

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 teal and green abstract shapes. The logo itself is black.

**kaspersky**

# **Kaspersky Managed Detection and Response**

© 2026 AO Kaspersky Lab

# Contents

[Kaspersky Managed Detection and Response Help](#)

[What's new](#)

[About Kaspersky Managed Detection and Response](#)

[Operating principle of Kaspersky Managed Detection and Response](#)

[Areas of responsibility](#)

[Hardware and software requirements](#)

[Kaspersky Managed Detection and Response components](#)

[Activating and deploying Kaspersky Managed Detection and Response](#)

[Components required for MDR operation](#)

[Integration with Kaspersky applications and solutions](#)

[Configuring MDR Plug-in](#)

[Activating and deploying MDR when using up-to-date application versions and a single tenant](#)

[Activating and deploying MDR when using up-to-date application versions and multitenancy](#)

[Activating and deploying MDR when using legacy application versions](#)

[Deploying a KPSN configuration file](#)

[Deploying an MDR configuration \(BLOB\) file](#)

[Deployment by capturing and copying the image of a device](#)

[Activating the MDR solution in Kaspersky applications](#)

[Activating the MDR solution in Kaspersky applications. Kaspersky MDR Add-on licenses](#)

[Activating the MDR solution in Kaspersky applications. Kaspersky MDR licenses](#)

[Activating the MDR solution in Kaspersky applications. Kaspersky Symphony MDR, Kaspersky Next Complete Security, Kaspersky Optimum Security and Kaspersky Next MXDR Optimum licenses](#)

[Activating the MDR solution in Kaspersky applications. Kaspersky Managed Detection and Response for Industrial CyberSecurity Add-on license](#)

[Licensing](#)

[Comparison of commercial license tiers](#)

[About the activation code](#)

[Providing a new activation code](#)

[Managing licenses in Kaspersky Security Center](#)

[Licensing troubleshooting](#)

[About the MDR Agreement](#)

[Data provision](#)

[Regions of data processing](#)

[About the Data Processing Agreement](#)

[Interfaces of Kaspersky Managed Detection and Response](#)

[MDR section in Kaspersky Security Center](#)

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

[Setting access rights in Kaspersky Security Center](#)

[Viewing and editing the MDR settings in Kaspersky Security Center](#)

[Using MDR Plug-in functions on a virtual Administration Server](#)

[Using MDR functions in Kaspersky Security Center through a proxy server](#)

[Changing the certificates to use MDR functions in Kaspersky Security Center with a proxy server or anti-virus software](#)

[Hiding and showing the MDR features in Kaspersky Security Center](#)

[MDR Web Console](#)

[Switching the interface language in Kaspersky Security Center](#)

[Switching the language for notifications and reports in Kaspersky Security Center](#)

[Switching the interface language in MDR Web Console](#)

[About the MDR configuration file](#)

[About Kaspersky Security Network](#)

[Periodic update of KPSN configuration files](#)

[Switching the MDR solution to operation without KPSN configuration files](#)

[Monitoring dashboards in MDR Web Console](#)

[Receiving summary information](#)

[Receiving a summary of all assets in a CSV file \(MDR Web Console\)](#)

[Receiving incident information as a PDF \(MDR Web Console\)](#)

[Setting up regular report delivery in MDR Web Console](#)

[Receiving notifications](#)

[Setting up notifications in MDR Web Console](#)

[Asset status notifications](#)

[Receiving extended notifications](#)

[Enabling extended notifications in MDR Web Console](#)

[Managing users](#)

[Inviting new users in MDR Web Console](#)

[Changing user roles in MDR Web Console](#)

[Editing user notification methods in MDR Web Console](#)

[Editing user access to tenants in MDR Web Console](#)

[Deleting user accounts](#)

[Managing assets](#)

[Viewing and searching assets in MDR Web Console](#)

[Filtering assets in MDR Web Console](#)

[Viewing detailed information about assets in MDR Web Console](#)

[Asset statuses](#)

[Checking assets status in Kaspersky Security Center](#)

[How to avoid loss of telemetry data from assets](#)

[Managing incidents](#)

[About the incidents](#)

[Viewing and searching incidents in MDR Web Console](#)

[Filtering incidents in MDR Web Console](#)

[Creating custom incidents in MDR Web Console](#)

[Viewing detailed information about incidents in MDR Web Console](#)

[Processing responses to incidents in MDR Web Console](#)

[Response types](#)

[Auto-accepting responses in MDR Web Console](#)

[Auto-accepting responses in Kaspersky Security Center](#)

[Closing incidents in MDR Web Console](#)

[Sending an incident to the Incident Response team for additional investigation](#)

[Kaspersky Unified Monitoring and Analysis integration](#)

[Creating Managed Detection and Response incidents from XDR incidents](#)

[Kaspersky Digital Footprint Intelligence integration for MDR](#)

[Using Kaspersky Endpoint Detection and Response Expert features](#)

[Responses](#)

## [Managing tenants](#)

### [Managing tenants in Kaspersky Security Center](#)

[Viewing tenants in Kaspersky Security Center](#)

