der Status **Warning** gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#)  wird dieser Status nicht angezeigt.

- **Critical** (rot)

Mögliche Gründe für den Status **Critical**:

- Große Verluste von Telemetriedaten. Die Daten sind unzureichend für eine Analyse. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

- **Aktivitätsmonitor oder Verhaltensanalyse**

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
 - [Kaspersky Endpoint Security für Linux](#) 

- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **Schutz vor bedrohlichen Dateien**

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Wenn eine dieser Komponenten deaktiviert ist oder fehlt, stellt Kaspersky Managed Detection and Response das Senden von Telemetriedaten von dem Asset ein. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft bald ab oder ist bereits abgelaufen. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#).

Dieser Status gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#)  wird dieser Status nicht angezeigt.

- **Offline** (schwarz)

Keine Telemetriedaten für mehr als 7 Tage (Standardwert). Im Abschnitt **Einstellungen** können Sie die Anzahl an Tagen ohne empfangene Telemetriedaten, nach denen für das Asset der Status **Offline** angezeigt soll, ändern. Der verfügbare Zeitraum beträgt 2–29 Tage.

Wenn für Ihre Assets der Status **Offline** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Der Status **Offline** gilt nicht für VDI-Assets (temporäre virtuelle Maschinen).

- **Absent** (schwarz)

Keine Telemetriedaten für mehr als 30 Tage für physische Assets oder für mehr als 24 Stunden für VDI-Assets (temporäre virtuelle Maschinen).

Wenn für Ihre Assets der Status **Absent** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Sie können Assets mit dem Status **Absent** in der [Asset-Liste](#), den [Berichten](#) und den Daten, die über [API-Schnittstelle](#) empfangenen werden, ausblenden.

- **IP address**

Die IP-Adresse des Assets.

- **Physical address**

- **Tenant**

Name des [Mandanten](#), wenn das Asset zu einem Mandanten gehört. Wenn das Asset keinem Mandanten besitzt, ist dieses Feld leer.

- **First seen**

- **Last seen**

- **Operating system**

Betriebssystem, das auf dem Asset installiert ist.

- **Kaspersky applications that work with MDR**

- **Domain**

Die Registerkarte **Incidents** enthält die Liste der Vorfälle. Die Spalte **ID/Created** der Liste enthält eine Vorfall-ID und die Uhrzeit, zu welcher der Vorfall erstellt wurde. Die Spalte **Status** der Liste enthält Informationen zum Vorfallstatus.

Status der Assets

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Der Status spiegelt den aktuellen Asset-Status wider. Für Assets mit dem Status *OK*, *Warnung* oder *Kritisch* listet das Programm zusätzlich die Probleme (falls vorhanden) der letzten 72 Stunden auf.

Die Assets nehmen einen der folgenden Statuswerte an:

- **OK (grün)**

Telemetriedaten werden versandt und der Schutz ist voll funktionsfähig.

- **Warning** (gelb)

Mögliche Gründe für den Status **Warning**:

- Geringe Verluste von Telemetriedaten. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Antiviren-Datenbanken sind mehr als 7 Tage veraltet.
- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

Firewall.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Schutz vor Netzwerkbedrohungen

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Schutz vor E-Mail-Bedrohungen und Zusätzliche Erweiterung von Microsoft Office Outlook

Im folgenden Artikel wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren: [Kaspersky Endpoint Security für Windows](#) .

Schutz vor Web-Bedrohungen.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 

Selbstschutz des Produkts

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Diese Komponenten wirken sich auf die Vollständigkeit der gesendeten Telemetrie aus. Wenn eine Komponente deaktiviert ist oder fehlt, sendet Kaspersky Managed Detection and Response keine Telemetriedaten von Ereignissen, die sich auf diese Komponente beziehen. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft ab. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#). Wenn Sie mit der aktuellen Konfigurationsdatei weiterarbeiten, ändert sich der Status einige Tage vor dem Ablaufdatum in **Critical**.

Der Status **Warning** gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#)  wird dieser Status nicht angezeigt.

- **Critical** (rot)

Mögliche Gründe für den Status **Critical**:

- Große Verluste von Telemetriedaten. Die Daten sind unzureichend für eine Analyse. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

- **Aktivitätsmonitor oder Verhaltensanalyse**

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **Schutz vor bedrohlichen Dateien**

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 

- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Wenn eine dieser Komponenten deaktiviert ist oder fehlt, stellt Kaspersky Managed Detection and Response das Senden von Telemetriedaten von dem Asset ein. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft bald ab oder ist bereits abgelaufen. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#).

Dieser Status gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#)  wird dieser Status nicht angezeigt.

- **Offline** (schwarz)

Keine Telemetriedaten für mehr als 7 Tage (Standardwert). Im Abschnitt **Einstellungen** können Sie die Anzahl an Tagen ohne empfangene Telemetriedaten, nach denen für das Asset der Status **Offline** angezeigt soll, ändern. Der verfügbare Zeitraum beträgt 2–29 Tage.

Wenn für Ihre Assets der Status **Offline** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Der Status **Offline** gilt nicht für VDI-Assets (temporäre virtuelle Maschinen).

- **Absent** (schwarz)

Keine Telemetriedaten für mehr als 30 Tage für physische Assets oder für mehr als 24 Stunden für VDI-Assets (temporäre virtuelle Maschinen).

Wenn für Ihre Assets der Status **Absent** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Sie können Assets mit dem Status **Absent** in der [Asset-Liste](#), den [Berichten](#) und den Daten, die über [API-Schnittstelle](#) empfangenen werden, ausblenden.

Status der Assets in Kaspersky Security Center überprüfen

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Sie können den Status Ihrer Assets mithilfe der Funktion "Status der MDR-Assets" prüfen. Damit können Sie überprüfen, welche Assets derzeit durch Kaspersky Managed Detection and Response geschützt werden und welche noch nie [Telemetriedaten](#) an Kaspersky Managed Detection and Response gesendet haben.

Für Assets mit Kaspersky Endpoint Security für Windows 12.3 oder höher, die in der [Konfiguration des Agenten von Endpoint Detection and Response \(EDR Agent\)](#) ausgeführt werden, entspricht der angezeigte Status in MDR nicht dem tatsächlichen Status.

Statuswerte der Assets, die mindestens einmal Telemetriedaten gesendet haben

So überprüfen Sie den Status der Assets:

1. Wechseln Sie in Kaspersky Security Center vom Abschnitt **MDR** zur Registerkarte **Status der MDR-Assets**.
2. Wählen Sie die Registerkarte **Alle jemals sichtbaren Assets** aus.

Es wird eine Liste mit allen Assets angezeigt, die mindestens einmal Telemetriedaten an Kaspersky Managed Detection and Response gesendet haben.

Für jedes Asset folgende Informationen angezeigt:

Status

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Der Status spiegelt den aktuellen Asset-Status wider. Für Assets mit dem Status *OK*, *Warnung* oder *Kritisch* listet das Programm zusätzlich die Probleme (falls vorhanden) der letzten 72 Stunden auf.

Die Assets nehmen einen der folgenden Statuswerte an:

- **OK** (grün)

Telemetriedaten werden versandt und der Schutz ist voll funktionsfähig.

- **Warning** (gelb)

Mögliche Gründe für den Status **Warning**:

- Geringe Verluste von Telemetriedaten. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Antiviren-Datenbanken sind mehr als 7 Tage veraltet.

- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

Firewall.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Schutz vor Netzwerkbedrohungen

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Schutz vor E-Mail-Bedrohungen und Zusätzliche Erweiterung von Microsoft Office Outlook

Im folgenden Artikel wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:
[Kaspersky Endpoint Security für Windows](#) .

Schutz vor Web-Bedrohungen.

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Endpoint Security für Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security für Linux](#) 

Selbstschutz des Produkts

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Diese Komponenten wirken sich auf die Vollständigkeit der gesendeten Telemetrie aus. Wenn eine Komponente deaktiviert ist oder fehlt, sendet Kaspersky Managed Detection and Response keine Telemetriedaten von Ereignissen, die sich auf diese Komponente beziehen. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft ab. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#). Wenn Sie mit der aktuellen Konfigurationsdatei weiterarbeiten, ändert sich der Status einige Tage vor dem Ablaufdatum in **Critical**.

Der Status **Warning** gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#) wird dieser Status nicht angezeigt.

- **Critical** (rot)

Mögliche Gründe für den Status **Critical**:

- Große Verluste von Telemetriedaten. Die Daten sind unzureichend für eine Analyse. Mehr darüber entnehmen Sie diesem Artikel: [So vermeiden Sie den Verlust von Telemetriedaten der Assets](#).
- Mindestens eine der folgenden EPP-Anwendungskomponenten auf dem Asset ist deaktiviert oder nicht installiert:

- **Aktivitätsmonitor oder Verhaltensanalyse**

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#)
 - [Kaspersky Endpoint Security für Linux](#)
 - [Kaspersky Embedded Systems Security for Windows](#)
 - [Kaspersky Embedded Systems Security für Linux](#)
 - [Kaspersky Industrial CyberSecurity for Nodes](#)
 - [Kaspersky Security for Virtualization Light Agent](#)

- **Schutz vor bedrohlichen Dateien**

In den folgenden Artikeln wird beschrieben, wie Sie diese Komponente aktivieren oder konfigurieren:

- [Kaspersky Endpoint Security für Windows](#)
 - [Kaspersky Endpoint Security für Linux](#)
 - [Kaspersky Endpoint Security for Mac](#)
 - [Kaspersky Security for Virtualization Light Agent](#)
 - [Kaspersky Embedded Systems Security for Windows](#)
 - [Kaspersky Embedded Systems Security für Linux](#)
 - [Kaspersky Industrial CyberSecurity for Nodes](#)

Wenn eine dieser Komponenten deaktiviert ist oder fehlt, stellt Kaspersky Managed Detection and Response das Senden von Telemetriedaten von dem Asset ein. Die installierte Epp-Anwendung enthält möglicherweise nicht alle aufgeführten Komponenten.

- Die KPSN-Konfigurationsdatei läuft bald ab oder ist bereits abgelaufen. Die Anwendung zeigt das Ablaufdatum an. Erwägen Sie eine [Aktualisierung der KPSN-Konfigurationsdatei](#).

Dieser Status gilt für Assets mit den folgenden installierten Programmen: Kaspersky Endpoint Security für Windows 11 oder höher, Kaspersky Endpoint Security für Linux 11.2 oder höher, Kaspersky Endpoint Security für Mac 11.2 oder höher oder Kaspersky Security for Virtualization Light Agent 5.2 oder höher. Für Assets mit [Kaspersky Endpoint Security für Windows in der Konfiguration mit Endpoint Detection and Response Agent \(EDR Agent\)](#) wird dieser Status nicht angezeigt.

- **Offline** (schwarz)

Keine Telemetriedaten für mehr als 7 Tage (Standardwert). Im Abschnitt **Einstellungen** können Sie die Anzahl an Tagen ohne empfangene Telemetriedaten, nach denen für das Asset der Status **Offline** angezeigt soll, ändern. Der verfügbare Zeitraum beträgt 2–29 Tage.

Wenn für Ihre Assets der Status **Offline** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Der Status **Offline** gilt nicht für VDI-Assets (temporäre virtuelle Maschinen).

- **Absent** (schwarz)

Keine Telemetriedaten für mehr als 30 Tage für physische Assets oder für mehr als 24 Stunden für VDI-Assets (temporäre virtuelle Maschinen).

Wenn für Ihre Assets der Status **Absent** angezeigt wird:

- Stellen Sie sicher, dass die mit den Statuswerten **Warning** und **Critical** aufgeführten Komponenten der EPP-Anwendung installiert und auf den Assets aktiviert sind.
- Stellen Sie sicher, dass Kaspersky Managed Detection and Response in Ihrer Infrastruktur [ordnungsgemäß bereitgestellt](#) wurde.

Sie können Assets mit dem Status **Absent** in der [Asset-Liste](#), den [Berichten](#) und den Daten, die über [API-Schnittstelle](#) empfangenen werden, ausblenden.

Asset-Name

Netzwerkname eines Computers

Sie können auf den **Asset name** klicken, um die Asset-Informationen in der Kaspersky Security Center Web Console anzuzeigen.

Asset-ID

Eine eindeutige Kennung eines Assets. Die Asset-ID wird von Kaspersky Managed Detection and Response automatisch generiert, bevor das Asset zum ersten Mal Telemetriedaten sendet.

Domäne

Netzwerkdomäne, der das Asset zugehörig ist.

Betriebssystemversion

Betriebssystem, das auf dem Asset installiert ist.

EPP-Anwendungen

Auf dem Asset installierte Endpoint Protection Platform (EPP-Anwendung), die für die Verwendung mit Kaspersky Managed Detection and Response konfiguriert ist.

Schnittstellen

Anzahl aller Netzwerkschnittstellen, die auf dem Gerät verfügbar sind.

Mandant

Name des [Mandanten](#), wenn das Asset zu einem Mandanten gehört. Wenn das Asset keinem Mandanten besitzt, ist dieses Feld leer.

Zuletzt gesehen

Anzahl der Tage, seit das Asset zuletzt in MDR Web Console gesehen wurde.

Assets werden nach diesem Attribut in absteigender Reihenfolge sortiert.

Standardmäßig werden die Assets angezeigt, die in den letzten 30 Tagen gesehen wurden. Sie können den Zeitraum erweitern, indem Sie Assets filtern.

3. Um mit dieser Liste zu arbeiten, verwenden Sie die folgenden Sortier- und Filteroptionen:

- Klicken Sie auf einen beliebigen Spaltentitel, um die Liste nach den Werten der ausgewählten Spalte zu sortieren.
- Klicken Sie auf die Spalte **Status** und wählen Sie anschließend die erforderlichen Statuswerte aus. Die Liste wird gefiltert und zeigt nur die Assets mit den ausgewählten Statuswerten an.
- Klicken Sie auf **Filter** und wählen Sie anschließend den Zeitraum aus. Dann werden nur die Assets angezeigt, die während des ausgewählten Zeitraums zum letzten Mal sichtbar waren. Sie können auch einen benutzerdefinierten Zeitraum angeben.
- Klicken Sie über der Asset-Liste auf **Exportieren**, um die Liste als csv-Datei zu exportieren.
- Verwenden Sie das Feld **Suche**, um nach Assets anhand ihrer Namen zu suchen.

Statuswerte der Assets, die nie Telemetriedaten gesendet haben

Diese Funktion wird in Kaspersky Security Center 15.1 Windows oder höher, Kaspersky Security Center 15.1 Linux oder höher sowie in Kaspersky Next Expert View ordnungsgemäß ausgeführt.

So zeigen Sie die Assets an, die nie Telemetriedaten gesendet haben:

1. Wechseln Sie in Kaspersky Security Center vom Abschnitt **MDR** zur Registerkarte **Status der MDR-Assets**.
2. Wählen Sie die Registerkarte **Beim Abrufen des Status der Assets ist ein Fehler aufgetreten**.

In der MDR Web Console wird eine Liste mit jenen Assets angezeigt, die zwar zu Kaspersky Security Center hinzugefügt wurden, aber noch nie Telemetriedaten an Kaspersky Managed Detection and Response gesendet haben.

Für jedes Asset folgende Informationen angezeigt:

- **Asset-Name**

Netzwerkname eines Computers

Sie können auf den **Asset name** klicken, um die Asset-Informationen in der Kaspersky Security Center Web Console anzuzeigen.

- **EPP-Anwendungen**

Auf dem Asset installierte Endpoint Protection Plattform (EPP-Anwendung), die für die Verwendung mit Kaspersky Managed Detection and Response konfiguriert ist.

- **MDR-Status**

Die MDR-Komponente einer EPP-Anwendung, die auf einem Asset installiert ist, kann einen der folgenden Statuswerte besitzen:

- *Unbekannt* – Im Gegensatz zu anderen Statuswerten wird der Status *Unbekannt* nicht von den Anwendungen selbst gesendet. Diese Option zeigt an, dass die Anwendungen keine Informationen über den Status der ausgewählten Komponente haben. Dies kann beispielsweise der Fall sein, wenn die ausgewählte Komponente zu keinem der auf dem Gerät installierten Anwendungen gehört oder wenn das Gerät ausgeschaltet ist.
- *Beendet* – Die Komponente ist deaktiviert und funktioniert derzeit nicht.
- *Pausiert* – Die Ausführung der Komponente wurde ausgesetzt, z. B. nachdem ein Benutzer den Schutz in der verwalteten Anwendung pausiert hat.
- *Startet* – Die Komponente wird gerade initialisiert.
- *Läuft* – Die Komponente ist aktiviert und wird ordnungsgemäß ausgeführt.
- *Fehlgeschlagen* – Im Rahmen der Ausführung der Komponente ist ein Fehler aufgetreten.
- *Nicht installiert* – Der Benutzer hat die Komponente bei der Konfiguration der benutzerdefinierten Installation der Anwendung nicht zur Installation ausgewählt.
- *Keine Lizenz* – Die Lizenz für die MDR-Funktionalität fehlt oder ist abgelaufen.

- **KSC-Server**

Name des Kaspersky Security Center Administrationsservers, der das ausgewählte Asset verwaltet.

- **Status wichtiger Komponenten**

Eine Liste mit den Komponenten der EPP-Anwendung, die kritisch für die Ausführung von MDR sind. Jede Komponente verfügt über eine farbige Anzeige, die vom Status der Komponente abhängt:

- Die Anzeige erscheint gelb, wenn die Komponente einen der folgenden Statuswerte besitzt: **Pausiert**, **Startet** oder **Unbekannt**.
- Die Anzeige erscheint gelb, wenn die Komponente einen der folgenden Statuswerte besitzt: **Beendet**, **Fehlgeschlagen**, **Keine Lizenz** oder **Nicht installiert**.

Auch die [Funktion zum Selbstschutz](#) wird zusammen mit den Komponenten der EPP-Anwendung aufgelistet. Wenn diese Funktion deaktiviert ist, erscheint die Anzeige ebenfalls rot.

- Die Komponenten mit dem Status **Läuft** werden in der Tabelle nicht aufgelistet und besitzen keine Anzeige.

Um die vollständige Liste der Komponenten anzuzeigen, einschließlich derer, die für den MDR-Betrieb nicht kritisch sind, klicken Sie auf den Namen des Assets. Die Komponenten und ihr Status werden im unteren Fenster mit den Details zum Asset angezeigt.

3. Bei Bedarf können Sie die Assets nach dem MDR-Status filtern. Klicken Sie dazu auf **Filter** und wählen Sie anschließend die erforderlichen MDR-Statuswerte aus. In der MDR Web Console werden anschließend nur die Assets angezeigt, auf denen die MDR-Komponente einen der ausgewählten MDR-Statuswerte besitzt. Alternativ können Sie eine der folgenden Optionen auswählen:

- **Installiert und aktiviert** – Die Liste wird gefiltert und zeigt Assets an, die einen der folgenden MDR-Statuswerte besitzen: *Unbekannt*, *Beendet*, *Pausiert*, *Startet*, *Läuft* oder *Fehlgeschlagen*.
- **Lizenz fehlt oder abgelaufen** – Die Liste wird gefiltert und zeigt Assets an, die den MDR-Status *Keine Lizenz* besitzen.

4. Klicken Sie bei Bedarf auf die Schaltfläche **Exportieren**, um die Asset-Liste in eine csv-Datei zu exportieren.

So vermeiden Sie den Verlust von Telemetriedaten der Assets

Unsere Empfehlung: Verwenden Sie die neuesten Versionen der Kaspersky-Anwendungen und -Lösungen, um einen optimalen Schutz sicherzustellen und alle neuen Funktionen und Updates vollständig zu nutzen.

Assets [senden Telemetriedaten](#) an Kaspersky Managed Detection and Response, um Sicherheitsvorfälle in Ihrer Infrastruktur zu erkennen und zu analysieren. Wenn Sie feststellen, dass im [Asset-Status](#) Verluste von Telemetriedaten angezeigt werden, stellen Sie sicher, dass die folgenden Anweisungen ausgeführt werden:

1. Es sind die empfohlenen Versionen der Kaspersky-Programme auf Ihren Assets installiert (siehe Spalte *Empfohlene Versionen und deren Support-Laufzeiten* im Unterabschnitt *Kompatible Versionen von Kaspersky-Programmen* des Abschnitts [Hard- und Softwarevoraussetzungen](#)).
2. Der Durchsatz Ihres Netzwerkkanals entspricht den Spezifikationen aus dem Unterabschnitt *Netzwerkkanal* des Abschnitts [Hard- und Softwarevoraussetzungen](#).
3. Ihr [KSN-Proxyserver](#)  bietet eine ausreichende Durchsatzleistung.