[Viewing tenant settings in Kaspersky Security Center](#)

[Editing tenant settings in Kaspersky Security Center](#)

[Adding new tenants in Kaspersky Security Center](#)

[Deleting tenants in Kaspersky Security Center](#)

[Moving assets between tenants](#)

### [Managing tenants in MDR Web Console](#)

[Viewing tenants in MDR Web Console](#)

[Viewing tenant settings in MDR Web Console](#)

[Editing tenant settings in MDR Web Console](#)

[Adding new tenants in MDR Web Console](#)

[Deleting tenants in MDR Web Console](#)

## [Managing the solution through the REST API](#)

[Scenario: performing token-based authorization](#)

[Creating an API connection in Kaspersky Security Center](#)

[Creating an API connection in MDR Web Console](#)

[Editing an API connection in Kaspersky Security Center](#)

[Editing an API connection in MDR Web Console](#)

[Creating an access token in Kaspersky Security Center](#)

[Creating an access token in MDR Web Console](#)

[Working with the REST API](#)

[Revoking a refresh token in Kaspersky Security Center](#)

[Deleting an API connection in Kaspersky Security Center](#)

[Deleting an API connection in MDR Web Console](#)

## [Deactivating Kaspersky Managed Detection and Response](#)

[Terminating the use of Kaspersky Managed Detection and Response](#)

[Suspending the use of Kaspersky Managed Detection and Response temporarily](#)

[Revoking your consent with the terms of using the MDR solution](#)

## [Known issues](#)

### [Contact Technical Support](#)

[How to get technical support](#)

[Technical support via Kaspersky CompanyAccount](#)

## [Sources of information about the solution](#)

### [Glossary](#)

[Asset](#)

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

[EPP application](#)

[Incident](#)

[IOC](#)

[MITRE tactic](#)

[MITRE technique](#)

[Response](#)

[Telemetry](#)

[Tenant](#)

[Information about third-party code](#)

[Trademark notices](#)

# Kaspersky Managed Detection and Response Help

## New features

- [What's new in the latest solution release](#)

## Hardware and software requirements

- [Check which operating systems and EPP applications are supported](#)

## Feature comparison

- [Comparison of commercial license solutions: MDR Optimum, MDR Expert, MDR Basic, MDR Advanced, and MDR Prime](#)

## How to start

- On-premises deployment
- Cloud-based deployment
- [Activation of Kaspersky Managed Detection and Response](#)

## Monitoring and reporting

- [Receiving notifications](#)
- [Receiving extended notifications](#)
- [Receiving summary information](#)
- [Monitoring dashboards](#)



## Data provision / Personal data protection

- [Data provision](#)
- [Kaspersky Security Network](#)

# What's new

Kaspersky Managed Detection and Response presents several new features and enhancements.

## August 2026

MDR Plug-in version 3.1.1 for Open Single Management Platform version 2.2 is released.

## July 2026

- Asset status notifications

MDR now supports [automatic notification delivery when the health of your protected assets requires attention](#). Configure threshold values for OK, Warning, Critical, and Offline asset statuses, and receive email or Telegram notifications when the configured conditions are met. This helps you quickly detect telemetry collection or connectivity issues without continuously monitoring the Assets page.

## June, 2026

- Kaspersky DFI Integration for MDR

Our MDR service now leverages compromised credential intelligence from the Kaspersky DFI service to enhance detection, investigation, and threat hunting workflows. By correlating leaked credentials with security events and incorporating this intelligence into proactive threat hunting activities, MDR can identify potential account compromise earlier, improve incident prioritisation, and help reduce the risk of unauthorised access.

Key capabilities:

- Alert enrichment with leaked credential context
  - Correlation of leaked credentials with security events
  - Credential-based threat hunting and compromise detection
- Updated MDR Application Support Matrix

The Compatible Kaspersky applications and solutions table has been updated. Some legacy product versions have been moved to the Limited MDR Compatibility category (certain MDR capabilities may not be available), while support for the Kaspersky Endpoint Agent has been discontinued.

For details, please refer to the [updated article in Online Help](#).

## May, 2026

- MDR Plug-in version 3.0.2 for Open Single Management Platform version 2.1 is released.
- Users can now leave feedback directly when closing an incident in the MDR Console. This helps improve service quality and capture customer satisfaction more efficiently.
- MDR Administrators can now [define the expected asset limit for each tenant](#) in the MDR Console.

If the number of connected assets exceeds the configured limit, a notification will be displayed both in the tenant list and in the tenant properties page. This helps administrators proactively monitor onboarding scope and licensing expectations.

This functionality will be added to the MDR Plug-in in a later release.

- The format of notifications delivered via email and Telegram has been improved for better readability and faster access to important information.

The update affects notifications related to:

- Incidents
- Comments in communication with MDR analysts
- Response actions
- License key status updates

## March, 2026

Added support for Kaspersky Embedded Systems Security for Linux version 4.0 or later. You can now [activate the MDR solution](#) in Kaspersky Embedded Systems Security for Linux with a Kaspersky MDR license.

## December, 2025

- Added support for the following EPP applications:
  - Kaspersky Embedded Systems Security for Windows version 4.0 or later
  - Kaspersky Industrial CyberSecurity for Nodes Windows version 4.5
- You can now set up [extended Telegram notifications](#) in MDR Plug-in in addition to MDR Web Console.
- You can [send incidents to the Incident Response team for additional investigation](#) using the MDR Web Console interface.

- Added support for the following Kaspersky solutions:
  - Integration with Kaspersky Endpoint Detection and Response version 8.0 or later that enables the following functionality:
    - [The ability to create MDR incidents from XDR incidents.](#)
    - Get artefacts [response type](#).
  - Integration with Kaspersky Anti Targeted Attack version 8.0 or later that adds the Get artefacts [response type](#).

Refer to the following article: [Integration with Kaspersky applications and solutions](#)

## October, 2025

You can now set up [extended Telegram notifications](#) in MDR Web Console.

## July, 2025

- Added the ability to use activation codes to activate the MDR solution in the following applications:
  - Kaspersky Endpoint Security for Linux version 12.3
  - Kaspersky Endpoint Security for Linux version 12.3 in the Light Agent mode
  - Kaspersky Endpoint Security for Windows version 12.6 or later
  - Kaspersky Endpoint Security for Windows version 12.8 or later in the Light Agent mode
  - Kaspersky Endpoint Security for Mac version 12.2

Refer to the following article for details: [Activating the MDR solution in Kaspersky applications.](#)
- The MDR solution can now operate without the KPSN configuration file with the following applications:
  - Kaspersky Endpoint Security for Linux version 12.3
  - Kaspersky Endpoint Security for Linux version 12.3 in the Light Agent mode
  - Kaspersky Endpoint Security for Windows version 12.6 or later
  - Kaspersky Endpoint Security for Windows version 12.8 or later in the Light Agent mode
  - Kaspersky Endpoint Security for Mac version 12.2

Refer to the following article for details: [Switching the MDR solution to operation without KPSN configuration files.](#)

- The MDR solution now supports [Kaspersky Endpoint Security for Windows version 12.8 or later in the Light Agent mode](#).
- The MDR Plug-in version 2.5.1 now supports MDR operation without the KPSN configuration file.
- Kaspersky Endpoint Security for Linux version 12.3 now supports the following response actions:
  - Isolate
  - Disable isolation
  - Quarantine file
  - Restore file from quarantine
  - Terminate process
  - Run process

## May, 2025

- In the [Licensing](#) section of the MDR Plug-in for Kaspersky Security Center:
  - For each MDR license, the name of the client to which the license is issued is now displayed.
  - The matrix of usage of specific licenses in tenants is now available.
- In the [Tenants](#) section of the MDR Plug-in for Kaspersky Security Center:
  - When creating an MDR configuration file for a specific license, the name of the client for whom the license is issued is now displayed.
  - The list of tenants now displays the root tenant, which is created by default after activating the client. You can download configuration files for all current licenses for the root tenant.

## February, 2025

- MDR Web Console now features the **Licensing** section. The following functionality is available:
  - Displaying current, unused and expired MDR licenses.
  - Displaying the total number of assets and their limit for each license.
  - Downloading the MDR configuration file for the root tenant.
 Use the [Tenants section](#) to create and download MDR configuration files for other tenants.

- Entering a new activation code.

If your organization has multiple licenses, you can only manage them in MDR Plug-in for Kaspersky Security Center. The **Licensing** section in MDR Web Console becomes read-only.

- MDR Plug-in for Kaspersky Security Center now supports [applying multiple licenses](#) in your organization. The following functionality is available:
  - Displaying current, unused and expired MDR licenses.
  - Terminating a current MDR license.
  - Entering a new activation code.
  - Downloading the root tenant's MDR configuration file for a license.
  - Choosing a license for an MDR configuration file when creating or editing a tenant in the [Tenants section](#).

## December, 2024

- Simplified activation of Kaspersky Managed Detection and Response on Kaspersky Endpoint Security for Windows devices (starting from version 12.4). All you need is a standard license for Kaspersky MDR solution. Note that you will still need to use the MDR configuration file (BLOB) in any of the following scenarios:
  - You have more than one tenant.
  - You are using the MDR solution together with Kaspersky Endpoint Detection and Response Optimum.
- Added support for managing the MDR solution in the Kaspersky Security Center Linux (starting from version 15.1).
- Added [detailed information about communication channel requirements](#) in the Help.

## October, 2024

MDR Plug-in for Kaspersky Security Center version 2.4.1 is released. It contains the following enhancements:

- The ability to configure automatic acceptance of response actions for selected tenants was added in the MDR Plug-in for Kaspersky Security Center.
- Enhanced functionality and user interface of the [section that provides the list of inactive assets](#). Such assets have been added to Kaspersky Security Center, have the MDR component installed, but never sent telemetry to Kaspersky Managed Detection and Response. You can filter the assets by MDR status, view the detailed information about each asset, and export the asset list to a CSV file.