Wenn mit der Durchsatzleistung des KSN-Proxyservers Probleme auftreten, deaktivieren Sie den KSN-Proxy in der [KSC-Richtlinie](#) um eine direkte Verbindung der Assets mit KSN zu erzwingen:

- a. Wechseln Sie im Hauptmenü von Kaspersky Security Center zu **Geräte** → **Richtlinien & Profile**.
 - b. Klicken Sie auf die Richtlinie für Kaspersky Endpoint Security für Windows, Linux oder Mac. Das Eigenschaftenfenster der ausgewählten Richtlinie wird geöffnet.
 - c. Klicken Sie in den Eigenschaften der Richtlinie auf **Programmeinstellungen** → **Erweiterter Schutz** → **Kaspersky Security Network**.
 - d. Aktivieren Sie die Optionen **KSN-Server verwenden, wenn kein KSN-Proxy verfügbar** (sofern für die Richtlinie zutreffend).
 - e. Klicken Sie auf **OK**.
4. Der KSN-Proxy ist auf der Seite des Verteilungspunkts in [Kaspersky Next Expert View](#) oder in der Kaspersky Security Center [Web Console](#) aktiviert, um die Auslastung des Netzwerks zu optimieren.
5. Die Workload Ihres Kaspersky Security Center Administrationsservers überschreitet nicht die [Beschränkungen](#).
6. Es wird die unter [Hard- und Softwarevoraussetzungen](#) angegebene empfohlene Version von Kaspersky Security Center verwendet und es sind die aktuellsten verfügbaren Hotfixes und Patches installiert.

Vorfälle verwalten

Ein *Vorfall* ist eine Aktivität, die von der Erkennungstechnologie als kritisch bewertet wird und eine sofortige Reaktion des Online-Dienstes erfordert. Dieser Abschnitt enthält Informationen zum Verwalten vorhandener Vorfälle und zum Hinzufügen neuer Vorfälle.

Sie können die Vorfälle auch in der [MDR Web Console](#) verwalten.

Um die Vorfälle in der MDR Web Console zu verwalten, müssen Sie einen [Kaspersky Account](#) ² erstellen und Ihren [MDR-Administrator](#) (Benutzer der MDR Web Console mit der Rolle **MDR Administrator**) darum bitten, Sie anhand der E-Mail-Adresse, die Sie für Ihren Kaspersky Account verwenden, [in der MDR Web Console einzuladen](#). Anschließend erhalten Sie per E-Mail die Einladung mit dem Link zur MDR Web Console.

Die MDR-Lösung bietet Reaktionen, die Sie [manuell verarbeiten](#) oder für die Sie die [automatische Annahme konfigurieren](#) können.

Sie können Integrationen mit [KUMA](#) und [XDR](#) konfigurieren, sodass MDR Daten von diesen Plattformen verarbeiten kann.

Über Vorfälle

Was genau ist ein Vorfall?

Im Sinne der Informationssicherheit stellt ein Vorfall jedes unvorhergesehene oder unerwünschte Ereignis dar, das die normale Aktivität oder die Informationssicherheit stören könnte.

Als Ereignis bezeichnet man die identifizierten äußerlichen Anzeichen für einen bestimmten Zustand eines Systems, Dienstes oder Netzwerks.

Das Hauptkriterium für die Entscheidung, ob es sich bei einer beobachteten Aktivität um einen Vorfall handelt, stellt im Rahmen der Kaspersky MDR-Lösung die Fähigkeit dar, wirksame Maßnahmen zu treffen, um möglichen Schäden durch diese Aktivität entgegenzuwirken, diese zu verhindern oder zu mindern. In der folgenden Tabelle finden Sie Beispiele für mögliche Vorfallkriterien und Maßnahmen für eine Reaktion in Abhängigkeit von der Quelle des Ereignisses.

Quelle des Ereignisses	Mögliche Vorfallkriterien	Mögliche Reaktionen auf den Vorfall
Endpunkt-Gerät	- Die aktive Phase des nicht automatisch verhinderten Angriffs - Nachweis für das Verbleiben von Schadfunktionen im System - Anzeichen für frühere Vorfälle - Anzeichen für Aktivitäten eines internen Eindringlings auf Kundenseite (einschließlich von Fällen, in denen der Angriff erfolgreich verhindert wurde)	- Problemerkennung durch auf Endpunkt-Geräten installierte Lösungen von AO Kaspersky Lab und Bewertung der Effizienz der automatischen Reaktionsmaßnahmen (soweit technisch möglich) - Empfohlene manuelle Reaktionsmaßnahmen - Geforderte automatische Reaktionsmaßnahmen - Empfehlungen zur Benutzersensibilisierung zum Thema Informationssicherheit
Endpunkt-Gerät + Netzwerk	Sicherheitsereignis einer unterstützten Technologie für Netzwerkerkennung und Bestätigung des Ereignisses auf dem Endpunkt-Gerät	- Problemerkennung durch auf Endpunkt-Geräten installierte Lösungen von AO Kaspersky Lab sowie durch Lösungen von AO Kaspersky Lab zur Überwachung des Netzwerkdatenverkehrs und Bewertung der Effizienz automatischer Reaktionsmaßnahmen (soweit technisch möglich) - Empfohlene manuelle Reaktionsmaßnahmen - Geforderte automatische Reaktionsmaßnahmen - Informieren des Kunden

Szenarien der Vorfallerkennung

Szenario 1. Vorfallerkennung durch die Kaspersky MDR-Lösung

In diesem Szenario wird ein Vorfall, der die Informationssicherheit betrifft, durch den Einsatz von Kaspersky MDR erkannt. Der Vorfall wird im Tracking-System für Vorfälle automatisch protokolliert. Die standardmäßige Prioritätsstufe eines solchen Vorfalls kann später geändert werden, allerdings muss für die Änderung ein Grund gemäß der Tabelle mit Prioritätsstufen für Vorfälle (siehe unten) angegeben werden. Kaspersky MDR verarbeitet protokollierte Vorfälle, um unverzüglich Informationen über den Zustand der IT-Infrastruktur des Kunden zu erhalten.

Wenn durch die Analyse die ursprünglichen Ursachen des Vorfalls identifiziert werden können, werden dem Kunden entsprechende Reaktionsempfehlungen vorgeschlagen. Wenn nur unzureichende Informationen vorhanden sind, um die ursprüngliche Ursache des Vorfalls zu ermitteln, werden dem Kunden alle verfügbaren Informationen und Analyseergebnisse zur unabhängigen Untersuchung zur Verfügung gestellt.

Szenario 2. Vorfallerkennung durch den Kunden (das Erstellen benutzerdefinierter Vorfälle ist für einige kommerzielle Lizenzstufen nicht verfügbar)

In diesem Szenario wird ein Vorfall, der die Informationssicherheit betrifft, durch den Kunden und unabhängig von Kaspersky MDR erkannt. Wenn der Vorfall durch Kaspersky MDR verarbeitet werden muss, kann der Kunde den Vorfall manuell protokollieren und alle verfügbaren Informationen über den erkannten Vorfall mithilfe der Funktionen von Kaspersky MDR bereitstellen. Standardmäßig ist die Prioritätsstufe eines solchen Vorfalls auf **Niedrig** festgelegt. Alternativ kann der Kunde bei der Protokollierung des Vorfalls einen anderen Wert angeben.

Die weitere Bearbeitung des Vorfalls verläuft ähnlich wie in Szenario 1.

Prioritätsstufen für Vorfälle

Prioritätsstufen für Vorfälle und deren Beschreibungen

Prioritätsstufe eines Vorfalls	Beschreibung
Hoch	Vorfälle, die nach Einschätzung der Experten von AO Kaspersky Lab zu erheblichen Störungen oder zu unbefugtem Zugriff auf die von Kaspersky MDR überwachten Kunden-Assets führen können. Dies können beispielsweise identifizierte Spuren eines gezielten Angriffs oder einer unbekannten Bedrohung sein, die der weiteren Untersuchung mit digitalen forensischen Methoden bedürfen.
Mittel	Vorfälle, die nach Einschätzung der Experten von AO Kaspersky Lab die Effizienz oder Leistung der von Kaspersky MDR überwachten Kunden-Assets beeinträchtigen können oder die zu einer einmaligen Datenbeschädigung führen können.
Niedrig	Vorfälle, die sich nach Einschätzung der Experten von AO Kaspersky Lab nicht wesentlich auf die Effizienz oder Leistung der von Kaspersky MDR überwachten Kunden-Assets auswirken. Dies kann beispielsweise die Erkennung von potenziell unerwünschter Software wie Adware oder Riskware sein.

Die standardmäßig eingestellte Prioritätsstufe für Vorfälle ist **Niedrig**.

Leistungsziele für die Ergreifung von Maßnahmen

Die Reaktionszeit und der Zielwert zur Ergreifung von Maßnahmen durch Kaspersky MDR sind Abhängig von der Priorität des Vorfalls

Prioritätsstufe eines Vorfalls	Reaktionszeit	Zielwert
Hoch	1 Stunde	90 %
Mittel	4 Stunden	90 %
Niedrig	24 Stunden	90 %

Ein Vorfall gilt als erledigt, wenn dem Kunden die Empfehlungen für Reaktionsmaßnahmen übermittelt wurden.

* Die Reaktionszeit entspricht der verstrichenen Zeit zwischen der Erkennung eines Vorfalls (Erstellungszeitpunkt) und der Veröffentlichung in der MDR Web Console (Update-Zeitpunkt).

** Der Zielwert entspricht dem Prozentsatz der Vorfälle, bei denen die Reaktionszeit der in der Tabelle angegebenen Zielsetzung entspricht.

Vorfälle in der MDR Web Console anzeigen und durchsuchen

So zeigen Sie Vorfälle an:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Vorfälle**.

Die Vorfall-Liste wird geöffnet. Jede Zeile steht für einen Vorfall. Sie können auf eine beliebige Stelle in der Zeile klicken, um Informationen zu dem Vorfall anzuzeigen.

Die folgenden Vorfall-Attribute sind oberhalb der Liste zu finden:

- **ID/Created** – Numerische Kennung des Vorfalls in der Konsole / Datum, an dem der Vorfall erstellt wurde.
- **Status** – Einer der folgenden Vorfall-Statuswerte:
 - **Open** – Der Vorfall muss vom Sicherheitsteam bearbeitet werden.
 - **Resolved** – Der Vorfall hat eine vom Sicherheitsteam erstellte Reaktion erhalten.
 - **On hold** – Der Vorfall wird vom Sicherheitsteam vorübergehend nicht bearbeitet.
 - **Closed** – Der Vorfall wurde vom Sicherheitsteam bearbeitet und seine Verarbeitung ist abgeschlossen.
- **Summary** – Einen kurzer Kommentar zum gesamten Vorfall.
- **Tenant** – Ein Mandant, dem ein Vorfall zugewiesen ist.
- **Updated** – Datum und Uhrzeit der Aktualisierung des Vorfalls.

Vorfälle werden entsprechend ihres Aktualisierungszeitpunkts in absteigender Reihenfolge sortiert.

Am Anfang der Vorfallsliste befinden sich die folgenden Schaltflächen:

- Die Schaltfläche **Columns** mit einem Zahnradsymbol, um auszuwählen, welche Spalten auf der Registerkarte **History** angezeigt werden sollen.
- Die Schaltfläche **Filter** mit einem Trichtersymbol, um nur die Änderungen anzuzeigen, die sich auf die ausgewählten Kontrollkästchen beziehen.
- Die Schaltfläche **Search** mit einem Lupensymbol, um nur die Änderungen anzuzeigen, die sich auf die eingegebenen Wörter oder Zeichen beziehen.

2. Wenn Sie die Anzahl der angezeigten Vorfälle pro Listenseite ändern möchten, wählen Sie im unteren Bereich der Seite durch Anklicken der Option **entries per page** eine Zahl aus der Dropdown-Liste aus. Sie können 10, 20 oder 50 Vorfälle pro Seite auswählen.

Wenn Sie durch die Vorfall-Liste navigieren möchten, wählen Sie die gewünschte Seite unterhalb der Liste aus. Mit den Optionen **Zurück** und **Weiter** können Sie zwischen benachbarten Seiten wechseln.

Um die [Vorfälle zu filtern](#), klicken Sie auf das Trichter-Symbol über der Liste.

Sie können die Vorfälle durchsuchen, indem Sie über der Vorfall-Liste neben dem Trichter-Symbol auf die Lupe klicken.

Vorfälle in der MDR Web Console filtern

Um bestimmte Vorfälle anzuzeigen, können Sie Filter erstellen und auf die Vorfall-Liste anwenden.

So erstellen Sie einen Filter für die Vorfall-Liste:

1. Klicken Sie in der MDR Web Console auf den Menüpunkt **Incidents**.

Die Vorfall-Liste wird geöffnet.

2. Klicken Sie über der Vorfall-Liste auf das Trichtersymbol.

Der Block **Filter** wird angezeigt.

Für die Filterung sind folgende Parameter verfügbar:

- **Created**
Zeitpunkt, an der Vorfall erstellt wurde.
- **Updated**
Zeitpunkt, an dem der Vorfall aktualisiert wurde.
- **Priority**
Vorfallpriorität. Mögliche Prioritäten sind Niedrig, Mittel und Hoch.
- **Status**
Vorfallstatus.
- **Resolution**
Auflösung für den Vorfall.
- **Assets**
Verfügbare Assets.
- **Tenant**
Verfügbare Mandanten-Namen.
Sie können den Wert **Root tenant** auswählen, um Vorfälle anzuzeigen, die keinem Ihrer Mandanten zugewiesen sind.
Sie können den Wert **Root tenant** zusätzlich zu angegebenen Namen der Mandanten auswählen.
- **Tactics**
Verfügbare MITRE Tactics zur Reaktion auf Vorfälle.
- **Response statuses**
Zeigt nur Vorfälle mit den ausgewählten Statuswerten der entsprechenden Reaktionen an.

3. Klicken Sie auf **Save**, um den erstellten Filter zu übernehmen. Klicken Sie auf **Clear**, um den erstellten Filter zu verwerfen.

Nachdem der Filter angewendet wurde, werden in der Vorfall-Liste nur Vorfälle angezeigt, die den ausgewählten Parameter des Filters entsprechen.

Benutzerdefinierte Vorfälle in der MDR Web Console erstellen

Das Erstellen benutzerdefinierter Vorfälle ist für einige [kommerzielle Lizenzstufen](#) nicht verfügbar.

Wenn Sie eine Aktivität in Ihrer Infrastruktur als Bedrohung ansehen, aber Kaspersky Managed Detection and Response nicht automatisch einen Vorfall erstellt hat, können Sie einen neuen Vorfall manuell hinzufügen.

Gemäß den Bedingungen des Service Level Agreements (SLA) ist die Anzahl der manuell erstellten Vorfälle, die für die Bearbeitung durch das Sicherheitsteam in Frage kommen, begrenzt. Informationen zu den Einschränkungen sind in [Kaspersky Security Center auf der Registerkarte MDR-Nutzung](#) verfügbar. Auf dieser Registerkarte können Sie die Verwendung der manuell erstellten Ereignisse für den aktuellen Zeitraum (z. B. für die aktuelle Woche) verfolgen:

- Die Gesamtzahl der Vorfälle, die Sie für den aktuellen Zeitraum erstellen können. Diese Vorfälle werden laut SLA vom Sicherheitsteam bearbeitet. Sie können eine größere Anzahl an Vorfällen erstellen, als laut MDR-Erklärung vorgesehen, aber die Einhaltung der SLA-Fristen wird für die Bearbeitung solcher Vorfälle nicht garantiert.
- Die verbleibende Anzahl an Vorfällen, die Sie für den aktuellen Zeitraum erstellen können.

So fügen Sie einen neuen Vorfall hinzu:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Incidents**.

Die Vorfall-Liste wird geöffnet.

2. Klicken Sie im oberen Teil des Fensters auf die Schaltfläche **Add**.

Der neue Vorfall-Block wird angezeigt.

3. Füllen Sie die folgenden Felder aus:

- **Summary**

Einen kurzen Kommentar zum Vorfall.

- **Beschreibung**

Frei wählbare, detaillierte Informationen zum Vorfall. Markdown wird unterstützt

- **Assets**

Das oder die durch den Vorfall gefährdeten Asset(s). Für dieses Feld werden Assets vorgeschlagen, die bereits in der MDR Web Console und in Kaspersky Security Center vorhanden sind.

4. Füllen Sie bei Bedarf das Feld **Tenant** aus.

Für das Feld **Tenant** werden bereits vorhandene Mandanten und der Wert **Root ohne Mandanten** vorgeschlagen.

5. Klicken Sie auf die Schaltfläche **Send**.

Der Block des neuen Vorfalls wird ausgeblendet.

Der neue Vorfall wird der Vorfall-Liste in der MDR Web Console hinzugefügt. Sie können detaillierte Informationen zu diesem Vorfall anzeigen und die Reaktionen auf ihn verarbeiten.

Detaillierte Informationen über Vorfälle in der MDR Web Console anzeigen

So zeigen Sie detaillierte Informationen zu Vorfällen an:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Incidents**.

Die Vorfall-Liste wird geöffnet.

2. Klicken Sie auf die Zeichenfolge mit dem Vorfall, dessen Details Sie anzeigen möchten.

Die Seite des Vorfalls wird geöffnet.

Der Titel der Seite enthält eine Kennung des Vorfalls. Unter dem Titel befinden sich vier Registerkarten:

- **Summary**

Enthält allgemeine Informationen zu dem Vorfall.

- **Responses**

Enthält Informationen zu den Reaktionen auf den Vorfall.

- **Communication**

Enthält sowohl Informationen zur Kommunikation als auch Dateien im Zusammenhang mit dem Vorfall.

- **History**

Enthält Informationen zu den Änderungen des Vorfalls.

Die allgemeine Informationen auf der Registerkarte **Summary** beginnen mit einer kurzen Zusammenfassung des Vorfalls. Weitere in diesem Abschnitt aufgeführte Informationen umfassen:

- Vorfallpriorität
- Vorfallstatus
- Behebung des Vorfalls
- Zeitstempel der Erstellung und Aktualisierung des Vorfalls
- MITRE Tactics
- MITRE Techniques
- Erkennungstechnologie

Unterhalb der Zusammenfassung des Vorfalls sind folgende Informationen aufgeführt:

- **Affected assets**
- **Asset-based IOCs**
- **Network-based IOCs**

Allgemeine Informationen auf der Registerkarte **Summary** enden mit einer Kundenbeschreibung und der Schaltfläche **Close incident**.

3. Wenn Sie wissen, dass es sich bei dem Vorfall um ein Duplikat handelt oder Sie ihn nicht lösen werden, klicken Sie auf die Schaltfläche **Close incident**.

4. [Senden Sie den Vorfall gegebenenfalls an IR-Retainer](#), um ihn zu Untersuchen und etwaige Konsequenzen zu eliminieren.

5. Auf der Registerkarte **Responses** finden Sie Informationen zu angeforderten Reaktionen.

Die Informationen auf der Registerkarte **Responses** werden als Liste dargestellt. Die Liste enthält folgende Spalten:

- **Status**
- **Asset ID**
- **Type**
- **Details**
- **Comment**
- **Changed by**
- **Update time**

6. So fügen Sie einem Vorfall einen Kommentar hinzu:

- a. Geben Sie auf der Seite mit den Informationen zum Vorfall auf der Registerkarte **Communication** Ihren Kommentar in das Textfeld ein.

Markdown und das Anhängen von Dateien werden unterstützt. Die maximale Dateigröße beträgt 10 MB.

- b. Klicken Sie auf die Schaltfläche **Send**.

Der Kommentar wird auf der Seite mit den Informationen zum Vorfall auf der Registerkarte **Communication** hinzugefügt. Nachdem Sie einen Kommentar gepostet haben, können Sie ihn noch 10 Minuten lang bearbeiten oder löschen.

7. Auf der Registerkarte **History** finden Sie Informationen über die Änderungen des Vorfalls.

Unter dem Titel befindet sich ein Umschalter zum Anzeigen von Änderungen in Bezug auf:

- **All events**
- **Only incidents**
- **Only responses**
- **Only communication**

Neben diesem Schalter befinden sich die folgenden Schaltflächen:

- Die Schaltfläche **Columns** mit einem Zahnradsymbol, um auszuwählen, welche Spalten auf der Registerkarte **History** angezeigt werden sollen.
- Die Schaltfläche **Filter** mit einem Trichtersymbol, um nur die Änderungen anzuzeigen, die sich auf die ausgewählten Kontrollkästchen beziehen.
- Die Schaltfläche **Search** mit einem Lupensymbol, um nur die Änderungen anzuzeigen, die sich auf die eingegebenen Wörter oder Zeichen beziehen.

Reaktionen auf Vorfälle in der MDR Web Console verarbeiten

Sie können [Reaktionen](#) auf Vorfälle anzeigen, akzeptieren und ablehnen.

So zeigen Sie Reaktionen auf einen Vorfall an:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Incidents**.

Die Vorfall-Liste wird geöffnet.

2. Klicken Sie auf die Zeichenfolge mit dem Vorfall, dessen Details Sie anzeigen möchten.

Die Seite des Vorfalls wird geöffnet.

3. Klicken Sie auf der Seite des Vorfalls auf die Registerkarte **Responses**.

Die Reaktions-Liste wird geöffnet.