This feature is working properly in Kaspersky Security Center 15.1 Windows or later versions, Kaspersky Security Center 15.1 Linux or later versions, and Kaspersky Next Expert View.

- [A task for regular delivery of a report on open incidents](#) can now be created only in MDR Web Console. This feature has been removed from the MDR section in Kaspersky Security Center.

## July, 2024

MDR Web Console now allows you to configure automatic acceptance of response actions for the selected tenants.

## June, 2024

- New [response actions](#) are now available:
  - Put file in quarantine
  - Restore file from quarantine
  - Run a script on an asset
- Updated [REST API documentation](#), including new script examples.
- Significantly redesigned [reports](#):
  - MITRE ATT&CK mapping for in-depth threat analysis.
  - List of the most frequently attacked computers to help clients focus on critical risks.

- Multi-tenant support:
  - Generate reports and [configure summary report schedule](#) for specific tenants.
  - Seamlessly switch widgets to tenant-specific statistics in the [monitoring dashboard](#).
  - Configure automatic confirmation of response task execution for specific tenants.
  - Enhanced MDR API for tenant management.

## December, 2023

- MDR Web Console now contains the **Telemetry statistics** dashboard, which shows the number of telemetry events, security events, and incidents.
- Kaspersky Managed Detection and Response now supports Kaspersky Endpoint Security for Windows in Endpoint Detection and Response Agent (EDR Agent) configuration (with the [limitations](#)).

## November, 2023

- Improved display of asset statuses in MDR Web Console and in MDR Plug-in for Kaspersky Security Center: the [asset status](#) now shows the operability of the asset's EPP application components, the asset's anti-virus database update status, and telemetry transmission status.
- Asset status now shows the presence of asset's telemetry losses, allowing you to identify assets with telemetry delivery issues. This feature is enabled by default for new customers and will be gradually enabled for existing customers.

## October, 2023

The client residency region **Saudi Arabia** is added, for clients who store telemetry data in the Kingdom of Saudi Arabia.

## September, 2023

MDR Plug-in for Kaspersky Security Center version 2.3.1 is released. In this version, the incident management functions have been removed from the MDR section in Kaspersky Security Center. You can manage incidents in [MDR Web Console](#).

## July, 2023

MDR Plug-in for Kaspersky Security Center version 2.3.0 is released. It contains the following enhancements:

- You can now set up extended notifications in MDR Plug-in.
- You can now use MDR functions in Kaspersky Security Center with MDR Plug-in through a proxy server.
- You can now change the certificates to use MDR functions in Kaspersky Security Center with a proxy server or anti-virus software.

## July, 2022

MDR Plug-in version 2.1.17 is released. This plug-in version is compatible with Kaspersky Security Center version 14 or later.

## May, 2022

General enhancements:

- The client residency region **USA/Canada** is added, for clients who store their telemetry data in Northern Europe.
- Changed the MDR deployment process description in the help.

Enhancements in MDR Plug-in:

- In the **Settings** section, you can now change the language for notifications in Telegram and email, and for communication in the chat about incidents.
- Improved interface for working with pictures and tables in the incident cards.
- MDR Expert. In the **Service Usage** section you can check how many incidents can be created according to the SLA.

Bug fixes and other improvements:

- Search in the incident and asset lists is now performed by a full occurrence of the searched substring anywhere in the string.
- In Kaspersky Endpoint Security for Mac version 11.2 or later after entering MDR activation code and adding KPSN configuration file, you no longer need to restart your Mac device in order to start a telemetry transfer.
- When calculating licenses for virtual machines with Kaspersky Security for Virtualization Light Agent version 5.2 or later, assets that have not transferred telemetry for more than 24 hours are not included.

March, 2022

[MDR Optimum](#) users now can chat with Kaspersky SOC analysts about an incident (with the following limitation: requests are processed only in relation to a particular incident and no SLA is applied).

October, 2021

- Kaspersky Managed Detection and Response Plug-in for Kaspersky Security Center Web Console and Kaspersky Next Expert View was updated with the enhanced [MDR asset statuses functionality](#):
  - Improved interface of MDR asset statuses.
  - The list of assets displays all the assets of all the statuses, which were previously available only in MDR Web Console.
  - Filtering and sorting options added to work with the list of assets.

July, 2021

- Support of Kaspersky Managed Detection and Response in Kaspersky Next Expert View, which allows managing the solution in the Kaspersky Security Center single administration console. The following features are available with the Kaspersky Managed Detection and Response solution:
  - [Working with incidents](#):
    - Viewing, creating, and commenting incidents
    - Contacting Kaspersky Security Operation Center about an incident, accepting or rejecting responses suggested by SOC analysts
    - [Responding to an incident by using Kaspersky Endpoint Detection and Response](#)

The following responses are available:

- Applying network isolation of devices
- Creating blocking rules by hash
- Creating tasks for deletion, moving to quarantine, ending the process, and searching by indicators of compromise (IOC) related to an incident
- [Monitoring Kaspersky Managed Detection and Response events on dashboards](#) in the monitoring console of Kaspersky Security Center Web Console

- [Configuring notifications](#) about Kaspersky Managed Detection and Response events by email and Telegram
- [Configuring the schedule of the MDR performance summary](#) sent by email
- [Viewing the devices on which there are problems](#) in MDR performance
- [New activation wizard](#), which allows connecting MDR in the Kaspersky Security Center Web Console
- [Automatic KPSN configuration](#), which no longer requires the manual downloading and uploading of a configuration file in the Kaspersky Security Center settings
- [Managing connections to the public MDR API](#): viewing, creating, editing, and deleting tokens
- [Managing the organization tenants, including their creation](#)
- Getting information about the number of incidents available for registration on the user's side, and which are eligible for processing according to the terms of the service level agreement (SLA)

These features are also available in Kaspersky Security Center Web Console.

- Managing several MDR Administrator accounts was added in the MDR Web Console: creating accounts and managing account privileges
- New versions of compatible applications no longer require the additional installation of Kaspersky Endpoint Agent. The built-in Kaspersky Managed Detection and Response functionality is compatible with the following EPP applications:
  - Kaspersky Endpoint Security for Windows 11.6 or later
  - Kaspersky Endpoint Security for Mac 11.2
  - Kaspersky Endpoint Security for Linux 11.2
  - Kaspersky Security for Virtualization 5.2 Light Agent

For details on different deployment scenarios, refer to [Deployment of Kaspersky Managed Detection and Response](#).

- Filtering by event type was added for Kaspersky Endpoint Security for Windows and for Linux with the built-in Kaspersky Managed Detection and Response functionality, which allows decreasing the load on channels and reducing traffic consumption when sending data by telemetry.
- Support of the following response types: [getting file from device, isolating the device, disabling the isolation of the device, deleting registry key](#), terminating process.

Performing these actions is possible with confirmation from the user who has the MDR Administrator role.

- Support of the following new localizations in the web plug-in for Kaspersky Security Center Web Console and Kaspersky Next Expert View: French, German, Italian, and Spanish.

March, 2021

A new web plug-in for Kaspersky Security Center Web Console allows using the following Kaspersky Managed Detection and Response functionality:

- Viewing incidents
- Creating incidents
- Adding comments to the incidents
- Contacting Kaspersky Security Operation Center about an incident
- Accepting or rejecting the responses, suggested by SOC analysts
- Possibility of independent response to an incident:
  - Isolate assets from the network
  - Create blocking rules by hash
  - Create tasks for deleting, moving to quarantine, ending the process, and searching by indicators of compromise (IOC) related to an incident
- Monitoring Kaspersky Managed Detection and Response events on dashboards in the monitoring console of Kaspersky Security Center Web Console
- Configuring email and Telegram notifications about Kaspersky Managed Detection and Response events
- Configuring the schedule of incidents summary sent by email

# About Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response is a solution that automatically detects and analyzes security incidents in your infrastructure by using telemetry and advanced machine learning technologies, and then transfers information about the incident to Kaspersky experts. The experts can then either process the incident themselves or give recommendations on how to process it.

Kaspersky Managed Detection and Response (also referred to as MDR) delivers round-the-clock protection from the growing volume of threats that circumvent automated security barriers to organizations that struggle to find the expertise and staff, or for those with limited in-house resources. The solution helps improve your corporate resilience to cyberthreats, while freeing up your existing resources to focus their attention on other tasks.

Unlike similar offerings on the market, this solution leverages a proven track record of effective targeted attack research to ensure continuous defense against even the most complex threats.

Kaspersky Managed Detection and Response (MDR) solution is not available in the United States or to U.S. persons. The use of MDR solution on the specified territory or by U.S. persons is a violation of [terms of using the MDR solution](#). To avoid violation of terms of using the MDR solution, it is required to [terminate the use of MDR](#) permanently on all assets located on the specified territory or used by U.S. persons. When non-U.S. persons are temporarily in the United States, it is required to [suspend the use of MDR](#) on their assets.

## Operating principle of Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response analyzes telemetry data from the EPP applications and generates security events that can be classified as incidents by the detection technology.

Kaspersky Managed Detection and Response receives data from the EPP applications that support MDR, process data, and then send it via [Kaspersky Security Network](#) streams to Kaspersky Managed Detection and Response. For the list of processed data, refer to [Data provision](#). EPP applications are installed on the assets within the IT infrastructure of your organization (for example, mobile devices, computers, or laptops). An example of an EPP application is Kaspersky Endpoint Security for Windows.

MDR Web Console is used to process incidents. Alternatively, you can integrate Kaspersky Managed Detection and Response with a third-party solution, as described in the [Managing the solution through the REST API](#) article.

The Kaspersky Managed Detection and Response solution may resolve an incident automatically or request a user response to a potential security threat. Refer to the [Response types](#) article for details. To ensure prompt response to potential security threats, the Kaspersky Managed Detection and Response solution may request a clarification from you for a suspicious event. You should process such requests in time.