Jede Zeile steht für eine Reaktion. Zur einer Reaktion werden die folgenden Informationen angezeigt:

- **Status**

Status der Reaktion.

- **Asset ID**

Kennung des Assets, für das die Reaktion ausgeführt werden soll.

- **Type**

Typ des Objekts, aus dem die Reaktion besteht.

- **Parameters**

Vom Betriebssystem abhängiger lokaler Pfad zum Abrufen der Reaktionsdatei und der erwarteten Dateigröße in MB. Die maximale Dateigröße beträgt 10 MB.

- **Comment**

Letzter Kommentar zu der Reaktion.

- **Changed by**

Letzter Benutzer, der die Reaktionsbeschreibung geändert hat.

Um die Reaktionsbeschreibung anzuzeigen, klicken Sie auf die Zeichenfolge mit der Reaktion.

So akzeptieren Sie Reaktionen auf einen Vorfall oder lehnen sie ab:

1. Navigieren Sie in der Konsole zum Menüelement **Incidents**.

Die Vorfall-Liste wird geöffnet.

2. Klicken Sie auf die Zeichenfolge mit dem Vorfall, dessen Details Sie anzeigen möchten.

Die Seite des Vorfalls wird geöffnet.

3. Klicken Sie auf der Seite des Vorfalls auf die Registerkarte **Responses**.

Die Reaktions-Liste wird geöffnet.

4. Wählen Sie eine Reaktion aus, die Sie genehmigen oder ablehnen möchten. Dies tun Sie, indem Sie das Kontrollkästchen am linken Ende der Zeichenfolge aktivieren, welche die Reaktion enthält.

Sie können auch mehrere Reaktionen auswählen, indem Sie links die entsprechenden Kontrollkästchen aktivieren. Um alle Reaktionen auszuwählen, aktivieren Sie in der Reaktionstabelle das Kontrollkästchen im linken Teil der Überschrift.

5. Um Reaktionen zu genehmigen oder abzulehnen, wählen Sie unter der Reaktions-Liste entweder die Schaltfläche **Accept** oder **Reject**. Das Kommentarfeld wird angezeigt. Geben Sie Ihren Kommentar ein und klicken Sie anschließend auf die Schaltfläche **Send**.

Sie können auf der Registerkarte **Responses** auch eine Reaktion anklicken, um deren Details zu überprüfen und diese Reaktion im eingblendeten Seitenbereich zu akzeptieren oder abzulehnen. Um die Reaktion abzulehnen, müssen Sie Ihren Kommentar in das Feld im Seitenbereich eingeben.

Der Reaktionsstatus wird geändert.

Arten von Reaktionen

Die MDR-Lösung untersucht Vorfälle und erstellt Reaktionen, die Sie entweder akzeptieren oder ablehnen können. Dies ist die Standardmethode für die Bearbeitung von Vorfällen in Kaspersky Managed Detection and Response.

Sie können jedoch auch Reaktionen manuell erstellen, indem Sie [die Funktionen von Kaspersky Endpoint Detection und Response Optimum verwenden](#).

In diesem Artikel werden nur die Arten von Reaktionen beschrieben, die von der MDR-Lösung erstellt werden.

Jede Reaktion kann eine Reihe von Parametern aufweisen, die auf der Registerkarte **Responses** eines Vorfalls angezeigt werden.

Die möglichen Arten von Reaktionen sind:

- **Get file**

Die Kopie einer Datei aus Ihrer Infrastruktur wird an das SOC von Kaspersky gesendet. Wenn Sie diese Reaktion akzeptieren, wird einer Kopie der angegebenen Datei an das SOC von Kaspersky SOC gesendet.

Beachten Sie, dass dieser Art von Reaktion auch Dateien mit persönlichen und/oder vertraulichen Daten abrufen kann.

Die möglichen Parameter sind:

- **Infected file path**

Der absolute Dateipfad. Beispiel: C:\\file.exe.

- **Maximum file size**

Die maximale Dateigröße in MB.

Wenn die infizierte Datei die angegebene maximale Dateigröße überschreitet, wird der Versuch, die Reaktion zu akzeptieren, fehlschlagen und die Reaktion wird nicht durchgeführt. Sie wird aber auf der Registerkarte **History** des Vorfalls angezeigt.

- **Isolate**

Die angegebenen Assets werden vom Netzwerk isoliert.

Falls Sie die Netzwerkisolation dringend deaktivieren müssen, [wenden Sie sich bitte an den Technischen Support](#) oder schreiben Sie auf der Registerkarte **Communication** des Vorfalls seine Anfrage.

Die möglichen Parameter sind:

- **Password for disabling isolation**

Das Kennwort zum Deaktivieren der Isolation. Sobald der Technische Support Ihre Anfrage zur Deaktivierung der Netzwerkisolation erhält, wird er Ihnen Details zum Verfahren und zur Verwendung des Passworts zusenden.

- **Aufgaben-ID**

Die eindeutige Aufgabenkennung, die in Kombination mit dem **Password for disabling isolation** verwendet wird, um die Netzwerkisolation manuell zu deaktivieren.

- **Password details**

Sie können die Gültigkeit des **Kennworts** überprüfen, indem Sie daraus einen abgeleiteten Schlüssel generieren und den resultierenden Wert mit dem Wert im Parameter **Derived key** vergleichen.

- **Version**

Die numerische Version für die Darstellung der Regeln zur Kennworterstellung. Eine Version von 1 bedeutet, dass die folgenden PBKDF2-Parameter zum Erstellen eines abgeleiteten Schlüssels verwendet werden:

- HMACSHA256-Hash-Algorithmus
 - 10.000 Iterationen
 - 32 Byte Schlüssellänge

- **Salt**

Der Salt im HEX-Format zum Abrufen eines abgeleiteten Schlüssels über PBKDF2.

- **Derived key**

Der abgeleitete Schlüssel im HEX-Format.

- **Exclude rules**

Array von Regeln mit benutzerdefinierten Ports, Protokollen, IP-Adressen und Prozessen, auf die keine Isolation angewendet wird.

- **Direction**

Die Richtung des Datenverkehrs. Die möglichen Werte sind: **Inbound**, **Outbound**, **Both**.

- **Protokoll**

Die Protokollnummer gemäß der [IANA-Spezifikation](#) ^[4].

Die möglichen Werte sind:

- **1** (ICMP)
- **6** (TCP)
- **17** (UDP)
- **58** (IPv6-ICMP)

- **Remote port range**

Der Remote-Portbereich wird in den verschachtelten Feldern **From** und **To** angegeben.

- **Remote IPv4 address**

Die Remote-IPv4-Adresse oder Subnetzmaske.

- **Remote IPv6 address**

Die Remote-IPv6-Adresse oder Subnetzmaske.

- **Local port range**

Der lokale Portbereich wird in den verschachtelten Feldern **From** und **To** angegeben.

- **Local IPv4 address**

Die lokale IPv4-Adresse oder Subnetzmaske.

- **Local IPv6 address**

Die lokale IPv6-Adresse oder Subnetzmaske.

- **Process**

Der Pfad zum Prozess-Image wird in den verschachtelten Feldern **Image** → **Path** angegeben.

- **Disable isolation**

Deaktivieren der Netzwerkisolation des angegebenen Assets.

- **Delete registry key**

Löschen eines Registrierungsschlüssels oder eines Unterabschnitts der Registrierung für das angegebene Asset.

Diese Aktion kann nicht rückgängig gemacht werden.

Die möglichen Parameter sind:

- **Key**

Der absolute Schlüsselpfad, der mit HKEY_LOCAL_MACHINE oder HKEY_USERS beginnt. Beispiel: HKEY_LOCAL_MACHINE\SYSTEM\WebClient.

Wenn der Schlüssel ein symbolischer Link ist, wird nur dieser Schlüssel gelöscht, während der Zielschlüssel des Links intakt bleibt.

- **Value**

Der Schlüsselwert.

Wird dieser Parameter nicht angegeben, wird der Schlüssel rekursiv gelöscht. Beim rekursiven Löschen wird jeder Unterschlüssel, der ein symbolischer Link ist, gelöscht, während sein Zielschlüssel intakt bleibt.

Wenn der Schlüsselwert eine leere Zeichenfolge ist, wird der Standardwert gelöscht.

- **Memory dump**

Erstellen eines Speicher-Dumps und Senden des Dumps an das SOC von Kaspersky.

Die möglichen Parameter sind:

- **Dump type**

Ein Speicher-Dump kann einem von zwei Typen entsprechen:

- **Full memory dump**

Ein Abbild des gesamten Speichers eines Assets.

- **Process dump**

Ein Abbild eines angegebenen Prozesses.

- **Maximum file size**

Die maximale Dateigröße für den Dump im zip-Format in MB. Der Standardwert ist 100 MB.

- **Process**

Die Prozess-ID und Image-Details.

- **Image**

- **Path**

Der absolute Dateipfad. Beispiel: %systemroot%\system32\svchost.exe.

- **SHA-256**

Die SHA256-Prüfsumme im HEX-Format.

- **MD5**

Die MD5-Prüfsumme im HEX-Format.

- **Unique ID**

Die eindeutige Prozesskennung.

- **Process count limit**

Die maximale Anzahl von Prozessen, die in der Dump-Datei enthalten sein können.

- **Terminate process**

Beenden eines Prozesses auf einem angegebenen Asset mit Kaspersky Endpoint Security für Windows. Der zu beendende Prozess kann durch seinen Namen oder die Prozesskennung (PID) angegeben werden.

- **Run process**

Ausführung eines Skriptes auf einem angegebenen Asset mit Kaspersky Endpoint Security für Windows.

Für diese Reaktion muss die PowerShell-Umgebung auf dem Asset installiert sein. Sie können das auszuführende Skript und seine Beschreibung in der [MDR Web Console](#) anzeigen.

- **Quarantine file**

Verschiebt eine potenziell gefährliche Datei in einem speziellen lokalen Speicherbereich. Die Dateien in diesem Speicherbereich werden verschlüsselt und stellen keine Gefahr für die Sicherheit Ihres Geräts dar. Es wird eine Bestätigungsanfrage angezeigt, in der das betroffene Asset sowie der Hash (MD5 oder SHA256) und der Pfad der Datei angegeben sind.

- **Datei aus Quarantäne wiederherstellen**

Stellt eine Datei, zuvor in die Quarantäne verschobene wurde, an ihrem ursprünglichen Speicherort wieder her. Wenn sich am ursprünglichen Speicherort eine Datei mit demselben Namen befindet, wird die Wiederherstellung nicht ausgeführt.

- **Get artefacts**

Bei dieser Art von Antwortreaktion können Dateien mit personenbezogenen und vertraulichen Daten übertragen werden.

Verfügbar, wenn Sie die Integration mit Kaspersky Anti Targeted Attack Version 8.0 oder höher konfiguriert haben

Kopiert Dateien, die sich auf Alarme aus Kaspersky Anti Targeted Attack beziehen, aus der Infrastruktur von Kaspersky Anti Targeted Attack zum Kaspersky SOC. Die kopierten Dateien werden von MDR-SOC-Analysten verwendet, um Alarme aus Kaspersky Anti Targeted Attack zu untersuchen.

Die möglichen Parameter sind:

- ID des Knotens mit der Kaspersky Anti Targeted Attack-Lösung.
- ID des Alarms in Kaspersky Anti Targeted Attack.
- Kategorien der Dateien, die sich auf Alarme beziehen und zum Kaspersky SOC kopiert werden:
 - PCAP- und Payload-Dateien, die sich auf einen IDS-Alarm beziehen.
 - Bericht über das Ergebnis der Datei-Untersuchung in der Sandbox. Enthält Screenshots der Objektausführung, das Aktivitätsprotokoll und andere Untersuchungsdaten.
 - Die infizierte, an die Sandbox gesendete Datei.
 - Datei mit den Alarm-Details.

Verfügbar, wenn Sie die Integration mit Kaspersky Next XDR Expert 2.1 konfiguriert haben

Kopiert Dateien, die sich auf Alarme oder Vorfälle aus Kaspersky Endpoint Detection and Response Expert in der Infrastruktur der Open Single Management Plattform beziehen, nach Kaspersky SOC. Die kopierten Dateien werden von MDR-SOC-Analysten verwendet, um Alarme und Vorfälle aus Kaspersky Endpoint Detection and Response Expert zu untersuchen.

Die möglichen Parameter sind:

- ID des Knotens der Lösung.
- ID des Alarms oder Vorfalls aus XDR.
- Kategorien der Dateien, die sich auf Alarme oder Vorfälle beziehen und zum Kaspersky SOC kopiert werden:
 - Dateien, die zu dem Alarm oder Vorfall aus XDR hochgeladen wurden.
 - Bericht über das Ergebnis der Datei-Untersuchung in der Sandbox. Enthält Screenshots der Objektausführung, das Aktivitätsprotokoll und andere Untersuchungsdaten.
 - Die infizierte, an die Sandbox gesendete Datei.
 - Dateien, die sich auf die von Benutzern ausgeführten Reaktionen für den Alarm oder den Vorfall beziehen:
 - Dateien abrufen
 - Forensische Daten sammeln
 - Registrierungsschlüssel erfassen
 - Dateien des NTFS-Dateisystemdienstes abrufen
 - Dumps der Prozess-Speicher erstellen
 - Dateien in Quarantäne verschieben
- Informationen zu allen Dateien, die sich auf den Alarm beziehen.
- Namen und IDs der kopierten Dateien.

Auto-Akzeptieren von Reaktionen in der MDR Web Console

Sie können für vorgeschlagene Reaktionen das automatische Akzeptieren (Auto-Akzeptieren) aktivieren. In diesem Fall werden die in den Reaktionen vorgeschlagenen Aktionen, beispielsweise das Löschen einer infizierten Datei, automatisch ausgeführt. Wenn diese Funktion deaktiviert ist, müssen [die in den Reaktionen vorgeschlagenen Maßnahmen](#) manuell akzeptiert oder abgelehnt werden.

Wenn Sie Mandanten einsetzen, können Sie das Auto-Akzeptieren von Reaktionen sowohl für alle Mandanten als auch für ausgewählte Mandanten aktivieren. Wenn Sie keine Mandanten einsetzen, können Sie diese Funktion für Ihre aktuelle Organisation aktivieren oder deaktivieren.

So aktivieren Sie das Auto-Akzeptieren von Reaktionen:

1. Navigieren Sie im Fenster der MDR Web Console zum Menüpunkt **Settings**.
2. Klicken Sie auf die Registerkarte **Incidents**.
3. Wählen Sie eine der folgenden Optionen aus:

- **Enabled for all tenants**

Wenn diese Option ausgewählt ist, wird das Auto-Akzeptieren von Reaktionen sowohl für vorhandene als auch für neu erstellte Mandanten aktiviert.

- **Enabled for the tenants selected below**

Wählen Sie die Mandanten aus, für welche Sie das Auto-Akzeptieren von Reaktionen aktivieren möchten. Für neu erstellte Mandanten ist das Auto-Akzeptieren von Reaktionen standardmäßig deaktiviert.

4. Klicken Sie auf **Save**.

Auto-Akzeptieren von Reaktionen ist aktiviert und die in den Reaktionen vorgeschlagenen Maßnahmen werden automatisch für alle Mandanten oder die von Ihnen ausgewählten Mandanten ausgeführt. Sie können diese Option jederzeit deaktivieren.

Zugriffsrechte zum Anzeigen oder Ändern der Auto-Akzeptieren-Einstellungen

Die [Benutzerrollen von Kaspersky Managed Detection and Response](#) haben die folgenden Zugriffsrechte auf die Auto-Akzeptieren-Einstellungen:

Vorgang	MDR-Administrator	Senior Security Officer	Security Officer
Zugriff auf die Registerkarte Incidents	✓	✓	—
Ändern der aktuell ausgewählten Option	✓	—	—
Anzeigen der aktuell ausgewählten Option	✓	✓	—
Aktivieren von Auto-Akzeptieren für alle Mandanten	✓	—	—
Aktivieren von Auto-Akzeptieren für ausgewählte Mandanten	✓	✓ (nur jene Mandanten, auf die der Benutzer Zugriff hat)	—
Anzeigen der Auto-Akzeptieren-Einstellungen eines bestimmten Mandanten	✓	✓ (nur jene Mandanten, auf die der Benutzer Zugriff hat)	—

Auto-Akzeptieren von Reaktionen in Kaspersky Security Center

Sie können für vorgeschlagene Reaktionen das automatische Akzeptieren (Auto-Akzeptieren) aktivieren. In diesem Fall werden die in den Reaktionen vorgeschlagenen Aktionen, beispielsweise das Löschen einer infizierten Datei, automatisch ausgeführt. Wenn diese Funktion deaktiviert ist, müssen [die in den Reaktionen vorgeschlagenen Maßnahmen](#) manuell akzeptiert oder abgelehnt werden.

Wenn Sie Mandanten einsetzen, können Sie das Auto-Akzeptieren von Reaktionen sowohl für alle Mandanten als auch für ausgewählte Mandanten aktivieren. Wenn Sie keine Mandanten einsetzen, können Sie diese Funktion für Ihre aktuelle Organisation aktivieren oder deaktivieren.

Wenn Sie die Benutzerrolle "MDR-Administrator" besitzen, können Sie die Einstellungen von Auto-Akzeptieren ändern. Benutzer mit der Rolle "Security Officer" dürfen die Einstellungen nicht ändern. Benutzer mit der Rolle "Senior Security Officer" können die folgenden Vorgänge ausführen:

- Anzeigen der aktuell ausgewählten Option
- Aktivieren oder deaktivieren des Auto-Akzeptierens von Reaktionen für bestimmte Mandanten, wenn die Option **Ändern der Reaktionsoption von Auto-Akzeptieren für jeden Mandanten erlauben** ausgewählt ist

So konfigurieren Sie das Auto-Akzeptieren von Reaktionen:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **Einstellungen**.

2. Wählen Sie in der Parametergruppe **Auto-Akzeptieren von Reaktionen** die erforderliche Option aus:

- **Auto-Akzeptieren von Reaktionen für alle Mandanten deaktivieren**

Wählen Sie diese Option, wenn Sie Reaktionsmaßnahmen manuell annehmen oder ablehnen möchten.

- **Ändern der Reaktionsoption von Auto-Akzeptieren für alle Mandanten erlauben**

Wählen Sie diese Option, wenn Sie das Auto-Akzeptieren von Reaktionen für alle Mandanten in Ihrer Organisation aktivieren möchten, einschließlich der bereits vorhandenen und neu erstellten Mandanten.

- **Ändern der Reaktionsoption von Auto-Akzeptieren für jeden Mandanten erlauben**

Wählen Sie diese Option, wenn Sie das Auto-Akzeptieren von Reaktionen für jeden Mandanten individuell konfigurieren möchten. Aktivieren Sie anschließend die Kontrollkästchen jener Mandanten, für welche die Reaktionsmaßnahmen automatisch ausgeführt werden sollen. Für neu erstellte Mandanten ist das Auto-Akzeptieren von Reaktionen standardmäßig deaktiviert.

Wenn Sie die Option **Alle Mandanten** auswählen, ist das Auto-Akzeptieren von Reaktionen für neu erstellte Mandanten standardmäßig aktiviert.

3. Klicken Sie auf **Speichern**.

Die Schaltfläche **Speichern** wird erst aktiv, wenn Sie Einstellungen geändert haben.

Vorfälle in der MDR Web Console schließen

Sie können einen Vorfall schließen, wenn Sie wissen, dass es sich um ein Duplikat handelt oder wenn Sie ihn nicht beheben werden. In anderen Fällen dürfen Sie Vorfälle nicht schließen, da sie von der MDR-Lösung behoben werden müssen. Die MDR-Lösung behebt einen Vorfall, wenn die in diesem Vorfall empfohlenen Maßnahmen umgesetzt werden. Ein behobener Vorfall wird nach 72 Stunden automatisch geschlossen.

So schließen Sie einen Vorfall:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Incidents**.

Die Vorfall-Liste wird geöffnet.

2. Klicken Sie auf die Zeichenfolge mit dem Vorfall, dessen Details Sie anzeigen möchten.

Die Seite des Vorfalls wird geöffnet.

3. Klicken Sie auf der Seite auf der Registerkarte **Summary** auf die Schaltfläche **Close incident** im unteren Teil des Fensters.

Für Vorfälle, die den Status **Closed** haben, gibt es die Schaltfläche **Close incident** nicht.

Der Block **Close incident** wird angezeigt.

4. Geben Sie im Feld **Reason why you are closing this incident** alle zusätzlichen Informationen an, die Sie an die SOC-Analysten von Kaspersky Managed Detection and Response weitergeben möchten. Sie können beispielsweise angeben, warum Sie diesen Vorfall für eine normale, nicht bedrohliche Situation für Ihre Infrastruktur halten. Sie können dieses Feld leer lassen.

5. Wählen Sie unter dem Kommentarfeld je nach Grund der Schließung die Option **True positive** oder **False positive** aus.