Detailed incident investigation (such as establishing preceding events, circumstances, and detailed mechanism of the attack) is handled by the Kaspersky Incident Response component that is not included in the Kaspersky Managed Detection and Response and must be purchased separately.

Kaspersky Managed Detection and Response usage involves you processing incidents with support of Kaspersky experts. Refer to the article for more information: [Areas of responsibility](#).

# Areas of responsibility

Kaspersky Managed Detection and Response usage involves users processing incidents with support of the MDR solution. Additionally, Kaspersky Technical Support handles solution-related issues.

The table below shows areas of responsibility for users, the MDR solution and Kaspersky Technical Support.

| Task                                                                                                                                 | The MDR solution    | Kaspersky Technical Support | MDR users           |
|--------------------------------------------------------------------------------------------------------------------------------------|---------------------|-----------------------------|---------------------|
| <a href="#">Activating MDR, deploying MDR, managing assets, setting up notifications, managing users, terminating the use of MDR</a> | –                   | Consult                     | Perform the task    |
| <a href="#">Using MDR Web Console to manage incidents</a>                                                                            | –                   | Consult                     | Perform the task    |
| Detecting, investigating, issuing response recommendations for incidents based on <a href="#">telemetry data</a>                     | Perform the task    | –                           | Receive information |
| Clarifying details during investigation, answering questions from the MDR solution for better response recommendations               | Receive information | –                           | Perform the task    |
| Creating requests to use tools and capabilities of MDR to handle incidents                                                           | Perform the task    | –                           | Receive information |
| Coordinating requests to use tools and capabilities of MDR to handle incidents                                                       | Receive information | –                           | Perform the task    |
| Performing tasks outside functional capabilities of MDR                                                                              | Consult             | –                           | Perform the task    |
| Manually creating an incident (it is important to choose an <a href="#">MDR asset</a> and describe the incident in detail)           | Receive information | –                           | Perform the task    |
| Handling issues with Kaspersky infrastructure components that affect MDR                                                             | Receive information | Consult                     | Perform the task    |
| Managing detection rules                                                                                                             | Perform the task    | –                           | –                   |

## Hardware and software requirements

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

## Required EPP applications and supported configurations

In order to use Kaspersky Managed Detection and Response, at least one of the following EPP applications must be deployed in your infrastructure:

- Laptops, desktops, tablets and servers
  - [Kaspersky Endpoint Security for Windows](#) 
  - [Kaspersky Endpoint Security for Linux](#) 
  - [Kaspersky Endpoint Security for Mac](#) 
- Industrial endpoints
  - [Kaspersky Industrial CyberSecurity for Nodes Windows](#) 
- Virtual systems
  - [Kaspersky Security for Virtualization Light Agent](#) 
- Embedded systems
  - [Kaspersky Embedded Systems Security for Windows](#) 
  - [Kaspersky Embedded Systems Security for Linux](#) 
- Network event monitoring
  - [Kaspersky Anti Targeted Attack Platform](#) 

## Operating systems

Kaspersky Managed Detection and Response is compatible with the same operating systems as the EPP applications listed below. For details, please refer to the *Hardware and software requirements* section in the documentation of compatible EPP applications listed in the table below.

## Compatible Kaspersky applications and solutions

Kaspersky Managed Detection and Response is compatible with the versions of Kaspersky applications listed in the table below.

| Kaspersky application                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Recommended versions and their term of support | Limited MDR compatibility * | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kaspersky Endpoint Security for Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <a href="#">12.10 or later</a>                 | <a href="#">12.6–12.9</a>   | Kaspersky Endpoint Security for Windows version 12.6–12.9 supports activating the MDR solution with an activation code.<br><br>Kaspersky Endpoint Security for Windows version 12.10 or later also supports activating the MDR solution with a key file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Kaspersky Endpoint Security for Windows in the Light Agent mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">12.9 or later</a>                  | <a href="#">12.8</a>        | Kaspersky Endpoint Security for Windows version 12.6–12.9 in the Light Agent mode supports activating the MDR solution with an activation code.<br><br>Kaspersky Endpoint Security for Windows version 12.10 or later in the Light Agent mode also supports activating the MDR solution with a key file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Kaspersky Endpoint Security for Windows in Endpoint Detection and Response Agent (EDR Agent) configuration</b><br><br>Starting with Kaspersky Endpoint Security for Windows version 12.3, the application includes the Endpoint Detection and Response Agent (EDR Agent) configuration. Endpoint Detection and Response Agent is an application that is installed on individual workstations and servers in the IT infrastructure of the organization to support the Kaspersky Managed Detection and Response and Kaspersky Anti Targeted Attack Platform (EDR) solutions. EDR Agent continuously monitors processes running on these computers, open network connections, and files being modified. Protection and control components are not available for EDR Agent.<br><br>EDR Agent is compatible with <a href="#">third-party EPP applications</a> . This lets you use third-party infrastructure security tools alongside Detection and Response by Kaspersky. For more details see <a href="#">Kaspersky Endpoint Security for Windows Online Help</a> . | <a href="#">12.8 or later</a>                  | <a href="#">12.6–12.7</a>   | <ul style="list-style-type: none"> <li>For assets with the Kaspersky Endpoint Security for Windows in the EDR Agent configuration, the <i>Warning</i> and <i>Critical</i> statuses for protection and control components are not displayed.</li> <li>You can not use <a href="#">Kaspersky Endpoint Detection and Response Optimum features</a> for the assets with Kaspersky Endpoint Security for Windows in EDR Agent configuration.</li> <li>The list of third-party EPP applications that are compatible with EDR Agent is provided in the <a href="#">Kaspersky Endpoint Security for Windows online help</a>.</li> </ul> Kaspersky Endpoint Security for Windows version 12.6–12.9 in Endpoint Detection and Response Agent (EDR Agent) configuration supports activating the MDR solution with an activation code.<br><br>Kaspersky Endpoint Security for Windows version 12.10 or later in Endpoint Detection and Response Agent (EDR Agent) configuration also supports activating the MDR solution with a key file. |
| Kaspersky Endpoint Security for Linux                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <a href="#">12.4 or later</a>                  | <a href="#">12.1–12.3</a>   | If you use Kaspersky Endpoint Security for Linux and do not have the Linux Audit Daemon (also referred to as auditd) package installed, system audit events are logged to the dmesg kernel log. We recommend installing the auditd package for the convenience of Kaspersky Endpoint Security for Linux managing log rotation.<br><br>Kaspersky Endpoint Security for Linux version 12.3 or later supports activating the MDR solution with both a key file and an activation code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Kaspersky Endpoint Security for Linux in the Light Agent mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <a href="#">12.4 or later</a>                  | <a href="#">12.1–12.3</a>   | Kaspersky Endpoint Security for Linux version 12.3 or later in the Light Agent mode supports activating the MDR solution with both a key file and an activation code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Kaspersky application                                | Recommended versions and their term of support | Limited MDR compatibility *  | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------|------------------------------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kaspersky Endpoint Security for Mac                  | <a href="#">12.2 or later</a>                  | <a href="#">12–12.1</a>      | Kaspersky Endpoint Security for Mac supports activating the MDR solution with an activation code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Kaspersky Security for Virtualization Light Agent    | <a href="#">6.3 or later</a>                   | <a href="#">5.2–6.2</a>      | Refer to the following article for details: <a href="#">Supported versions of applications in Light Agent mode</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Kaspersky Embedded Systems Security for Windows      | <a href="#">4.0 or later</a>                   | <a href="#">4.0</a>          | Kaspersky Endpoint Security for Windows supports activating the MDR solution with both a key file and an activation code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Kaspersky Embedded Systems Security for Linux        | <a href="#">4.0 or later</a>                   | <a href="#">4.0</a>          | Kaspersky Embedded Systems Security for Linux supports activating the MDR solution with both a key file and an activation code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Kaspersky Industrial CyberSecurity for Nodes Windows | <a href="#">4.5</a>                            | <a href="#">4.5</a>          | <p>Use the MDR Plug-in version 3.0.0 or later to apply multiple activation codes for the Kaspersky Industrial CyberSecurity for Nodes license. You can use the MDR Web Console if you only have a single activation code for the Kaspersky Industrial CyberSecurity for Nodes license.</p> <p>Applying new activation codes for Kaspersky Industrial CyberSecurity for Nodes is not available in the Kingdom of Saudi Arabia <a href="#">region</a>, if you have any of the following licenses:</p> <ul style="list-style-type: none"> <li>• Kaspersky Managed Detection and Response Basic Add-on</li> <li>• Kaspersky Managed Detection and Response Advanced Add-on</li> <li>• Kaspersky Managed Detection and Response Prime Add-on</li> </ul> |
| Kaspersky Endpoint Agent                             | –                                              | <a href="#">4.0 or later</a> | <p>We recommend that you switch to Kaspersky Endpoint Security for Windows.</p> <p>Kaspersky Endpoint Agent is only used if you use Kaspersky Security for Windows Server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

\* MDR integration is available with certain functional limitations (for example, reduced telemetry, or fewer automated response actions).

To learn more about the supported versions of Kaspersky applications and solutions, refer to the [Product Support Lifecycle webpage](#).

Refer to the following article for details about integration with other Kaspersky solutions: [Integration with Kaspersky applications and solutions](#).