Wählen Sie die Option **True positive** aus, wenn Kaspersky Managed Detection and Response eine Bedrohung erkannt hat, Sie aber nicht möchten, dass die MDR-SOC-Analysten den Vorfall untersuchen und beheben.

Wählen Sie die Option **False positive** aus, wenn Kaspersky Managed Detection and Response eine nicht bedrohliche Aktivität als Bedrohung erkannt hat. Kaspersky Managed Detection and Response verwendet diese Informationen, um die automatischen Erkennungsalgorithmen zu verbessern.

6. Klicken Sie im unteren Teil des Blocks auf die Schaltfläche **Close**.

Das Formular **Feedback geben** wird angezeigt.

7. Wählen Sie im Formular **Feedback geben** eine Bewertung zwischen 1 und 5 aus. Sie können auch einen Kommentar in Textform zum Umgang mit diesem Vorfall hinterlassen. Das Feedback wird von Kaspersky-Experten verarbeitet, um die Leistung der MDR-Lösung zu verbessern.

8. Klicken Sie auf **Absenden**.

Der Block **Close incident** wird ausgeblendet.

Der Vorfall ist geschlossen. Von nun an führt Kaspersky Managed Detection and Response keine Aktionen in Bezug auf diesen Vorfall mehr durch.

Vorfall zur weiteren Untersuchung an das Sicherheitsvorfall-Reaktionsteam senden

Sie können einen Vorfall zur [Untersuchung an das Sicherheitsvorfall-Reaktionsteam](#) senden. Dieser Dienst umfasst das vollständige Spektrum an Reaktionen: von der anfänglichen Analyse und ersten Reaktionen bis zur Erkennung zusätzlicher Angriffsmerkmale und Erstellung eines Plans zur Beseitigung möglicher Folgen.

Wenn Sie für das Abonnement dieses Dienstes bezahlen, erhalten Sie eine bestimmte Anzahl von Untersuchungsstunden. Diese Untersuchungsstunden werden angerechnet, wenn Sie einen Vorfall an das Sicherheitsvorfall-Reaktionsteam senden. Wenn Sie keine Untersuchungsstunden zur Verfügung haben, können Sie trotzdem einen Vorfall zur Untersuchung einsenden. Dafür müssen Sie einen kommerziellen Dienst erwerben und manuell eine Anfrage erstellen.

Die Untersuchungsergebnisse erhalten Sie auf der Registerkarte **Communication** für den Vorfall.

Benutzer mit den Rollen MDR Administrator oder Senior Security Officer dürfen Vorfälle an das Sicherheitsvorfall-Reaktionsteam senden.

So senden Sie einen Vorfall an das Sicherheitsvorfall-Reaktionsteam:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Incidents**.

Die Vorfall-Liste wird geöffnet.

2. Klicken Sie auf den Eintrag mit dem Vorfall, den Sie an das Sicherheitsvorfall-Reaktionsteam senden möchten.

Die Seite des Vorfalls wird geöffnet.

3. Führen Sie auf der Registerkarte **Summary** im Abschnitt **Actions** einen der folgenden Schritte aus:

- Wenn Sie über Untersuchungsstunden verfügen, klicken Sie auf **Escalate incident to the IR team** und bestätigen Sie dann, dass Sie den Vorfall das Sicherheitsvorfall-Reaktionsteam senden möchten.
- Wenn Sie nicht über Untersuchungsstunden verfügen, klicken Sie auf den Link und füllen Sie das Anfrageformular aus, um einen kommerziellen Dienst zu erwerben.

Der Vorfall wird gesendet. Nachdem das Sicherheitsvorfall-Reaktionsteam den Vorfall erhalten hat, melden sich die Experten so schnell wie möglich über MDR Web Console bei Ihnen.

Integration von Kaspersky Unified Monitoring and Analysis

Kaspersky Unified Monitoring and Analysis Platform (KUMA) ist eine integrierte Software-Lösung, welche die folgenden Funktionen vereint:

- Empfangen, Verarbeiten und Speichern von Ereignissen zur Informationssicherheit
- Analyse und Korrelation eingehender Daten
- Durchsuchen abgerufener Ereignisse
- Erstellen von Benachrichtigungen über erkannte Indikatoren von Gefahren der Informationssicherheit

Sie können die Integration von Kaspersky Managed Detection and Response in KUMA Version 4.0 oder höher so konfigurieren, dass KUMA-Daten automatisch in MDR importiert werden.

Der folgende Artikel erklärt, wie Sie die Integration konfigurieren: [Integration von Kaspersky Endpoint Managed Detection and Response](#).

Vorfälle für Managed Detection and Response aus XDR-Vorfällen erstellen

Sie können aus einem XDR-Vorfall einen MDR-Vorfall erstellen, wenn die Integration mit Managed Detection and Response in der Open Single Management Platform aktiviert ist und die Alarme der XDR-Vorfälle die folgenden Bedingungen erfüllen:

- Die Quelle der Erkennung ist ein Endpunkt.
- Es ist mindestens ein zugehöriges Asset im Alarm enthalten.
- Eine der folgenden Erkennungstechnologien wurde verwendet:
 - IOA-Regeln von Kaspersky
 - SB (Sandbox)
 - AM (Anti-Malware Engine)
 - IOC
 - YARA

Es wird empfohlen, dass Sie die MDR-Lösung auf allen verwalteten Assets aktivieren, um einen ununterbrochenen verwalteten Schutz mit automatisierter Bedrohungserkennung zu gewährleisten. Dies entlastet die Mitarbeiter der IT-Security, welche sich anderen Aufgaben zuwenden können.

So exportieren Sie einen XDR-Vorfall zu MDR:

1. Navigieren Sie im Hauptmenü der Konsolenoberfläche von OSMP zu **Überwachung** → **Vorfälle**.
2. Klicken Sie in der Tabelle mit den Vorfällen auf die ID des erforderlichen Vorfalls. Das Fenster mit den Vorfalldetails wird angezeigt.
3. Klicken Sie in der Werkzeugleiste auf das Symbol mit den drei Punkten und wählen Sie **MDR-Vorfall** erstellen aus.
4. Geben Sie im Dialog **MDR-Vorfall erstellen** den Namen und die Beschreibung des Vorfalls an und klicken Sie auf **Erstellen**.

Wenn der Vorfall erfolgreich erstellt wurde, wird eine entsprechende Meldung angezeigt. Sie können jetzt in der MDR Web Console auf diesen Vorfall zugreifen. Der Link zum Vorfall ist im Abschnitt **Zusammenfassung** des XDR-Vorfalls verfügbar.

Integration von Kaspersky Digital Footprint Intelligence für MDR

Die MDR-Lösung kann von Kaspersky Digital Footprint Intelligence (DFI) identifizierte kompromittierte Anmeldeinformationen verwenden, um die Arbeitsabläufe für den Fund und die Untersuchung von Bedrohungen sowie für das Threat Hunting zu optimieren.

Kunden benötigen keine aktive Lizenz für Kaspersky DFI, um diese Funktion nutzen zu können. Die Daten von Kaspersky DFI sind im Rahmen der entsprechenden MDR-Funktionalität verfügbar.

Die MDR-Lösung analysiert offengelegte Anmeldeinformationen, die für das Kundenunternehmen und die damit verbundenen, von der MDR-Überwachung abgedeckten Assets relevant sind. Der primäre Schwerpunkt liegt auf offengelegten Anmeldeinformationen im Zusammenhang mit Infostealern, die auf eine mögliche Kompromittierung des Geräts eines Mitarbeiters hindeuten können.

Die Daten von Kaspersky DFI werden von MDR für die folgende Funktionalität verwendet:

- Anreicherung von Alarmen um Kontext zu offengelegten Anmeldeinformationen;
- Korrelation abgeflossener Anmeldeinformationen mit Sicherheitsereignissen;
- Threat Hunting und Fund potenzieller Kompromittierungen anhand von Informationen zu Anmeldeinformationen.

Die Integration von Kaspersky DFI hilft der MDR-Lösung, potenziell kompromittierte Konten schneller zu identifizieren, damit zusammenhängende Vorfälle besser zu priorisieren und das Risiko unbefugter Zugriffe zu verringern.

Neben offengelegten Anmeldeinformationen im Zusammenhang mit Infostealern kann Kaspersky DFI auch öffentlich zugängliche offengelegte Anmeldeinformationen aus Ressourcen von Drittanbietern analysieren, in denen ebenfalls Anmeldeinformationen von Mitarbeitern vorkommen können. Der Überwachungsumfang kann sich auch auf Partner und andere mit der Organisation verbundene Einrichtungen erstrecken.

Zusammenfassend stellt Kaspersky DFI MDR Erkenntnisse über kompromittierte Anmeldeinformationen bereit, während MDR diese Daten durch die Anreicherung von Alarmen, Korrelation und Threat Hunting in SOC-Arbeitsabläufen einsetzt.

Funktionen von Kaspersky Endpoint Detection and Response Expert verwenden

Die Integration von Kaspersky Endpoint Detection and Response Expert in die Open Single Management Platform ermöglicht die folgende Funktionalität:

- Kaspersky Endpoint Detection and Response sendet Alarmdaten an MDR, wodurch Sie Telemetriedaten und Alarme von Endpoint Detection and Response in der MDR-Lösung verarbeiten können.
- [Die Möglichkeit, MDR-Vorfälle aus XDR-Vorfällen zu erstellen](#).
- Im Rahmen der [Art der Reaktion](#) können Artefakte abgerufen werden.

Integration mit Kaspersky Endpoint Detection and Response Expert aktivieren

Für die Konfiguration der Integration wird die Rolle MDR-Administrator benötigt.

So aktivieren Sie die Integration:

1. [Konfigurieren Sie das MDR-Plug-in](#) in der Konsole der Open Single Management Platform.
2. Klicken Sie in der Konsolenoberfläche von OSMP im MDR-Abschnitt auf die Registerkarte **MDR-Nutzung**.
3. Erweitern Sie den Block **KPSN-Konfigurationsdatei für die Integration mit KEDR Expert**.
4. Aktivieren Sie die Option **KPSN-Vereinbarung akzeptieren** und klicken Sie auf **KPSN-Konfigurationsdatei für die Integration mit KEDR Expert anwenden**.

Die Integration ist aktiviert.

Reaktionen

[Kaspersky Endpoint Detection and Response Expert](#) bietet im Rahmen von Reaktionen die folgenden Funktionen an (im Weiteren auch als EDR-Reaktionen bezeichnet), die Sie manuell ausführen und konfigurieren können.

- Netzwerkisolation
- Datei in Quarantäne verschieben
- Dateien an Cloud Sandbox senden
- Datei löschen
- Untersuchung kritischer Bereiche ausführen
- IOC-Untersuchung ausführen

- Ausführungsprävention
- Einen Prozess starten
- Prozess beenden
- Datei abrufen

Weitere Informationen zu diesen EDR-Reaktionen finden Sie in der [Online-Hilfe von Kaspersky Endpoint Detection and Response Expert](#).

Die in diesem Abschnitt beschriebenen EDR-Reaktionen sind für Assets mit Kaspersky Endpoint Security für Windows 11.7 oder höher verfügbar. Wenn Sie Kaspersky Endpoint Security für Windows 11.6 oder älter für Ihre Assets verwenden, muss auf diesen Assets Kaspersky Endpoint Agent installiert sein, um die EDR-Reaktionen verarbeiten zu können.

Um die Maßnahmen von Reaktion auf EDR-Warnungen zu verwalten, wechseln Sie in [Kaspersky Security Center](#) zum Abschnitt **Überwachung und Berichterstattung** → **Alarme**.

Verwalten von Mandanten

Mandantenfähigkeit ist ein Mechanismus, der es Ihnen ermöglicht, für andere Unternehmen als Anbieter von Kaspersky Managed Detection and Response-Lieferant aufzutreten. Sobald Sie über ein MDR-Konto verfügen, können Sie in Ihrem MDR-Konto [Mandanten](#) erstellen.

Sie können in Ihrer Organisation bis zu 100 Mandanten erstellen.

Ihr Benutzerkonto in Kaspersky Security Center Web Console oder Kaspersky Next Expert View muss über eine Rolle mit den folgenden [Zugriffsrechten](#) verfügen: **Zugriff auf Vorfälle** und **Verwaltung von Mandanten** sowie über die Möglichkeit, Mandanten im Abschnitt **MDR** in Kaspersky Security Center anzuzeigen, hinzuzufügen, zu bearbeiten und zu löschen.

Wenn Ihre Organisation über mehrere Lizenzen verfügt, können Sie die [Mandanten nur in Kaspersky Security Center verwalten](#).

Um MDR-Anbieter zu werden, benötigen Sie Zugriff auf die Infrastruktur Ihres Mandanten, um die Bereitstellungsszenarien durchführen zu können.

Alle Mandanten sind unabhängig und isoliert, so dass ein Mandant nicht auf die Daten eines anderen Mandanten zugreifen kann.

Assets mit Kaspersky Embedded Systems Security for Windows und Kaspersky Embedded Systems Security for Linux können nur dem Root-Mandanten zugewiesen werden.

Nur Benutzer, denen die Rolle [MDR-Administrator](#) zugewiesen ist, können Mandanten in der MDR Web Console hinzufügen, bearbeiten und löschen.

Mandanten in Kaspersky Security Center verwalten

Dieser Abschnitt enthält Informationen über die Verwaltung vorhandener Mandanten und über das Hinzufügen neuer Mandanten in Kaspersky Security Center.

Mandanten in Kaspersky Security Center anzeigen

Sie können verfügbare Mandanten anzeigen, indem Sie die Mandantenliste verwenden.

Ihr Benutzerkonto in Kaspersky Security Center Web Console oder Kaspersky Next Expert View muss über eine Rolle mit den folgenden [Zugriffsrechten](#) verfügen: **Zugriff auf Vorfälle** und **Verwaltung von Mandanten** sowie über die Möglichkeit, Mandanten im Abschnitt **MDR** in Kaspersky Security Center anzuzeigen, hinzuzufügen, zu bearbeiten und zu löschen.

So zeigen Sie Mandanten an:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **Mandanten**.

Die Liste **Mandanten** wird angezeigt. Jede Zeile steht für einen Mandanten. Sie können auf den Namen eines Mandanten klicken, um Informationen über den Mandanten anzuzeigen.

2. Die folgenden Mandantenattribute sind über der Liste vorhanden:

Name

Ein beliebiger, für Menschen lesbarer Name des Mandanten, den Sie beim Erstellen des Mandanten angeben. Ein Mandantennamen kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 100 Zeichen nicht überschreiten. Mandanten können nicht umbenannt werden.

Status

Folgende Statuswerte sind für Mandanten möglich:

- **Aktiv**

Der Mandant kann Kaspersky Managed Detection and Response verwenden.

- **Inaktiv**

Der Mandant kann Kaspersky Managed Detection and Response nicht verwenden.

Sie können den Status "Inaktiv" in der Mandantenkarte manuell einstellen. Zusätzlich wird der Status "Inaktiv" am Ende der Lebensdauer des Mandanten automatisch eingestellt.

Assets / Limit

Anzahl der Assets, die einem Mandanten zugeordnet sind / Asset-Limit.

Das Asset-Limit wird beim Erstellen zusätzlicher Mandanten angegeben und dient nur zu Informationszwecken. Eine Überschreitung des Limits ist zulässig und hat keinen Einfluss auf die Funktionsfähigkeit der MDR-Lösung.

Beschreibung

Frei wählbare Informationen, die Sie beim Erstellen oder Bearbeiten des Mandanten eingeben. Beispiele hierfür sind der Verwendungszweck des Mandanten oder die voraussichtliche Anzahl der Assets. Die Beschreibung kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 2000 Zeichen nicht überschreiten.

Erstellt am

Datum, an dem der Mandant erstellt wurde.

Ablaufdatum

Datum, an dem die Lebensdauer des Mandanten abläuft.

Vorfälle werden entsprechend ihrer Gültigkeitszeiträume in absteigender Reihenfolge sortiert.

Sie können auch [Mandanten in der MDR Web Console anzeigen](#).

Mandanteneinstellungen in Kaspersky Security Center anzeigen

Sie können für jeden Mandanten die Einstellungen in Ihrem Benutzerkonto anzeigen.

Ihr Benutzerkonto in Kaspersky Security Center Web Console oder Kaspersky Next Expert View muss über eine Rolle mit den folgenden [Zugriffsrechten](#) verfügen: **Zugriff auf Vorfälle** und **Verwaltung von Mandanten** sowie über die Möglichkeit, Mandanten im Abschnitt **MDR** in Kaspersky Security Center anzuzeigen, hinzuzufügen, zu bearbeiten und zu löschen.

So zeigen Sie die Mandanteneinstellungen an:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **Mandanten**.

Die Liste **Mandanten** wird angezeigt. Jede Zeile steht für einen Mandanten. Sie können auf den Namen eines Mandanten klicken, um Informationen über den Mandanten anzuzeigen.

2. Klicken Sie auf die Zeile des Mandanten, dessen Details Sie anzeigen möchten.

Der Block **Mandanten-Einstellungen** wird angezeigt.

Die Einstellung beginnt mit dem Umschalter **Aktiv**, der anzeigt, ob ein Mandant aktiv ist oder nicht. Bei Bedarf können Sie den Umschalter **Aktiv** umschalten. Darunter sind die folgenden Felder vorhanden:

Name

Ein beliebiger, für Menschen lesbarer Name des Mandanten, den Sie beim Erstellen des Mandanten angeben. Ein Mandantennamen kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 100 Zeichen nicht überschreiten. Mandanten können nicht umbenannt werden.

ID

Die eindeutige, automatisch generierte ID des Mandanten.

Beschreibung

Frei wählbare Informationen, die Sie beim Erstellen oder Bearbeiten des Mandanten eingeben. Beispiele hierfür sind der Verwendungszweck des Mandanten oder die voraussichtliche Anzahl der Assets. Die Beschreibung kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 2000 Zeichen nicht überschreiten.

Zugewiesene Assets

Die Anzahl der dem Mandanten zugewiesenen Assets.

Maximale Anzahl der Assets

Die Anzahl der Assets, die mit dem Mandanten verbunden werden sollen. Eine Überschreitung dieses Limits ist zulässig und hat keinen Einfluss auf die Funktionsfähigkeit der MDR-Lösung.

Konfigurationsdateien für den Mandanten

Dieser Abschnitt zeigt Informationen über die [MDR-Konfigurationsdatei](#) des Mandanten an:

- **Lizenz** – Die [Lizenz](#), die dem Mandanten entspricht.
- **Ablaufdatum** – Die Lebensdauer des Mandanten. Sie können das Ablaufdatum während der Erstellung des Mandanten manuell angeben. Das Ablaufdatum dieses Mandanten muss sich vor dem letzten gültigen Tag des MDR-Lizenzzeitraums befinden.
- **Maßnahme** – Sie können auf den Link **Konfigurationsdatei herunterladen** klicken, um das zip-Archiv mit der MDR-Konfigurationsdatei herunterzuladen.

Klicken Sie auf die Schaltfläche **X**, um eine Konfigurationsdatei zu löschen. Sie können eine Konfigurationsdatei nur dann löschen, wenn dem Mandanten eine andere Konfigurationsdatei hinzugefügt wird.

Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Konfigurationsdatei hinzuzufügen. Geben Sie die Lizenz und das Ablaufdatum an.

3. Klicken Sie im unteren Teil des Blocks **Mandanten-Einstellungen** auf die Schaltfläche **Schließen**, um den Block zu schließen.

Sie können auch die [Mandanteneinstellungen auch in der MDR Web Console anzeigen](#).

Mandanteneinstellungen in Kaspersky Security Center bearbeiten

Sie können die Einstellungen für jeden Mandanten in Ihrem Konto bearbeiten.

Ihr Benutzerkonto in Kaspersky Security Center Web Console oder Kaspersky Next Expert View muss über eine Rolle mit den folgenden [Zugriffsrechten](#) verfügen: **Zugriff auf Vorfälle** und **Verwaltung von Mandanten** sowie über die Möglichkeit, Mandanten im Abschnitt **MDR** in Kaspersky Security Center anzuzeigen, hinzuzufügen, zu bearbeiten und zu löschen.

So bearbeiten Sie die Mandanteneinstellungen:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **Mandanten**.

Die Liste **Mandanten** wird angezeigt. Jede Zeile steht für einen Mandanten. Sie können auf den Namen eines Mandanten klicken, um Informationen über den Mandanten anzuzeigen.

2. Klicken Sie auf die Zeile des Mandanten, den Sie bearbeiten möchten.

Der Block **Mandanten-Einstellungen** wird angezeigt. Hier können Sie Folgendes tun:

- Den Mandanten durch das Betätigen des Umschalters **Aktiv** aktivieren oder deaktivieren.
- Den Wert des Feldes **Beschreibung** ändern.
- Eine Konfigurationsdatei durch das Anklicken der Schaltfläche **X** löschen. Sie können eine Konfigurationsdatei nur dann löschen, wenn dem Mandanten eine andere Konfigurationsdatei hinzugefügt wird.
- Eine neue Konfigurationsdatei durch das Anklicken der Schaltfläche **Save** hinzufügen. Geben Sie die Lizenz und das Ablaufdatum an.

3. Klicken Sie im unteren Teil des Blocks **Mandanten-Einstellungen** auf die Schaltfläche **Save**.

- Der Block **Mandanten-Einstellungen** wird ausgeblendet. Nachdem Sie auf die Schaltfläche **Save** geklickt haben, erstellt Kaspersky Managed Detection and Response die MDR-Konfigurationsdatei, die mit den aktualisierten Mandanteneinstellungen übereinstimmt. Sie können auf den Link **Konfigurationsdatei herunterladen** klicken, um das zip-Archiv mit der MDR-Konfigurationsdatei herunterzuladen.

Die Mandanteneinstellungen werden bearbeitet. Die aktualisierten Einstellungen werden auf die Assets der ausgewählten Administrationsgruppen angewendet.

Sie können auch die [Mandanteneinstellungen in der MDR Web Console bearbeiten](#).

Neue Mandanten in Kaspersky Security Center hinzufügen

Wenn Sie für eine andere Organisation zum Anbieter von Kaspersky Managed Detection and Response werden möchten, müssen Sie Ihrem Konto einen neuen Mandanten hinzufügen.

Ihr Benutzerkonto in Kaspersky Security Center Web Console oder Kaspersky Next Expert View muss über eine Rolle mit den folgenden [Zugriffsrechten](#) verfügen: **Zugriff auf Vorfälle** und **Verwaltung von Mandanten** sowie über die Möglichkeit, Mandanten im Abschnitt **MDR** in Kaspersky Security Center anzuzeigen, hinzuzufügen, zu bearbeiten und zu löschen.

So fügen Sie einen neuen Mandanten hinzu:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **Mandanten**.

Die Liste **Mandanten** wird angezeigt.

2. Klicken Sie im oberen Teil des Fensters auf die **+** Schaltfläche **Mandant hinzufügen**.

Der Block **Mandanten-Einstellungen** wird angezeigt.

3. Schalten Sie gegebenenfalls den Umschalter **Aktiv** um.

Der Umschalter **Aktiv** ist standardmäßig aktiviert.

4. Füllen Sie die folgenden Felder aus:

Name

Ein beliebiger, für Menschen lesbarer Name des Mandanten, den Sie beim Erstellen des Mandanten angeben. Ein Mandantennamen kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 100 Zeichen nicht überschreiten. Mandanten können nicht umbenannt werden.

Beschreibung

Frei wählbare Informationen, die Sie beim Erstellen oder Bearbeiten des Mandanten eingeben. Beispiele hierfür sind der Verwendungszweck des Mandanten oder die voraussichtliche Anzahl der Assets. Die Beschreibung kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 2000 Zeichen nicht überschreiten.

Konfigurationsdateien für den Mandanten

Dieser Abschnitt zeigt Informationen über die [MDR-Konfigurationsdatei](#) des Mandanten an:

- **Lizenz** – Die [Lizenz](#), die dem Mandanten entspricht.
- **Ablaufdatum** – Die Lebensdauer des Mandanten. Sie können das Ablaufdatum während der Erstellung des Mandanten manuell angeben. Das Ablaufdatum dieses Mandanten muss sich vor dem letzten gültigen Tag des MDR-Lizenzzeitraums befinden.
- **Maßnahme** – Sie können auf den Link **Konfigurationsdatei herunterladen** klicken, um das zip-Archiv mit der MDR-Konfigurationsdatei herunterzuladen.

Klicken Sie auf die Schaltfläche **X**, um eine Konfigurationsdatei zu löschen. Sie können eine Konfigurationsdatei nur dann löschen, wenn dem Mandanten eine andere Konfigurationsdatei hinzugefügt wird.

Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Konfigurationsdatei hinzuzufügen. Geben Sie die Lizenz und das Ablaufdatum an.

Maximale Anzahl der Assets

Die Anzahl der Assets, die mit dem Mandanten verbunden werden sollen. Eine Überschreitung dieses Limits ist zulässig und hat keinen Einfluss auf die Funktionsfähigkeit der MDR-Lösung.

5. Klicken Sie im unteren Teil des Blocks **Mandanten-Einstellungen** auf die Schaltfläche **Speichern**.

Der Block **Mandanten-Einstellungen** wird ausgeblendet. Nachdem Sie auf die Schaltfläche **Speichern** geklickt haben, erstellt Kaspersky Managed Detection and Response eine [MDR-Konfigurationsdatei](#) für den neuen Mandanten. Sie können auf den Link **Konfigurationsdatei herunterladen** klicken, um das zip-Archiv mit der MDR-Konfigurationsdatei herunterzuladen.

Der neue Mandant wird hinzugefügt.

Sie können auch [neue Mandanten in der MDR Web Console hinzufügen](#).

Mandanten in Kaspersky Security Center löschen

Wenn Sie einen Mandanten löschen, der mehrere Assets enthält, werden alle seine Assets von der MDR-Lösung getrennt. Um die Assets des Mandanten weiterhin verwalten zu können, [verschieben Sie die Assets auf den Root-Mandanten oder auf einen neuen Mandanten](#), bevor Sie den Mandanten löschen.

Ihr Benutzerkonto in Kaspersky Security Center Web Console oder Kaspersky Next Expert View muss über eine Rolle mit den folgenden [Zugriffsrechten](#) verfügen: **Zugriff auf Vorfälle** und **Verwaltung von Mandanten** sowie über die Möglichkeit, Mandanten im Abschnitt **MDR** in Kaspersky Security Center anzuzeigen, hinzuzufügen, zu bearbeiten und zu löschen.

So löschen Sie einen Mandanten:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **Mandanten**.

Die Liste **Mandanten** wird angezeigt.

2. Zeigen Sie in der Liste **Mandanten** auf den Mandanten, den Sie löschen möchten, und klicken Sie anschließend in der Spalte **Actions** auf das Papierkorbsymbol (🗑).

3. Bestätigen Sie das Löschen.

Der ausgewählte Mandant wird gelöscht.

Sie können auch [Mandanten in der MDR Web Console](#) löschen.

Assets zwischen Mandanten verschieben

Wenn Sie einen Mandanten löschen, der mehrere Assets enthält, stellen alle seine Assets die Übertragung von Telemetriedaten an die MDR-Lösung ein. Verschieben Sie vor dem Löschen eines Mandanten alle seine Assets zum Root-Mandanten oder zu einem neuen Mandanten.

Ihr Benutzerkonto in Kaspersky Security Center Web Console oder Kaspersky Next Expert View muss über eine Rolle mit den folgenden [Zugriffsrechten](#) verfügen: **Zugriff auf Vorfälle** und **Verwaltung von Mandanten** sowie über die Möglichkeit, Mandanten im Abschnitt **MDR** in Kaspersky Security Center anzuzeigen, hinzuzufügen, zu bearbeiten und zu löschen.

So verschieben Sie Assets zu einem neuen Mandanten:

1. **Erstellen Sie einen neuen Mandanten** in Kaspersky Security Center im Abschnitt [MDR](#). Sie werden diesem Mandanten später Assets hinzufügen.

Beim Erstellen eines neuen Mandanten laden Sie eine MDR-Konfigurationsdatei herunter.

2. Erstellen Sie in der Kaspersky Security Center Web Console [eine neue Administrationsgruppe](#).
3. [Fügen Sie die Assets hinzu](#), die Sie zu dem neuen Mandanten in die neue Administrationsgruppe verschieben möchten.
4. [Erstellen Sie eine neue Richtlinie](#) für Kaspersky Endpoint Agent oder eine EPP-Anwendung für die erstellte Administrationsgruppe.
5. Wenden Sie die MDR-Konfigurationsdatei auf die erstellte Richtlinie an.

Ausführliche Informationen zu den verschiedenen Bereitstellungsszenarien finden Sie unter [Bereitstellung von Kaspersky Managed Detection and Response](#).

Nachdem die Richtlinie auf die Assets der Administrationsgruppe angewendet wurde, werden die Assets vom Root-Mandanten zu dem neu erstellten Mandanten verschoben.

So verschieben Sie Assets zum Root-Mandanten:

1. Laden Sie eine MDR-Konfigurationsdatei für den Root-Mandanten herunter:
 - Wechseln Sie in der MDR Web Console (<https://mdr.kaspersky.com/guide>) zur Seite **Getting Started** und klicken Sie auf den Link **MDR-Konfigurationsdatei**.
 - Wechseln Sie in der Kaspersky Security Center Web Console oder in Kaspersky Next Expert View zu **MDR > Getting Started** und klicken Sie auf den Link **Download**.
2. Erstellen Sie in der Kaspersky Security Center Web Console [eine neue Administrationsgruppe](#).
3. [Fügen Sie die Assets hinzu](#), die Sie zum Root-Mandanten in die neue Administrationsgruppe verschieben möchten.

4. [Erstellen Sie eine neue Richtlinie](#)  für Kaspersky Endpoint Agent oder eine EPP-Anwendung für die erstellte Administrationsgruppe.

5. Wenden Sie die MDR-Konfigurationsdatei auf die erstellte Richtlinie an.

Nachdem die Richtlinie auf die Assets der Administrationsgruppe angewendet wurde, werden die Assets zum Root-Mandanten verschoben.

Mandanten in der MDR Web Console verwalten

Dieser Abschnitt enthält Informationen über die Verwaltung von Mandanten in der MDR Web Console.

Mandanten in der MDR Web Console anzeigen

So zeigen Sie Mandanten an:

1. Navigieren Sie im Fenster der MDR Web Console zum Menüpunkt **Settings**.

2. Klicken Sie auf die Registerkarte **Tenants**.

Die Liste **Tenants** wird angezeigt. Jede Zeile steht für einen Mandanten. Sie können auf eine beliebige Stelle in der Zeile klicken, um Informationen zu dem Mandanten anzuzeigen.

3. Die folgenden Mandantenattribute sind über der Liste vorhanden:

Name

Ein beliebiger, für Menschen lesbarer Name des Mandanten, den Sie beim Erstellen des Mandanten angeben. Ein Mandantennamen kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 100 Zeichen nicht überschreiten. Mandanten können nicht umbenannt werden.

Status

Folgende Statuswerte sind für Mandanten möglich:

- **Aktiv**

Der Mandant kann Kaspersky Managed Detection and Response verwenden.

- **Inaktiv**

Der Mandant kann Kaspersky Managed Detection and Response nicht verwenden.

Sie können den Status "Inaktiv" in der Mandantenkarte manuell einstellen. Zusätzlich wird der Status "Inaktiv" am Ende der Lebensdauer des Mandanten automatisch eingestellt.

Assets / limit

Anzahl der Assets, die einem Mandanten zugeordnet sind / Asset-Limit.

Das Asset-Limit wird beim Erstellen zusätzlicher Mandanten angegeben und dient nur zu Informationszwecken. Eine Überschreitung des Limits ist zulässig und hat keinen Einfluss auf die Funktionsfähigkeit der MDR-Lösung.

Description

Frei wählbare Informationen, die Sie beim Erstellen oder Bearbeiten des Mandanten eingeben. Beispiele hierfür sind der Verwendungszweck des Mandanten oder die voraussichtliche Anzahl der Assets. Die Beschreibung kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 2000 Zeichen nicht überschreiten.

Created on

Datum, an dem der Mandant erstellt wurde.

Expiration date

Datum, an dem die Lebensdauer des Mandanten abläuft.

Vorfälle werden entsprechend ihrer Gültigkeitszeiträume in absteigender Reihenfolge sortiert.

Actions

Zeigt beim Darüberbewegen des Mauszeigers für Nicht-Root-Mandanten das Papierkorb-Symbol (🗑️) an. Um den Mandanten zu löschen, klicken Sie auf das Papierkorb-Symbol und bestätigen Sie den Löschvorgang.

Mandanteneinstellungen in der MDR Web Console anzeigen

So zeigen Sie die Mandanteneinstellungen an:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Settings**.

2. Klicken Sie auf die Registerkarte **Tenants**.

Die Liste **Tenants** wird angezeigt. Jede Zeile steht für einen Mandanten. Sie können auf eine beliebige Stelle in der Zeile klicken, um Informationen zu dem Mandanten anzuzeigen.

3. Klicken Sie auf die Zeile des Mandanten, dessen Details Sie anzeigen möchten.

Der Block **Tenant settings** wird angezeigt.

Die Einstellung beginnt mit dem Umschalter **Active**, der anzeigt, ob ein Mandant aktiv ist oder nicht. Sie können den Umschalter **Active** umlegen, um den Mandanten zu deaktivieren.

Darunter sind die folgenden Felder vorhanden:

Tenant name

Ein beliebiger, für Menschen lesbarer Name des Mandanten, den Sie beim Erstellen des Mandanten angeben. Ein Mandantename kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 100 Zeichen nicht überschreiten. Mandanten können nicht umbenannt werden.

Description

Frei wählbare Informationen, die Sie beim Erstellen oder Bearbeiten des Mandanten eingeben. Beispiele hierfür sind der Verwendungszweck des Mandanten oder die voraussichtliche Anzahl der Assets. Die Beschreibung kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 2000 Zeichen nicht überschreiten.

Assets / limit

Die Anzahl der Assets, die mit dem Mandanten verbunden werden sollen. Eine Überschreitung dieses Limits ist zulässig und hat keinen Einfluss auf die Funktionsfähigkeit der MDR-Lösung.

Configuration file lifetime

Das Datum, an dem die Konfigurationsdatei des Mandanten abläuft.

Dieses Feld wird für den Root-Mandanten nicht angezeigt.

Im unteren Teil des Blocks befindet sich eine Schaltfläche zum Herunterladen der [MDR-Konfigurationsdatei](#) für die Bereitstellung des Mandanten.

4. Klicken Sie im unteren Teil des Blocks **Tenant settings** auf die Schaltfläche **Cancel**, um den Block zu schließen.

Mandanteneinstellungen in der MDR Web Console bearbeiten

Die Möglichkeit, Mandanten hinzuzufügen und zu bearbeiten, steht nur dem Benutzer zur Verfügung, dem die Rolle [MDR-Administrator](#) zugewiesen ist.

So bearbeiten Sie die Mandanteneinstellungen:

1. Öffnen Sie MDR Web Console.

2. Klicken Sie in MDR Web Console im Abschnitt **Settings** auf die Registerkarte **Tenants**.

Die Liste **Tenants** wird angezeigt. Jede Zeile steht für einen Mandanten. Sie können auf eine beliebige Stelle in der Zeile klicken, um Informationen zu dem Mandanten anzuzeigen.

3. Klicken Sie auf die Zeile des Mandanten, den Sie bearbeiten möchten.

Der Block **Tenant settings** wird angezeigt.

4. Betätigen Sie gegebenenfalls den Umschalter **Active**.

5. Ändern Sie bei Bedarf die Werte der Felder.

6. Klicken Sie im unteren Teil des Blocks **Tenant settings** auf die Schaltfläche **Save**.

Der Block **Tenant settings** wird ausgeblendet. Nachdem Sie auf die Schaltfläche **Save** geklickt haben, erstellt Kaspersky Managed Detection and Response eine neue MDR-Konfigurationsdatei, die mit den aktualisierten Mandanteneinstellungen übereinstimmt.

7. Klicken Sie in der Liste **Tenants** auf die Zeile mit dem bearbeiteten Mandanten.

Der Block **Tenant settings** wird angezeigt. Im unteren Teil des Blocks befindet sich eine Schaltfläche zum Herunterladen der [MDR-Konfigurationsdatei](#) für die Bereitstellung des Mandanten.

8. Klicken Sie im unteren Teil des Blocks **Tenant settings** auf die Schaltfläche **Cancel**, um den Block zu schließen.

Die Mandanteneinstellungen werden bearbeitet. Sie müssen jetzt die neue MDR-Konfigurationsdatei auf den Assets des Mandanten bereitstellen, um die bearbeiteten Einstellungen übernehmen.

Neue Mandanten in der MDR Web Console hinzufügen

Die Möglichkeit, Mandanten hinzuzufügen und zu bearbeiten, steht nur dem Benutzer zur Verfügung, dem die Rolle [MDR-Administrator](#) zugewiesen ist.

So fügen Sie einen neuen Mandanten hinzu:

1. Navigieren Sie im Fenster der MDR Web Console zum Menüpunkt **Settings**.

2. Klicken Sie auf die Registerkarte **Tenants**.

Die Liste **Tenants** wird angezeigt.

3. Klicken Sie im oberen Teil des Fensters auf die Schaltfläche **Add**.

Der Block **Tenant settings** wird angezeigt.

4. Schalten Sie gegebenenfalls den Umschalter **Active** um.

Der Umschalter **Active** ist standardmäßig aktiviert.

5. Füllen Sie die folgenden Felder aus:

Tenant name

Ein beliebiger, für Menschen lesbarer Name des Mandanten, den Sie beim Erstellen des Mandanten angeben. Ein Mandantennamen kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 100 Zeichen nicht überschreiten. Mandanten können nicht umbenannt werden.

Description

Frei wählbare Informationen, die Sie beim Erstellen oder Bearbeiten des Mandanten eingeben. Beispiele hierfür sind der Verwendungszweck des Mandanten oder die voraussichtliche Anzahl der Assets. Die Beschreibung kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Die Länge darf 2000 Zeichen nicht überschreiten.

Assets / limit

Die Anzahl der Assets, die mit dem Mandanten verbunden werden sollen. Eine Überschreitung dieses Limits ist zulässig und hat keinen Einfluss auf die Funktionsfähigkeit der MDR-Lösung.

Configuration file lifetime

Das Datum, an dem die Konfigurationsdatei des Mandanten abläuft.

Dieses Feld wird für den Root-Mandanten nicht angezeigt.

6. Klicken Sie im unteren Teil des Blocks **Tenant settings** auf die Schaltfläche **Save**.

Der Block **Tenant settings** wird ausgeblendet. Nachdem Sie auf die Schaltfläche **Save** geklickt haben, erstellt Kaspersky Managed Detection and Response eine [MDR-Konfigurationsdatei](#) für den neuen Mandanten.

7. Klicken Sie in der Liste **Tenants** auf die Zeile mit dem neuen Mandanten.

Der Block **Tenant settings** wird angezeigt. In diesem Block können Sie die [MDR-Konfigurationsdatei](#) zur Bereitstellung von Mandanten herunterladen.

8. Klicken Sie auf **Configuration archive**, um die neue MDR-Konfigurationsdatei herunterzuladen.

9. Klicken Sie im unteren Teil des Blocks **Tenant settings** auf die Schaltfläche **Cancel**, um den Block zu schließen.

Der neue Mandant wird hinzugefügt. Jetzt können Sie die heruntergeladene MDR-Konfigurationsdatei auf den Assets des Mandanten bereitstellen.

Beachten Sie: Die in MDR Web Console erstellten Mandanten sind in Kaspersky Security Center im Abschnitt **MDR** nicht verfügbar. Um mit diesen Mandanten zu arbeiten, verwenden Sie bitte die MDR Web Console.

Mandanten in der MDR Web Console löschen

Wenn Sie einen Mandanten löschen, der mehrere Assets enthält, werden alle seine Assets von der MDR-Lösung getrennt. Vorfälle, die einem gelöschten Mandanten zugewiesen wurden, sind nicht mehr verfügbar. Diese Aktion ist unwiderruflich. Vor dem Löschen eines Mandanten sollten Sie [alle seine Assets zum Root-Mandanten oder zu einem neuen Mandanten verschieben](#).

Die Möglichkeit, Mandanten hinzuzufügen und zu bearbeiten, steht nur dem Benutzer zur Verfügung, dem die Rolle [MDR-Administrator](#) zugewiesen ist.

So löschen Sie einen Mandanten:

1. Navigieren Sie in der MDR Web Console zum Menüpunkt **Settings**.
2. Klicken Sie auf die Registerkarte **Tenants**.
Die Liste **Tenants** wird angezeigt.
3. Bewegen Sie den Mauszeiger in der Mandantenliste über den Mandanten, den Sie löschen möchten, und klicken Sie rechts auf die Schaltfläche **Delete tenant** mit dem Papierkorb-Symbol.
Es öffnet sich das Fenster **Confirm tenant deletion**.
4. Klicken Sie auf die Schaltfläche **Delete**, um den Mandanten zu löschen.

Beachten Sie, dass die in MDR Console erstellten Mandanten in Kaspersky Security Center im Abschnitt **MDR** nicht verfügbar sind. Um mit diesen Mandanten zu arbeiten, verwenden Sie bitte die MDR Web Console.

Die Lösung mittels REST-API verwalten

Diese Funktion ist in MDR Expert, MDR Advanced (nur in einigen Regionen erhältlich) und MDR Prime (nur in einigen Regionen erhältlich) verfügbar. Den Vergleich der Lizenzlösungen finden Sie [in diesem Abschnitt](#).

Um in Kaspersky Security Center Zugriff auf die REST-API zu haben, muss Ihr Benutzerkonto in der Kaspersky Security Center Web Console über die folgenden Zugriffsrechte verfügen: "Zugriff auf Vorfälle" und "Zugriff auf REST-API".

Für einige [kommerzielle Lizenzstufen](#) ist es nur möglich, einen Aktualisierungstoken in der MDR Web Console zu generieren, um ihn für die [Einrichtung des MDR-Plug-ins zu](#) verwenden, ohne Zugriff auf die REST-API von Kaspersky Security Center zu bekommen.

Mit Kaspersky Managed Detection and Response können Sie MDR-Objekte über die REST-API programmgesteuert abrufen, erstellen und aktualisieren. Die REST-API arbeitet über HTTP und besteht aus einer Reihe von Methoden mit "Anfrage-Antwort"-Prinzip. Das bedeutet, dass Sie Kaspersky Managed Detection and Response auch über die Lösung eines Drittanbieters verwalten können und nicht ausschließlich über die MDR Web Console.

Um mit der REST-API zu arbeiten, müssen Sie [einen Aktualisierungstoken](#) und [einen Zugriffstoken](#) erstellen.

[REST-API-REFERENZ ÖFFNEN](#) 

Szenario: Tokenbasierte Autorisierung durchführen

In diesem Szenario wird erläutert, wie Sie eine tokenbasierte Autorisierung durchführen, um mit der REST-API zu arbeiten.

Voraussetzungen

Stellen Sie sicher, dass Sie über ein MDR-Benutzerkonto mit einer der zugewiesenen Rollen verfügen:

- [Rolle](#) des MDR-Administrators
- Benutzerdefinierte Rolle mit folgenden [Zugriffsrechten](#) (gilt nur für Kaspersky Security Center):
 - Zugriff auf Vorfälle
 - Zugriff auf REST-API

Stufen

Die Token-basierte Autorisierung wird in Stufen vollzogen:

1 Erstellen eines Aktualisierungstokens in der MDR Web Console

Sie benötigen einen [Aktualisierungstoken](#), um ein Zugriffstoken zu erstellen. Ein Aktualisierungstoken ist 24 Stunden lang gültig. Sie können ein Aktualisierungstoken nur einmal verwenden.

2 Erstellen eines Zugriffstokens über die REST-API

Sie benötigen einen [Zugriffstoken](#), um mit der REST-API zu arbeiten. Ein Zugriffstoken ist 1 Stunde lang gültig. Sie können ein Zugriffstoken während seiner Lebensdauer mehrmals verwenden.

Wenn Sie einen Zugriffstoken erstellen, generiert die REST-API einen neuen Aktualisierungstoken und fügt ihn in die Antwort ein. Wenn der Zugriffstoken abläuft, können Sie einen neuen Zugriffstoken erstellen, indem Sie den neuesten Aktualisierungstoken verwenden, der von der API generiert wurde.

Ein von der API generierter Aktualisierungstoken ist 7 Tage lang gültig.

Ergebnisse

Nach Abschluss dieses Szenarios können Sie die [Arbeit mit der REST-API beginnen](#), indem Sie Anfragen mit dem Zugriffstoken senden.

Eine API-Verbindung in Kaspersky Security Center erstellen

Wenn Sie eine neue API-Verbindung erstellen, wird ein Aktualisierungstoken generiert. Ein *Aktualisierungstoken* ist eine eindeutige Folge von Buchstaben, Ziffern und Symbolen. Nach der Erstellung eines Aktualisierungstokens können Sie mit ihm einen Zugriffstoken erstellen.

So erstellen Sie eine API-Verbindung:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **API**.

Die Liste mit den **API** wird angezeigt.

2. Klicken Sie im oberen Teil des Fensters auf **Verbindung hinzufügen**.

Der Block **Neue API-Verbindung hinzufügen** wird angezeigt.

3. Legen Sie die folgenden Einstellungen fest:

- **Verbindungsname**

Ein Verbindungsname kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Ein Name einer Verbindung wird in REST-API-Antworten als `author_name` angegeben und als Autor des Kommentars auf der Registerkarte **Communication** eines Vorfalls angezeigt.

- **Zugriffsberechtigungen**

Legen Sie fest, welche Zugriffsrechte zum Ausführen von Aktionen über die HTTP-API gewährt werden sollen:

- **Vollzugriff + API und Mandanten**

Zugriffsrechte der Rolle "MDR-Administrator". Ein MDR-Administrator ist ein Superuser mit Zugriff auf alle Funktionen von Kaspersky Managed Detection and Response, die von der Lizenz gewährt werden. Der MDR-Administrator kann anderen Benutzern den Zugriff auf die Client-Datenquellen gewähren. Wenn Sie Kaspersky Managed Detection and Response aktivieren, werden Sie automatisch zum MDR-Administrator. Aus diesem Grund wird empfohlen, für den Aktivierungsprozess die E-Mail-Adresse des Unternehmens anstelle einer persönlichen E-Mail-Adresse zu verwenden. Wenn der MDR-Administrator mit einer persönlichen E-Mail-Adresse erstellt wird, kann dies ein Sicherheitsrisiko darstellen, z. B. wenn das Konto des MDR-Administrators gestohlen werden.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	✓	—
Verwaltung von Reaktionen	✓	—
Verwaltung von Mandanten	✓	—
Planung einer Zusammenfassung des Vorfalls	✓	—
Zugriff auf REST-API	✓	—

- **Einstellungen für Zugriff auf Vorfälle, Verwaltung von Reaktionen und Auto-Akzeptieren**

Zugriffsrechte der Rolle "Senior Security Officer". Ein Senior Security Officer ist ein Mitarbeiter, der Zugriff auf die durch die Lizenz gewährten Funktionen von Kaspersky Managed Detection and Response hat. Er hat jedoch keinen Zugriff auf die REST-API. Der Senior Security Officer hat das Recht, [Reaktionen](#) zu akzeptieren und abzulehnen.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	✓	—
Verwaltung von Reaktionen	✓	—
Verwaltung von Mandanten	—	✓
Planung einer Zusammenfassung des Vorfalls	—	✓
Zugriff auf REST-API	—	✓

- **Zugriff auf Vorfälle**

Zugriffsrechte der Rolle "Security Officer". Ein Security Officer ist ein Mitarbeiter, der Zugriff auf die durch die Lizenz gewährten Funktionen von Kaspersky Managed Detection and Response hat. Er hat jedoch keinen Zugriff auf die REST-API. Der Security Officer kann [Reaktionen](#) weder akzeptieren noch ablehnen.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	—	✓
Verwaltung von Reaktionen	—	✓
Verwaltung von Mandanten	—	✓

Funktionsbereich	Erlauben	Verweigern
Planung einer Zusammenfassung des Vorfalls	—	✓
Zugriff auf REST-API	—	✓

- **Mandant**

Wählen Sie bei Bedarf den Wert (oder die Werte) in der Dropdown-Liste **Mandant** aus.

Der Benutzer kann nur die Assets und Vorfälle anzeigen, die sich auf die angegebenen Mandanten beziehen.

4. Klicken Sie auf **Generieren**.

Das Feld **JWT-Token** wird angezeigt.

5. Klicken Sie auf die Schaltfläche **Schließen**.

Die neue API-Verbindung wird in der Liste mit den **API** angezeigt. Sie können den Aktualisierungstoken jetzt verwenden, um einen [Zugriffstoken zu erstellen](#).

Sie können auch [API-Verbindungen in der MDR Web Console konfigurieren](#).

Eine API-Verbindung in der MDR Web Console erstellen

Ein *Aktualisierungstoken* ist eine eindeutige Folge von Buchstaben, Ziffern und Symbolen. Nach der Erstellung eines Aktualisierungstokens können Sie mit ihm einen Zugriffstoken erstellen.

So erstellen Sie einen Aktualisierungstoken:

1. Navigieren Sie im Fenster der MDR Web Console zum Menüpunkt **Settings**.

2. Klicken Sie auf die Registerkarte **API**

Die Liste **All tokens** wird angezeigt.

3. Klicken Sie im oberen Teil des Fensters auf die Schaltfläche **Add**.

Der Block **Generate token** wird angezeigt.

4. Legen Sie die folgenden Einstellungen fest:

- **Connection name**

Der Name eines Tokens.

Der Name eines Tokens kann lateinische Buchstaben, Ziffern und Sonderzeichen enthalten. Der Name eines Tokens wird in REST-API-Antworten als `author_name` angegeben und als Autor des Kommentars auf der **Communication**-Registerkarte eines Vorfalls angezeigt.

Für einige [kommerzielle Lizenzstufen](#) ist dies das einzige verfügbare Feld beim Erstellen eines Aktualisierungstokens.

- **User role**

Die Benutzerrolle zum Angeben von Berechtigungen, die zum Ausführen von Vorgängen über die HTTP-API gewährt werden.

Folgende Benutzerrollen stehen zur Verfügung:

- **MDR Administrator**

Der Superuser mit Zugriff auf alle Funktionen von Kaspersky Managed Detection and Response, die von der Lizenz gewährt werden. Der MDR-Administrator kann anderen Benutzern den Zugriff auf die Client-Datenquellen gewähren. Wenn Sie Kaspersky Managed Detection and Response aktivieren, werden Sie automatisch zum MDR-Administrator. Aus diesem Grund wird empfohlen, für den Aktivierungsprozess die E-Mail-Adresse des Unternehmens anstelle einer persönlichen E-Mail-Adresse zu verwenden. Wenn der MDR-Administrator mit einer persönlichen E-Mail-Adresse erstellt wird, kann dies ein Sicherheitsrisiko darstellen, z. B. falls das Konto des MDR-Administrators gestohlen wird.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	✓	—
Verwaltung von Reaktionen	✓	—
Verwaltung von Mandanten	✓	—
Planung einer Zusammenfassung des Vorfalls	✓	—
Zugriff auf REST-API	✓	—

- **Senior Security Officer**

Ein Mitarbeiter, der Zugriff auf die durch die Lizenz gewährten Funktionen von Kaspersky Managed Detection and Response hat. Er hat jedoch keinen Zugriff auf die REST-API. Der Senior Security Officer hat das Recht, [Reaktionen](#) zu akzeptieren und abzulehnen.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	✓	—
Verwaltung von Reaktionen	✓	—
Verwaltung von Mandanten	—	✓
Planung einer Zusammenfassung des Vorfalls	—	✓
Zugriff auf REST-API	—	✓

- **Security Officer**

Ein Mitarbeiter, der Zugriff auf die durch die Lizenz gewährten Funktionen von Kaspersky Managed Detection and Response hat. Er hat jedoch keinen Zugriff auf die REST-API. Der Security Officer kann [Reaktionen](#) weder akzeptieren noch ablehnen.

Im Kaspersky Security Center entspricht diese Rolle den folgenden Zugriffsrechten:

Funktionsbereich	Erlauben	Verweigern
Zugriff auf Vorfälle	✓	—
Einstellungen für das Auto-Akzeptieren	—	✓
Verwaltung von Reaktionen	—	✓
Verwaltung von Mandanten	—	✓
Planung einer Zusammenfassung des Vorfalls	—	✓
Zugriff auf REST-API	—	✓

- **Tenant**

Wählen Sie bei Bedarf den Wert (oder die Werte) in der Dropdown-Liste **Tenant** aus.

Es werden Mandanten vorgeschlagen, die bereits in der Konsole existieren und den Wert **Root tenant** besitzen.

Der Benutzer kann nur die Assets und Vorfälle anzeigen, die sich auf die angegebenen Mandanten beziehen. Wenn Sie über Assets und Vorfälle verfügen, die keinem Mandanten zugewiesen sind, kann der Benutzer diese anzeigen, wenn Sie den Wert **Root tenant** auswählen.

Sie können den Wert **Root tenant** zusätzlich zu angegebenen Namen der Mandanten auswählen.

5. Klicken Sie im unteren Teil des Blocks auf die Schaltfläche **Generate**.

Der Block **Token info** ersetzt den Block **Generate token**.

6. Klicken Sie im unteren Teil des Blocks **Token info** auf die Schaltfläche **Close**.

Der von Ihnen erstellte Aktualisierungstoken wird in der Liste **All tokens** angezeigt. Sie können diesen Aktualisierungstoken jetzt verwenden, um [einen Zugriffstoken zu erstellen](#).

Eine API-Verbindung in Kaspersky Security Center bearbeiten

Vorhandene API-Verbindungen können bearbeitet werden.

So bearbeiten Sie eine API-Verbindung:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **API**.

Die Liste mit den **API** wird angezeigt.

2. Klicken Sie auf die API-Verbindung, die Sie bearbeiten möchten.

Es wird ein Block mit den Verbindungsinformationen angezeigt.

3. Ändern Sie die Verbindungseinstellungen.

4. Klicken Sie auf **Speichern**.

Die neuen Einstellungen der ausgewählten API-Verbindung werden gespeichert.

Eine API-Verbindung in der MDR Web Console bearbeiten

Vorhandene API-Verbindungen können bearbeitet werden.

So bearbeiten Sie eine API-Verbindung:

1. Klicken Sie in der MDR Web Console auf die Registerkarte **API**.

Die Liste **All tokens** wird angezeigt.

2. Klicken Sie auf den Token der API-Verbindung, die Sie bearbeiten möchten.

Es wird ein Block mit den Verbindungsinformationen angezeigt.

3. Ändern Sie die Verbindungseinstellungen.

4. Klicken Sie auf **Save**.

Die neuen Einstellungen der ausgewählten API-Verbindung werden gespeichert.

Einen Zugriffstoken in Kaspersky Security Center erstellen

Ein *Zugriffstoken* ist eine eindeutige Zeichenfolge (Buchstaben, Ziffern und Sonderzeichen), die Sie dazu berechtigt, die Methoden der REST-API zu verwenden.

So erstellen Sie einen Zugriffstoken:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **API**.

Die Liste mit den **API** wird angezeigt.

2. Klicken Sie auf eine Verbindung mit dem Status **Aktivierung ausstehend**.

Es wird ein Block mit den Verbindungsinformationen angezeigt.

3. Klicken Sie im Feld **JWT-Token** auf die Schaltfläche **Aktualisieren**.

Ein Aktualisierungstoken wird angezeigt.

4. Wählen und speichern Sie den Wert aus dem Feld **Client-ID**.

5. Wählen Sie die Zeichenfolge des Tokens aus und speichern Sie diese in der Zwischenablage.

6. Senden Sie eine POST-Anfrage an den `/session/confirm`-Endpunkt.

Ersetzen Sie `{client_id}` und `{refresh_token}` durch die in den vorherigen Schritten ausgewählten und gespeicherten Werte.

Beispiel (Python):

```
#####
# Allgemeiner Teil
#####

import time
import datetime
import requests
import jwt

# Das Zertifikat wird für die Authentifizierung einer externen Ressource benötigt
# Sie können das Zertifikat von https://mdr.kaspersky.com herunterladen,
# es auf Ihrer Festplatte speichern und seinen Pfad der Variablen hinzufügen:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# ID Ihres Kunden und Ihres Tokens
# Für Einzelheiten zum Abrufen Ihrer ID und der Token-ID siehe Hilfe https://support.kaspersky.com/MDR/de-DE/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Fügen Sie Ihren Wert ein)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Fügen Sie Ihren Wert ein)
ACCESS_TOKEN = "AcCeSsToKeN" # (Fügen Sie Ihren Wert ein)

#####
# Zugriffstoken und Aktualisierungstoken (refresh token) für das nächste Update des Zugriffstokens anfordern
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN Ablaufdatum und -uhrzeit: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN ist aktuell")
    else:
        print(
            "Ihr REFRESH_TOKEN muss aktualisiert werden. Sie finden ihn in MDR Web Console (https://support.kaspersky.com/MDR/en-US/258285.htm)"
        )
        exit()
else:
    print(
        "Der Wert Ihres REFRESH_TOKEN muss angegeben werden. Sie finden ihn in MDR Web Console (https://support.kaspersky.com/MDR/de-DE/258285.htm)"
    )
    exit()

# Prüfung, ob ein Zugriffstoken (access token) vorhanden und gültig ist
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 gültig bis: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN ist aktuell")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# Bei Bedarf Zugriffs- und Refresh-Tokens für das nächste Update des Zugriffstokens aktualisieren
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()

    #Aktualisierungstoken muss gespeichert werden, um nach Ablauf des aktuellen Zugriffstokens den nächsten Zugriffstoken zu erhalten
    refresh_token = result_json["refresh_token"]
    print(
        f'Ihr neuer REFRESH_TOKEN für die nächste Anfrage eines ACCESS_TOKEN (ersetzen Sie den Wert für REFRESH_TOKEN durch diesen Wert): "{refresh_token}"'
    )

    # Neuer Zugriffstoken zum Datenabruf erforderlich
    access_token = result_json["access_token"]
    print(f'Ihr neuer ACCESS_TOKEN (ersetzen Sie den Wert für ACCESS_TOKEN mit diesem Wert): "{access_token}"')

# Zugriffstoken zum Request-Header hinzufügen
headers = {"Authorization": f"Bearer {access_token}"}
```

Beispiel (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

Die REST-API liefert eine Antwort mit dem Zugriffstoken und einem neuen Aktualisierungstoken:

```
{
  "access_token": "SamPLET346yoKeNSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOKenSaMP1et2590KenS123aMP1e926tOKenSaMP1e"
}
```

Sie können jetzt mithilfe des Zugriffstokens Anfragen an die REST-API senden. Jede Anfrage an die REST-API erfordert einen Zugriffstoken – eine Anfrage ohne Zugriffstoken gibt lediglich einen Autorisierungsfehler zurück.

Sie können auch einen [Zugriffstoken in der MDR Web Console erstellen](#).

Einen Zugriffstoken in der MDR Web Console erstellen

So erstellen Sie einen Zugriffstoken:

1. Navigieren Sie im Fenster der MDR Web Console zum Menüpunkt **Settings**.

2. Klicken Sie auf die Registerkarte **API**

Die Liste **All tokens** wird angezeigt. Jede Zeile steht für einen Token. Sie können auf eine beliebige Stelle in der Zeile klicken, um Informationen zu dem Token anzuzeigen.

3. Klicken Sie auf ein Token mit dem **Pending activation**.

Der Block **Token info** wird angezeigt.

4. Klicken Sie im Feld **JWT token** auf die Schaltfläche **Aktualisieren**.

Ein Aktualisierungstoken wird angezeigt.

5. Wählen und speichern Sie den Wert aus dem Feld **Client ID**.

6. Wählen Sie die Zeichenfolge des Tokens aus und speichern Sie diese in der Zwischenablage.

7. Senden Sie eine POST-Anfrage an den `/session/confirm`-Endpunkt (siehe folgendes Beispiel)

Ersetzen Sie `{client_id}` und `{refresh_token}` durch die in den vorherigen Schritten ausgewählten und gespeicherten Werte.

Beispiel (Python):

```
#####
# Allgemeiner Teil
#####

import time
import datetime
import requests
import jwt

# Das Zertifikat wird für die Authentifizierung einer externen Ressource benötigt
# Sie können das Zertifikat von https://mdr.kaspersky.com herunterladen,
# es auf Ihrer Festplatte speichern und seinen Pfad der Variablen hinzufügen:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# ID Ihres Kunden und Ihres Tokens
# Für Einzelheiten zum Abrufen Ihrer ID und der Token-ID siehe Hilfe https://support.kaspersky.com/MDR/de-DE/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Fügen Sie Ihren Wert ein)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Fügen Sie Ihren Wert ein)
ACCESS_TOKEN = "AcCeSsToKeN" # (Fügen Sie Ihren Wert ein)

#####
# Zugriffstoken und Aktualisierungstoken (refresh token) für das nächste Update des Zugriffstokens anfordern
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN Ablaufdatum und -uhrzeit: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN ist aktuell")
    else:
        print(
            "Ihr REFRESH_TOKEN muss aktualisiert werden. Sie finden ihn in MDR Web Console (https://support.kaspersky.com/MDR/en-US/258285.htm)"
        )
        exit()
else:
    print(
        "Der Wert Ihres REFRESH_TOKEN muss angegeben werden. Sie finden ihn in MDR Web Console (https://support.kaspersky.com/MDR/de-DE/258285.htm)"
    )
    exit()

# Prüfung, ob ein Zugriffstoken (access token) vorhanden und gültig ist
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 gültig bis: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN ist aktuell")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# Bei Bedarf Zugriffs- und Refresh-Tokens für das nächste Update des Zugriffstokens aktualisieren
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()

    #Aktualisierungstoken muss gespeichert werden, um nach Ablauf des aktuellen Zugriffstokens den nächsten Zugriffstoken zu erhalten
    refresh_token = result_json["refresh_token"]
    print(
        f'Ihr neuer REFRESH_TOKEN für die nächste Anfrage eines ACCESS_TOKEN (ersetzen Sie den Wert für REFRESH_TOKEN durch diesen Wert): "{refresh_token}"'
    )

    # Neuer Zugriffstoken zum Datenabruf erforderlich
    access_token = result_json["access_token"]
    print(f'Ihr neuer ACCESS_TOKEN (ersetzen Sie den Wert für ACCESS_TOKEN mit diesem Wert): "{access_token}"')

# Zugriffstoken zum Request-Header hinzufügen
headers = {"Authorization": f"Bearer {access_token}"}
```

Beispiel (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

Die REST-API liefert eine Antwort mit dem Zugriffstoken und einem neuen Aktualisierungstoken:

```
{
  "access_token": "SamPLET346yoKeNSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOKenSaMP1et2590KenS123aMP1e926tOKenSaMP1e"
}
```

Sie können jetzt mithilfe des Zugriffstokens Anfragen an die REST-API senden. Jede Anfrage an die REST-API erfordert einen Zugriffstoken – eine Anfrage ohne Zugriffstoken gibt lediglich einen Autorisierungsfehler zurück.

Die REST-API verwenden

Im Rahmen von MDR ermöglicht die REST-API das Abrufen, Erstellen und Aktualisieren von Assets, Vorfällen, Reaktionen und Benutzern.

[OPEN THE REST API REFERENCE](#)

Die REST-API-Methoden erfordern einen Wert für die `client_id`. Sie können den Wert Ihrer `client_id` im Block **Token info** eines beliebigen Aktualisierungstokens in der MDR Web Console abrufen.

Im Folgenden sind Beispiele für Python- und Shell-Skripte aufgeführt, welche die Kernfunktionen der REST-API veranschaulichen:

- Zertifikatspfad, REST-API-URL, Client-ID und Token definieren
- Zugriffstoken und Aktualisierungstoken für das nächste Update des Zugriffstokens abrufen
- Anzahl der Assets abrufen
- Asset-Liste oder Asset-Details abrufen
- Anzahl der Vorfälle, der Vorfall-Liste, oder von Vorfällen-Details abrufen
- Reaktions-Liste für einen Vorfall abrufen
- Reaktionen bestätigen, ablehnen oder die Reaktions-Liste aktualisieren
- Liste an Kommentaren für den angegebenen Vorfall abrufen oder einen neuen Kommentar für den angegebenen Vorfall erstellen

Beispiel (Python):

```
#####
# Allgemeiner Teil
#####

import time
import datetime
import requests
import jwt

# Das Zertifikat wird für die Authentifizierung einer externen Ressource benötigt
# Sie können das Zertifikat von https://mdr.kaspersky.com herunterladen,
# es auf Ihrer Festplatte speichern und seinen Pfad der Variablen hinzufügen:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# ID Ihres Kunden und Ihres Tokens
# Für Einzelheiten zum Abrufen Ihrer ID und der Token-ID siehe Hilfe https://support.kaspersky.com/MDR/de-DE/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Fügen Sie Ihren Wert ein)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Fügen Sie Ihren Wert ein)
ACCESS_TOKEN = "AcCeSsToKeN" # (Fügen Sie Ihren Wert ein)

#####
# Zugriffstoken und Aktualisierungstoken (refresh token) für das nächste Update des Zugriffstokens anfordern
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN Ablaufdatum und -uhrzeit: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN ist aktuell")
    else:
        print(
            "Ihr REFRESH_TOKEN; muss aktualisiert werden. Übernehmen Sie ihn aus der MDR Console (https://support.kaspersky.com/MDR/de-DE/258285.htm)"
        )
        exit()
else:
    print(
        "Der Wert Ihres REFRESH_TOKEN muss gefüllt werden. Übernehmen Sie ihn aus der MDR Console (https://support.kaspersky.com/MDR/de-DE/258285.htm)"
    )
    exit()

# Prüfung, ob ein Zugriffstoken (access token) vorhanden und gültig ist
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: Ablaufdatum und -uhrzeit: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN ist aktuell")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# Bei Bedarf Zugriffs- und Refresh-Tokens für das nächste Update des Zugriffstokens aktualisieren
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()

    #Aktualisierungstoken muss gespeichert werden, um nach Ablauf des aktuellen Zugriffstokens den nächsten Zugriffstoken zu erhalten
    refresh_token = result_json["refresh_token"]
    print(
        f'Ihr neuer REFRESH_TOKEN für die nächste Anfrage eines ACCESS_TOKEN (ersetzen Sie den Wert für REFRESH_TOKEN durch diesen Wert): '
        f'{refresh_token}'
    )

    # Neuer Zugriffstoken zum Datenabruf erforderlich
    access_token = result_json["access_token"]
    print(f'Ihr neuer ACCESS_TOKEN (ersetzen Sie den Wert für ACCESS_TOKEN mit diesem Wert): "{access_token}"')

# Zugriffstoken zum Request-Header hinzufügen
headers = {"Authorization": f"Bearer {access_token}"}
```

```
#####
# Anzahl der Assets abrufen
#####

# Datum und Uhrzeit in Millisekunden seit 1970-01-01T00:00:00Z
request_body = {
    "max_last_seen": int(time.time())
    * 1000, # Maximale Zeit für das letzte Erscheinen des Assets auf die aktuelle Zeit beschränken
    "min_last_seen": 1639311132000, # Minimale Zeit für das letzte Erscheinen des Assets mit einer Konstanten beschränken - Sonntag, 12. Dezember 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())

#####
# Liste der Assets abrufen
#####

request_body = {
    # Suchparameter:
    "version": 2, # 2 als neue Version der Lösung festlegen
    "max_last_seen": int(time.time())
    * 1000, # Maximale Zeit für das letzte Erscheinen des Assets auf die aktuelle Zeit beschränken
    "min_last_seen": 1639311132000, # Minimale Zeit für das letzte Erscheinen des Assets mit einer Konstanten beschränken - Sonntag, 12. Dezember 2021
}
```

```

12:12:12 (GMT)
"domain": "",
"host_names": ["MA-MDR-KES-S", "SIN-MDR-KSC"], # (Fügen Sie Ihre Werte ein) Liste mit Hostnamen
"is_isolated": False,
"network_interface": "10.70.104.1",
"os_version": "Windows", # Betriebssystem-Name des Assets muss die angegebene enthalten
"product": "",
"search_phrase": "mdr", # Phrase zur Suche nach Feldwerten: "host_name", "domain", "installed_product_info", "network_interfaces", "os_version"
"statuses": ["OK", "ABSENT"], # Suche nach Assets mit hier angegebenen Statuswerten
# Optionen zur Anzeige von Suchergebnissen:
"sort": "first_seen:asc", # Sortierung der Ergebnisse nach dem Zeitpunkt des erstens Auftretens. Beim seitenweisen Abrufen von Ergebnissen muss für
die Sortierung ein Feld angegeben werden, das sich von Abfrage zu Abfrage nicht ändert, z. B. "first_seen" (Geben Sie keine Felder an, deren Werte sich
permanent ändern, z. B. das Feld "last_seen", da dies die Ergebnisse verfälschen kann)
"page_size": 100, # Assets pro Seite - 100
"page": 1, # Erste Seite der Suchergebnisse anzeigen
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Asset-Details abrufen
#####

request_body = {
    "version": 2, # 2 als neue Version der Lösung festlegen
    "asset_id": "0xFA6A68CC9A9415963DE841048A3BE929", # (Fügen Sie Ihren Wert ein) Asset-ID
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
).json()
print(result)

#####
# Anzahl der Vorfälle abrufen
#####

request_body = {
    "max_update_time": int(time.time())
    * 1000, # Maximale Zeit des letzten Vorfall-Updates auf die aktuelle Zeit beschränken
    "min_update_time": 1639311132000, # Minimale Zeit für das letzte Vorfall-Update mit einer Konstanten beschränken - Sonntag, 12. Dezember 2021
12:12:12 (GMT)
    "affected_hosts": [
        "MA-MDR-KES-S-0xFA6A68CC9A94145456E841048A3BE929"
    ], # (Fügen Sie Ihren Wert ein) Hostliste im "host_name:asset_id"-Format
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Liste der Vorfälle abrufen
#####

request_body = {
    # Suchparameter:
    "max_creation_time": int(time.time())
    * 1000, # Maximale Zeit für die Erstellung von Vorfällen auf die aktuelle Zeit beschränken
    "min_creation_time": 1639311132000, # Minimale Zeit für die Erstellung von Vorfällen mit einer Konstanten beschränken - Sonntag, 12. Dezember 2021
12:12:12 (GMT)
    "asset_ids": [
        "0xFA6A68CC9A9415963DE841048A3BE929"
    ], # (Fügen Sie Ihren Wert ein) Liste mit Assets, deren Vorfälle abgerufen werden sollen
    "priorities": ["HIGH"],
    "resolutions": ["True positive"],
    "response_statuses": ["Confirmed"],
    "response_types": ["hash"],
    "statuses": ["Closed"],
    # Parameter für die Aufbereitung der Ergebnisse
    "markdown_to_html": True, # Ergebnisse im html-Format ausgeben. Bei "False" wird das Markdown-Format verwendet
    "sort": "creation_time:asc", # Sortierung der Ergebnisse nach dem Zeitpunkt der Vorfallerstellung. Beim seitenweisen Abrufen von Ergebnissen muss
für die Sortierung ein Feld angegeben werden, das sich von Abfrage zu Abfrage nicht ändert, z. B. "creation_time" (Geben Sie keine Felder an, deren
Werte sich permanent ändern, z. B. das Feld "update_time", da dies die Ergebnisse verfälschen kann)
    "page_size": 100, # Vorfälle pro Seite - 100
    "page": 1, # Erste Seite der Suchergebnisse anzeigen
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Details zu einem Vorfall abrufen
#####

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m", # (Fügen Sie Ihren Wert ein) Vorfalls-ID
    "markdown_to_html": True, # Ergebnisse im html-Format ausgeben. Bei "False" wird das Markdown-Format verwendet
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Reaktions-Liste für einen Vorfall abrufen
#####

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m", # (Fügen Sie Ihren Wert ein) Vorfalls-ID
    "page_size": 10, # Reaktionen pro Seite - 10
    "page": 1, # Erste Seite der Suchergebnisse anzeigen
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)

```

```

)
print(result.json())

#####
# Eine Reaktion bestätigen
#####

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W", # (Fügen Sie Ihren Wert ein) Reaktions-ID
    "comment": "comment_text", # Kommentar, der zur Reaktion hinzugefügt werden soll
    "status": "Confirmed", # Neuer Status der Reaktion - "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Eine Antwort ablehnen
#####

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W", # (Fügen Sie Ihren Wert ein) Reaktions-ID
    "comment": "comment_text", # Kommentar, der zur Reaktion hinzugefügt werden soll
    "status": "Declined", # Neuer Status der Reaktion - "Declined"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Liste mit Reaktionen aktualisieren
#####

request_body = {
    "responses_ids": [
        "CEgYG4UBMUGN-LWULP7W",
        "2ES16IgB4cAOuyXBb5IB",
    ], # (Fügen Sie Ihre Werte ein) Reaktions-IDs
    "comment": "comment_text", # Kommentar, der zu den Reaktionen hinzugefügt werden soll
    "status": "Confirmed", # Neue Statuswerte der Reaktionen - "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

```

Beispiel (Shell):

```
#Zugriffstoken und neuen Aktualisierungstoken abrufen
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
# Beispielantwort. Verwenden Sie als nächstes "access_token", um die Daten abzurufen, und "refresh_token", um den neuen Zugriffstoken und den
Aktualisierungstoken abzurufen
{
  "access_token": "SamPLET346yoKEsSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkEnSaMPlEt259OkEnS123aMPlE926tOkEnSaMPlE"
}

# Anzahl der Assets abrufen
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}'

# Liste der Assets abrufen
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}'

# Asset-Details abrufen
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}'

# Anzahl der Vorfälle abrufen
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"]}'

# Liste der Vorfälle abrufen
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}'

# Details zu einem Vorfall abrufen
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}'

# Reaktions-Liste für einen Vorfall abrufen
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}'

# Eine Reaktion aktualisieren
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"}'

# Liste mit Reaktionen aktualisieren
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", "2ES16IgB4cA0UyXB5iB"], "comment": "comment_text", "status": "Confirmed"}'
```

Beispiel einer REST-API-Antwort mit Zugriffstoken und neuem Aktualisierungstoken:

```
{
  "access_token": "SamPLET346yoKEsSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkEnSaMPlEt259OkEnS123aMPlE926tOkEnSaMPlE"
}
```

Beispiel einer REST-API-Antwort mit Struktur und Werten von Kommentaren:

```
[{
  "comment_id": "bfu6TiNghqp",
  "author_name": "Mandy Musterfrau",
  "text": "<p>Der erste Kommentar</p>",
  "creation_time": 1601295428640
}, {
  "comment_id": "bfu6TiNghqt",
  "author_name": "Max Mustermann",
  "text": "<p>Der zweite Kommentar</p>",
  "creation_time": 1601295433441
}]
```

Beispiel einer REST-API-Antwort, wenn die REST-API einen neuen Kommentar erstellt und eine Antwort mit Kommentardetails liefert:

```
{
  "comment_id": "AXTej0Qi4bfu6TiNgmvT",
```

```
"author_name": "Tokenname",  
"text": "Dieser neue Kommentar wurde mit der REST API erstellt",  
"creation_time": 1601461748122  
}
```

Einen Aktualisierungstoken in Kaspersky Security Center widerrufen

Sie können Aktualisierungstoken von API-Verbindungen widerrufen, die als aktuellen Status *Aktiv* oder *Inaktiv* haben.

So widerrufen Sie einen Aktualisierungstoken:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **API**.

Die Liste mit den **API** wird angezeigt.

2. Klicken Sie auf die API-Verbindung, von der Sie ein Aktualisierungstoken widerrufen möchten.

Es wird ein Block mit den Verbindungsinformationen angezeigt.

3. Klicken Sie auf die Schaltfläche **Widerrufen**.

Der Aktualisierungstoken wird widerrufen.

Eine API-Verbindung in Kaspersky Security Center löschen

Vorhandene API-Verbindungen können gelöscht werden.

So löschen Sie eine API-Verbindung:

1. Klicken Sie in Kaspersky Security Center im Abschnitt **MDR** auf die Registerkarte **API**.

Die Liste mit den **API** wird angezeigt.

2. Aktivieren Sie das Optionsfeld neben der API-Verbindung, die Sie löschen möchten, und klicken Sie auf **Verbindung löschen**.

Die ausgewählte API-Verbindung wird gelöscht.

Eine API-Verbindung in der MDR Web Console löschen

Vorhandene API-Verbindungen können bearbeitet werden.

So bearbeiten Sie eine API-Verbindung:

1. Klicken Sie in der MDR Web Console auf die Registerkarte **API**.

Die Liste **All tokens** wird angezeigt.

2. Wählen Sie API-Verbindung aus, die Sie löschen möchten, und klicken Sie anschließend auf das Papierkorbsymbol () auf der rechten Seite der Zeile.

Die ausgewählte API-Verbindung wird gelöscht.

Kaspersky Managed Detection and Response deaktivieren

Wenn Sie die Verwendung von Kaspersky Managed Detection and Response einstellen möchten, können Sie dessen Nutzung entweder dauerhaft beenden oder für ausgewählte Assets vorübergehend aussetzen.

Die Nutzung von Kaspersky Managed Detection and Response beenden

Wenn Sie die Nutzung von Kaspersky Managed Detection and Response beenden möchten, können Sie es manuell deaktivieren.

Wenn Sie die Nutzung von Kaspersky Managed Detection and Response beenden, stellt Kaspersky Managed Detection and Response das Übertragen von Telemetriedaten von Ihren Assets ein. Um die Daten Ihres Unternehmens aus der Infrastruktur von Kaspersky Managed Detection and Response zu löschen, wenden Sie sich bitte an den [Technischen Support](#).

So beenden Sie die Nutzung von Kaspersky Managed Detection and Response

1. Wenn Sie [EPP-Anwendungen](#) verwenden, die Richtlinien unterstützen, wechseln Sie in der Kaspersky Security Center Web Console oder in Kaspersky Next Expert View zum Abschnitt **Assets (Geräte)** → **Richtlinien und Profile**.

Wenn Sie eine EPP-Anwendung verwenden, die keine Richtlinien unterstützt, wechseln Sie zum Abschnitt **Assets (Geräte)** → **Aufgaben**.

Die Liste der Richtlinien (oder die Liste der Aufgaben) wird geöffnet.

2. Klicken Sie auf eine Richtlinie oder Aufgabe, die Sie während der Bereitstellung von Kaspersky Managed Detection and Response erstellt haben, um die Integration zwischen einer EPP-Anwendung und Kaspersky Managed Detection and Response einzurichten.

Das Fenster mit den Richtlinieneinstellungen (oder das Fenster mit den Aufgabeneinstellungen) wird geöffnet.

3. Wählen Sie im linken Bereich der Registerkarte **Programmeinstellungen** die Option **Detection and Response** und anschließend im rechten Bereich **Managed Detection and Response**.

Der Einstellungsbereich für **Managed Detection and Response** wird geöffnet.

4. Deaktivieren Sie die Option **Managed Detection and Response ist aktiviert**.

Der Name der Option ändert sich in **Managed Detection and Response deaktiviert**.

5. Speichern Sie die Änderungen in der Richtlinie oder Aufgabe.

6. [Widerrufen Sie Ihre Einwilligung in die Nutzungsbedingungen der MDR-Lösung](#).
7. Wenn Sie eine lokale Bereitstellung von Kaspersky Security Center Web Console im Zusammenspiel mit Kaspersky MDR verwenden, wird es zusätzlich empfohlen, [die KPSN-Konfigurationsdatei von vom Kaspersky Security Center Administrationsserver zu entfernen](#) [↗].

Die Nutzung von Kaspersky Managed Detection and Response ist beendet.

Die Nutzung von Kaspersky Managed Detection and Response vorübergehend aussetzen

Um die [Nutzungsbedingungen der MDR-Lösung](#) einzuhalten, ist es erforderlich, die Verwendung der Lösung auf Assets auszusetzen, wenn sich diese Assets vorübergehend auf dem Territorium der Vereinigten Staaten befinden (etwa während Rahmen einer Dienstreise).

So setzen Sie die Verwendung der MDR-Lösung auf bestimmten Assets vorübergehend aus:

1. Erstellen Sie in Kaspersky Security Center eine neue [Administrationsgruppe](#) [↗] zur Verwaltung der Assets, auf denen Sie die Verwendung der MDR-Lösung vorübergehend aussetzen möchten. Sie können die Liste der Assets in dieser Gruppe später ändern.
2. [Erstellen Sie für diese Administrationsgruppe neue Richtlinien](#) [↗] für die EPP-Anwendungen, die zur Bereitstellung der Telemetriedaten der Assets verwendet werden, und deaktivieren Sie anschließend die Verwendung der MDR-Lösung und von Kaspersky Security Network in den Richtlinieneinstellungen.

Weitere Informationen zur Konfiguration der Richtlinien finden Sie den Hilfe-Artikeln der entsprechenden EPP-Anwendungen. Beispielsweise enthält die Hilfe von Kaspersky Endpoint Security für Windows Anleitungen zur [Verwaltung von Richtlinien](#) [↗] und zur Konfiguration der [Integration mit der MDR-Lösung](#) [↗].

3. [Verschieben Sie die Assets](#) [↗], auf denen Sie die Verwendung der MDR-Lösung aussetzen möchten, in die erstellte Administrationsgruppe.

Die neue Richtlinie mit deaktivierter Nutzung der MDR-Lösung und von Kaspersky Security Network wird nach der Synchronisierung auf die Assets angewendet. Sie können auch [die Synchronisation manuell erzwingen](#) [↗].

So setzen Sie eine ausgesetzte Verwendung von Kaspersky Managed Detection and Response fort:

1. Entfernen Sie das Asset aus der Administrationsgruppe, die zum Aussetzen verwendet wurde.
2. Wenden Sie eine reguläre Richtlinie mit aktivierter und konfigurierter Verwendung der MDR-Lösung auf das Asset an.

Das Asset wird erst dann von der MDR-Lösung überwacht, wenn eine Richtlinie mit aktivierter und konfigurierter Verwendung der MDR-Lösung auf das Asset angewendet wird.

Widerruf Ihrer Einwilligung in die Nutzungsbedingungen der MDR-Lösung

Wenn Sie sich dazu entschließen, Kaspersky Managed Detection and Response nicht mehr zu verwenden, widerrufen Sie Ihre Einwilligung in die Nutzungsbedingungen der MDR-Lösung und [deaktivieren Sie anschließend die Verwendung von Kaspersky Managed Detection and Response auf den Assets](#).

Diese Funktion ist nur verfügbar, wenn Sie in der [Kaspersky Security Center Web Console](#) [☐] oder in [Kaspersky Next Expert View](#) [☐] das Zugriffsrecht **Integration von Anwendungen** festgelegt haben.

So widerrufen Sie Ihre Einwilligung in die Nutzungsbedingungen der MDR-Lösung:

1. Klicken Sie im Fenster von Kaspersky Security Center im Abschnitt MDR auf die Registerkarte **MDR-Nutzung**.
2. Erweitern Sie den Block **Nutzungsbedingungen für die MDR-Lösung**, indem Sie auf dessen Namen klicken.
3. Klicken Sie auf den Link **Zustimmung zu den Nutzungsbedingungen für die MDR-Lösung widerrufen**
4. Bestätigen Sie, dass Sie Ihre Einwilligung in die Nutzungsbedingungen der MDR-Lösung widerrufen möchten.
Ihre Einwilligung in die Nutzungsbedingungen der MDR-Lösung wird widerrufen.

Wenn Sie die Informationen zu Ihrer Organisation aus der MDR-Infrastruktur entfernen möchten, wenden Sie sich bitte an den [Technischen Support](#).

Bekannte Probleme

Kaspersky Managed Detection and Response weist eine Reihe von Einschränkungen auf, die aber für die Ausführungs des Programms nicht kritisch sind:

- Beim Klonen eines virtuellen oder physischen Assets, auf dem bereits Kaspersky Endpoint Security für Linux mit der MDR-Lösung verbundenen wurde, werden die Telemetriedaten des geklonten Assets nicht korrekt übertragen. Entfernen Sie auf den geklonten Assets Kaspersky Endpoint Security for Linux und löschen Sie die Datei "install_id" im Ordner "/var/opt/kaspersky/epagent/" dieser Assets. Installieren Sie anschließend Kaspersky Endpoint Security for Linux erneut.
- Für Assets mit Kaspersky Endpoint Security für Windows in der Konfiguration des Agenten für Endpoint Detection and Response (EDR Agent) werden die Statuszustände *Warnung* und *Kritisch* für Schutz- und Kontrollkomponenten nicht angezeigt.
- Sie können die [Funktionen von Kaspersky Endpoint Detection and Response Optimum](#) nicht für Assets mit Kaspersky Endpoint Security für Windows in der EDR Agent-Konfiguration verwenden.
- In der MDR Web Console können auf Asset-Karten im Abschnitt **Kaspersky Programme, die MDR verwenden** veraltete EPP-Anwendungen (Endpoint Protection Platform) angezeigt werden, die nicht mehr für Kaspersky Managed Detection and Response verwendet werden. Das Verhalten tritt auf, wenn auf einem Asset eine veraltete EPP-Anwendung durch eine neue ersetzt wurde. Bei diesen veralteten Anwendungen enthält das Feld **Zuletzt sichtbar** das alte Datum, während für die neue EPP-Anwendung das Feld **Zuletzt sichtbar** das neuere Datum enthält.
- Eine MDR-Lösung, die eine KPSN-Konfiguration verwendet, unterstützt keine Hierarchie von Kaspersky Security Center Administrationsservern, wenn in der Hierarchie nur der primäre Server über einen Internetzugang verfügt.
- Das automatische Hochladen von Dateien, die größer als 64 MB sind, wird durch die MDR-Lösung nicht unterstützt, wenn die [Reaktion Get artefacts](#) verwendet wird. Diese Reaktion ist über Kaspersky Endpoint Detection and Response Expert verfügbar, das in die Open Single Management Platform integriert ist.
- Die Anzeige von Informationen über Kaspersky Embedded Systems Security für Linux Version 4.0 oder höher in der Liste der nicht funktionierenden Assets wird durch das MDR-Plug-in für Kaspersky Security Center und das MDR-Plug-in für die Open Single Management Platform nicht unterstützt.

Anfrage an den Technischen Support

Dieser Abschnitt beschreibt, wie und unter welchen Bedingungen Sie technischen Support erhalten.

Technischen Support erhalten

Wenn Sie in der [Dokumentation zu Kaspersky Managed Detection and Response](#) oder in einer der [Informationsquellen zu Kaspersky Managed Detection and Response](#) keine Lösung für Ihr Problem finden, wenden Sie sich an den Kaspersky Kundenservice. Die Spezialisten des Technischen Supports beantworten alle Ihre Fragen zur Installation und Verwendung von Kaspersky Managed Detection and Response.

Kaspersky bietet den Support für Kaspersky Managed Detection and Response innerhalb des Zeitraums an, der durch den Lebenszyklus vorgesehen ist (siehe auch: [Seite mit Lebenszyklen unserer Anwendungen](#)). Lesen Sie bitte die [Supportregeln](#), bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit dem Technischen Support ist auf folgende Weise möglich:

- [Durch das Aufrufen der Website des Technischen Supports](#)
- Durch das Senden einer Anfrage an den Technischen Support über das Portal [Kaspersky CompanyAccount](#)

Technischer Support über Kaspersky CompanyAccount

[Kaspersky CompanyAccount](#) ist ein Portal für Unternehmen, die Kaspersky-Programme verwenden. Das Portal "Kaspersky CompanyAccount" soll die Interaktion zwischen Benutzern und Kaspersky-Spezialisten durch Online-Anfragen erleichtern. Mithilfe von Kaspersky CompanyAccount können Sie den Status Ihrer Online-Anfragen verfolgen und eine Chronik mit allen Anfragen speichern.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Mithilfe eines einheitlichen Kontos können Sie die Online-Anfragen der bei Kaspersky registrierten Mitarbeiter zentral verwalten und die Berechtigungen dieser Mitarbeiter für Kaspersky CompanyAccount verwalten.

Das Portal Kaspersky CompanyAccount ist in den folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch

- Russisch
- Französisch
- Japanisch

Weitere Informationen über Kaspersky CompanyAccount finden Sie auf der [Webseite des Technischen Supports](#)¹².

Informationsquellen zu dieser Lösung

Auf der Seite [Kaspersky Managed Detection and Response](#) können Sie allgemeine Informationen zu dieser Lösung, ihren Funktionen und ihren Merkmale anzeigen.

Glossar

Asset

Ein Gerät mit einer installierten EPP-Anwendung von Kaspersky (z. B. Kaspersky Endpoint Security für Windows).

Endpoint Protection Platform (EPP)

Ein integriertes System mit komplexem Schutz für Endgeräte (z. B. Mobilgeräte, Computer oder Laptops), das verschiedene Sicherheitstechnologien umfasst. Ein Beispiel für eine Endpoint Protection Platform ist Kaspersky Endpoint Security for Business.

EPP-Anwendung

Eine Anwendung, die in einem Schutzsystem für Endpunktgeräte enthalten ist (Endpoint Protection Platform oder EPP). EPP-Anwendungen werden auf den Endgeräten innerhalb der IT-Infrastruktur eines Unternehmens installiert (z. B. Mobilgeräte, Computer oder Laptops). Ein Beispiel für eine EPP-Anwendung ist Kaspersky Endpoint Security für Windows als Teil der EPP-Lösung Kaspersky Endpoint Security for Business.

IOC

Ein Kompromittierungsindikator (oder IOC) zeigt auf einem Gerät die Hinweise an, die auf eine Sicherheitsverletzung hinweisen.

Mandant

Ein Mandant ist eine Organisation, für die Sie Kaspersky Managed Detection and Response bereitstellen.

MITRE Tactic

Das Ziel, das ein Angreifer bei einem Cyberangriff auf die Client-Infrastruktur erreichen wollte.

MITRE Technique

Die vom Angreifer verwendete Methode, um während eines Cyberangriffs auf die Client-Infrastruktur böswillige Aktionen auszuführen. Jede MITRE Tactic umfasst eine Reihe von MITRE Techniques.

Reaktion

Die Reaktion auf einen Vorfall ist ein strukturierter Vorgang im Umgang mit Sicherheitsvorfällen, Sicherheitsverletzungen und Cyberbedrohungen.

Telemetriedaten

Daten, die von Assets an Kaspersky Managed Detection and Response gesendet werden.

Vorfall

Eine Aktivität, die von der Erkennungstechnologie als kritisch eingestuft wird und eine sofortige Reaktion von Kaspersky Managed Detection and Response erfordert.

Informationen über den Code von Drittherstellern

Bei der Entwicklung der Lösung wurde Code von Drittherstellern verwendet.

Informationen über den in MDR Web Console verwendeten Drittherstellercode erhalten Sie beim Support für Kaspersky Managed Detection and Response.

Informationen über den im MDR-Plugin verwendeten Drittanbieter-Code finden Sie in der Datei [legal_notices.txt](#).

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Apple, Mac, macOS und Safari sind Markenzeichen von Apple Inc.

Amazon AWS und Amazon Web Services sind Markenzeichen von Amazon.com, Inc. oder seinen Tochtergesellschaften.

Active Directory, Internet Explorer, Microsoft, Microsoft Edge, Outlook, PowerShell, Windows PowerShell, Windows und Windows Server sind Markenzeichen der Microsoft-Unternehmensgruppe.

Firefox und Mozilla sind Markenzeichen der Mozilla Foundation in den USA und anderen Ländern.

Google und Google Chrome sind Markenzeichen von Google, Inc.

Linux ist die eingetragenes Markenzeichen von Linus Torvalds in den USA und anderen Ländern.

Python ist ein Markenzeichen oder eingetragenes Markenzeichen der Python Software Foundation.

Die Überwachungseinstellungen für den Betrieb mit Kaspersky Managed Detection and Response konfigurieren

Wir empfehlen, die folgenden Überwachungseinstellungen anzupassen, um einen stabilen Betrieb zu gewährleisten und die Effizienz von Kaspersky Managed Detection and Response zu maximieren:

- **Konfiguration der Überwachungsrichtlinie von Windows-Ereignissen:**

Um die Effizienz von Kaspersky Managed Detection and Response zu maximieren, müssen Sie die Überwachungsrichtlinie von Windows-Ereignissen auf Ihren Assets konfigurieren.

So konfigurieren Sie die Überwachungsrichtlinie von Windows-Ereignissen:

1. Drücken Sie auf Ihrem Windows-Assets **Win+R**, um das Fenster **Ausführen** zu öffnen.
2. Geben Sie im **Öffnen**-Feld `gpedit.msc` ein und drücken Sie die **Eingabetaste** oder klicken Sie auf **OK**. Das Fenster **Editor für lokale Gruppenrichtlinien** wird angezeigt.
3. Klicken Sie in der Konsolenstruktur auf **Computerkonfiguration** → **Windows-Einstellungen** → **Sicherheitseinstellungen** → **Erweiterte Konfiguration der Überwachungsrichtlinie** → **Systemüberwachungsrichtlinien – Lokales Gruppenrichtlinienobjekt**.
4. Klicken Sie auf den Knoten **Kontoanmeldung**. Geben Sie auf der rechten Seite des Fensters folgende Werte an:

Unterkategorie	Überwachungsereignisse
Überprüfen der Anmeldeinformationen überwachen	Erfolg und Fehler
Kerberos-Authentifizierungsdienst überwachen	Erfolg und Fehler
Ticketvorgänge des Kerberos-Diensts überwachen	Erfolg und Fehler

5. Klicken Sie auf den Knoten **Kontoverwaltung**. Geben Sie auf der rechten Seite des Fensters folgende Werte an:

Unterkategorie	Überwachungsereignisse
Computerkontoverwaltung überwachen	Erfolg und Fehler
Sicherheitsgruppenverwaltung überwachen	Erfolg
Benutzerkontenverwaltung überwachen	Erfolg und Fehler

6. Klicken Sie auf den Knoten **DS-Zugriff**. Geben Sie auf der rechten Seite des Fensters folgende Werte an:

Unterkategorie	Überwachungsereignisse
Verzeichnisdienstzugriff überwachen	Erfolg und Fehler
Verzeichnisdienständerungen überwachen	Erfolg und Fehler

7. Klicken Sie auf den Knoten **Anmelden/Abmelden**. Geben Sie auf der rechten Seite des Fensters folgende Werte an:

Unterkategorie	Überwachungsereignisse
Kontosperrung überwachen	Fehler
Anmelden überwachen	Erfolg und Fehler
Spezielle Anmeldung überwachen	Erfolg und Fehler

8. Klicken Sie auf den Knoten **Objektzugriff**. Geben Sie auf der rechten Seite des Fensters folgende Werte an:

Unterkategorie	Überwachungsereignisse
Zertifizierungsdienste überwachen	Erfolg und Fehler
Dateifreigabe überwachen	Erfolg
Filterplattformverbindung überwachen	Erfolg
Andere Objektzugriffsereignisse überwachen	Erfolg

9. Klicken Sie auf den Knoten **Richtlinienänderung**. Geben Sie auf der rechten Seite des Fensters folgende Werte an:

Unterkategorie	Überwachungsereignisse
Überwachungsrichtlinienänderung überwachen	Erfolg
MPSSVC-Richtlinienänderung auf Regelebene überwachen	Erfolg

10. Klicken Sie auf den Knoten **Berechtigungen**. Geben Sie auf der rechten Seite des Fensters folgende Werte an:

Unterkategorie	Überwachungsereignisse
Sensible Verwendung von Rechten überwachen	Erfolg

11. Klicken Sie auf den Knoten **System**. Geben Sie auf der rechten Seite des Fensters folgende Werte an:

Unterkategorie	Überwachungsereignisse
Sicherheitsstatusänderung überwachen	Erfolg
Sicherheitssystemerweiterung überwachen	Erfolg

12. Klicken Sie in der Konsolenstruktur auf **Computerkonfiguration** → **Verwaltungsvorlagen** → **Windows-Komponenten** → **Windows PowerShell**. Geben Sie auf der rechten Seite des Fensters folgende Werte an:

Unterkategorie	Überwachungsereignisse
Aktivieren Sie für PowerShell die Protokollierung von Skriptblöcken	Aktiviert

13. Schließen Sie das Fenster **Editor für lokale Gruppenrichtlinien**.

Alle Änderungen werden automatisch gespeichert.

Die Überwachungsrichtlinie von Windows-Ereignissen ist jetzt für die Arbeit mit Kaspersky Managed Detection and Response konfiguriert.

- **Konfiguration der Überwachung für Active Directory-Objekte:**

Um die Effizienz von Kaspersky Managed Detection and Response zu maximieren, müssen Sie auf Ihren Assets die Überwachung konfigurieren.

So konfigurieren Sie die Überwachung für Active Directory-Objekte:

1. Drücken Sie auf Ihrem Windows-Domänencontroller **Win+R**, um das Fenster **Ausführen** zu öffnen.
2. Geben Sie im Feld **Öffnen** den Text `dsa.msc` ein und drücken Sie anschließend die **Eingabetaste** oder klicken Sie auf **OK**. Das Fenster **Active Directory-Benutzer und -Computer** wird angezeigt.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf <Ihren Domännennamen> und wählen Sie **Suchen** aus. Das Fenster **Benutzer, Kontakte und Gruppen suchen** wird angezeigt.
4. Geben Sie in dem Feld **Name** das Wort **Administrator** ein und klicken Sie auf **Jetzt suchen**.
5. Klicken Sie im Bereich mit den **Suchergebnissen** mit der rechten Maustaste auf das Objekt **Administrator** und wählen Sie anschließend unter **Eigenschaften** → **Sicherheit** → **Erweitert** die Registerkarte **Überwachung** aus.
6. Klicken Sie auf **Hinzufügen**, um das Fenster **Überwachungseintrag für Administratoren** zu öffnen. Klicken Sie auf **Prinzipal auswählen** und geben Sie `Jeder` an. Klicken Sie anschließend auf **Namen prüfen** und abschließend auf **OK**.
7. Aktivieren Sie im Fenster **Überwachungseintrag für Administratoren** die Kontrollkästchen **Inhalte auflisten**, **Leseberechtigungen**, **Berechtigungen ändern**, **Besitzer ändern**, **Alle Eigenschaften lesen** und **Alle Eigenschaften schreiben**.
8. Klicken Sie auf die Schaltflächen **OK** → **Übernehmen** → **OK**.

Der Audit für das Active Directory-Objekt **Administrator** ist jetzt für die Verwendung mit Kaspersky Managed Detection and Response konfiguriert.

9. Führen Sie dieselben Schritte für die folgenden standardmäßigen Active Directory-Objekte und Ihre sensiblen Domänenbenutzer und Domänengruppen aus, die in Ihrem System vorhanden und aktiviert sind:

- **Administratoren**
- **Zulässige RODC-Kennwortreplikationsgruppe**
- **Cert-Herausgeber**
- **Klonbare Domänencontroller**
- **Abgelehnte RODC-Kennwortreplikationsgruppe**
- **DnsAdmins**
- **DnsUpdateProxy**
- **Domänenadministratoren**
- **Domänencomputer**
- **Domänencontroller**
- **Organisationsadministratoren**
- **Administratoren von Unternehmensschlüsseln**

- Organisationsschlüsseladministratoren
- Gruppenrichtlinien Ersteller Besitzer
- Schlüsseladministratoren
- krbtgt
- Geschützte Benutzer
- RAS- und IAS-Server
- Schreibgeschützte Domänencontroller
- Schemaadministratoren
- Konfigurieren der Überwachung für die Active Directory Certificate Services, Zertifikatvorlagen und Zertifikatobjekte

Um die Effizienz von Kaspersky Managed Detection and Response zu maximieren, müssen Sie die Überwachung des Dienstes **Active Directory Certificate Services**, der Zertifikatvorlagen und der Objekte auf den Hosts mit aktivierten **Active Directory Certificate Services** (AD CS) konfigurieren.

*So konfigurieren Sie die Überwachung für den Dienst **Active Directory Certificate Services**:*

1. Drücken Sie **Win+R**, um das Fenster **Ausführen** zu öffnen.
2. Geben Sie im **Öffnen**-Feld `cmd` ein und drücken Sie die **Eingabetaste** oder klicken Sie auf **OK**. Das Fenster **Eingabeaufforderung** wird angezeigt.
3. Um die Überwachungseinstellungen für die Zertifizierungsstelle zu konfigurieren, geben Sie die folgenden Befehle ein und drücken Sie anschließend die Eingabetaste:
`certutil -setreg CA\AuditFilter 127`
`certutil -setreg policy\EditFlags +EDITF_AUDITCERTTEMPLATELOAD`
4. Um den Dienst **Certificate Services** neu zu starten, geben Sie den folgenden Befehl ein und drücken Sie anschließend die Eingabetaste:
`net stop certsvc && net start certsvc`

So konfigurieren Sie die Sicherheitsüberwachung für Zertifikatvorlagen:

1. Drücken Sie **Win+R**, um das Fenster **Ausführen** zu öffnen.
2. Geben Sie im **Öffnen**-Feld `adsiedit.msc` ein und drücken Sie die **Eingabetaste** oder klicken Sie auf **OK**.
3. Klicken Sie mit der rechten Maustaste auf **ADSI-Editor** und wählen Sie anschließend **Verbindung herstellen** aus.
4. Wählen Sie im Abschnitt **Verbindungspunkt** im Feld **Bekannten Namenskontext auswählen** die Option **Konfiguration** aus.
5. Doppelklicken Sie im linken Bereich auf **Konfiguration/Schema**.
6. Wählen Sie den Ordner **CN=Configuration,DC=...** → **CN=Services** → **CN=Public Key Services** → **CN=Certificate Templates** aus.

7. Klicken Sie mit der rechten Maustaste auf den Ordner **CN=Certificate Templates**, wählen Sie **Eigenschaften** aus und öffnen Sie anschließend die Registerkarte **Sicherheit**.
8. Klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie anschließend die Registerkarte **Überwachung** aus.
9. Klicken Sie auf das Prinzipal **Jeder**, aktivieren Sie die Kontrollkästchen **Alle Eigenschaften schreiben**, **Löschen**, **Berechtigungen ändern**, **Besitzer ändern** und **Alle validierten Schreibvorgänge** und klicken Sie anschließend auf **OK**.

So konfigurieren Sie die Sicherheitsüberwachung für das NTAAuthCertificates-Objekt:

1. Geben Sie im **Öffnen**-Feld `adsiedit.msc` ein und drücken Sie anschließend die **Eingabetaste** oder klicken Sie auf **OK**.
2. Klicken Sie mit der rechten Maustaste auf **ADSI-Editor** und wählen Sie anschließend **Verbindung herstellen** aus.
3. Wählen Sie im Abschnitt **Verbindungspunkt** im Feld **Bekannten Namenskontext auswählen** die Option **Konfiguration** aus.
4. Doppelklicken Sie im linken Bereich auf **Konfiguration/Schema**.
5. Wählen Sie den Ordner **CN=Configuration,DC=...** → **CN=Services** → **CN=Public Key Services** → **CN=NTAuthCertificates** aus.
6. Klicken Sie mit der rechten Maustaste auf den Ordner **CN=NTAuthCertificates**, wählen Sie **Eigenschaften** aus und öffnen Sie anschließend die Registerkarte **Sicherheit**.
7. Klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie anschließend die Registerkarte **Überwachung** aus.
8. Klicken Sie auf das Prinzipal **Jeder**, aktivieren Sie die Kontrollkästchen **Alle Eigenschaften schreiben**, **Löschen**, **Berechtigungen ändern**, **Besitzer ändern** und **Alle validierten Schreibvorgänge** und klicken Sie anschließend auf **OK**.

Onboarding-Video

Sie können sich das Video anschauen, um mehr über die Hauptfunktionen der MDR-Lösung zu erfahren.



MDR-Lösung. Onboarding-Video