## Kaspersky Security Center

The table below lists Kaspersky Security Center components supported by the MDR solution.

| Kaspersky Security Center components      | Versions and their term of support | Notes                                                                     |
|-------------------------------------------|------------------------------------|---------------------------------------------------------------------------|
| Kaspersky Security Center Windows         | <a href="#">15.1 or later</a>      | Used with the <a href="#">MDR Plug-in for Kaspersky Security Center</a> . |
| Kaspersky Security Center Linux           | <a href="#">15.1 or later</a>      | Used with the <a href="#">MDR Plug-in for Kaspersky Security Center</a> . |
| Kaspersky Next Expert View                | Expert view                        |                                                                           |
| MDR Plug-in for Kaspersky Security Center | Latest version                     | Version 2.5.1 is the minimum supported version.                           |

## MDR Web Console

MDR Web Console has the following hardware and software requirements:

- Monitor that supports a display resolution of 1024x768 or higher
- Any of the following browsers:
  - Apple Safari—18.3 or later on macOS
  - Google Chrome—143.0.7499.40 or later (official build)
  - Microsoft Edge—143.0.3650.66 or later
  - Mozilla Firefox Extended Support Release—140.5.0.2342 or later

## Network channel

The following table shows network channel throughput calculated from our statistical data.

| Operating system                      | Estimated bandwidth for 1000 assets |
|---------------------------------------|-------------------------------------|
| Windows                               | 4.3 Mbit/s                          |
| Windows server                        | 5.2 Mbit/s                          |
| Linux (average for hosts and servers) | 14.7 Mbit/s                         |
| macOS                                 | 8.5 Mbit/s                          |

These bandwidth values are approximate, as the necessary bandwidth greatly depends on the type of asset load generating telemetry events. Peak throughput can be significantly higher. You will need to provide an accordingly higher network bandwidth if your infrastructure regularly operates at peak throughput. Various conditions may presume the load to be higher. For example:

- program code compilation by developers
- full system scan
- high-load servers (for example, DNS and domain controllers)
- multiple network connections

## MDR Plug-in versions functionality and compatibility with Kaspersky Security Center and Open Single Management Platform

The following table shows which versions of Kaspersky Security Center and Open Single Management Platform are compatible with versions of the MDR Plug-in.

| MDR Plug-in version | Compatible Kaspersky Security Center version                                                                             | Features added in the MDR Plug-in version                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.5.1               | Kaspersky Security Center Windows version 15.1 or later<br>Kaspersky Security Center Windows Linux version 16.1 or later | Usage of multiple license keys.<br>The ability to generate an MDR configuration (BLOB) file for a specific license key.<br>Automatic response actions configuration for tenants.<br>Configurable tenant-specific reports.                                                                                                                                                                                   |
| 2.5.2               | Kaspersky Security Center Windows version 15.1 or later<br>Kaspersky Security Center Windows Linux version 16.1 or later | Operation without KPSN configuration files.                                                                                                                                                                                                                                                                                                                                                                 |
| 3.0.0               | Kaspersky Security Center Windows version 15.1 or later<br>Kaspersky Security Center Windows Linux version 16.1 or later | Support for the following EPP applications: <ul style="list-style-type: none"> <li>Kaspersky Industrial CyberSecurity for Nodes Windows version 4.5 or later</li> <li>Kaspersky Embedded Systems Security for Windows version 4.0 or later</li> </ul>                                                                                                                                                       |
| 3.1.0               | Kaspersky Security Center Windows version 15.1 or later<br>Kaspersky Security Center Windows Linux version 16.1 or later | Support for the following EPP applications: <ul style="list-style-type: none"> <li>Kaspersky Embedded Systems Security for Linux version 4.0 or later</li> </ul> <p>The ability to specify the asset limit for tenants.</p> <p>Starting with the MDR Plug-in version 3.1.0, notifications can no longer be configured in Kaspersky Security Center. Use the MDR Web Console to configure notifications.</p> |

## MDR Plug-in versions compatibility with Open Single Management Platform

| MDR Plug-in version | Compatible Open Single Management Platform version | Features added in the MDR Plug-in version                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.0.1               | 2.0                                                | Kaspersky Endpoint Detection and Response Expert integration: <ul style="list-style-type: none"> <li>Creating MDR incidents from EDR incidents.</li> <li>The Get artefacts response action that allows you to copy files related to alerts or incidents from Kaspersky EDR to Kaspersky SOC.</li> </ul> Open Single Management Platform version 2.0 support is limited to the MDR Plug-in version 3.0.1.          |
| 3.0.2               | 2.1                                                | MDR integration with Open Single Management Platform version 2.1.                                                                                                                                                                                                                                                                                                                                                 |
| 3.1.0               | 2.1                                                | Support for the following EPP applications: <ul style="list-style-type: none"> <li>Kaspersky Embedded Systems Security for Linux version 4.0 or later</li> </ul> <p>The ability to specify the asset limit for tenants.</p> <p>Starting with the MDR Plug-in version 3.1.0, notifications can no longer be configured in Open Single Management Platform. Use the MDR Web Console to configure notifications.</p> |
| 3.1.1               | 2.2                                                | MDR integration with Open Single Management Platform version 2.2.                                                                                                                                                                                                                                                                                                                                                 |

## Kaspersky Managed Detection and Response components

Description of Kaspersky Managed Detection and Response components:

- [Asset](#) is an organization's device that is protected by Kaspersky solutions.
- Endpoint Protection Platform (EPP) application is a Kaspersky application that protects assets, and the data stored on them, from malware and other threats.

- The Kaspersky Endpoint Agent is a program component that is installed on workstations and servers of the corporate IT infrastructure. Kaspersky Endpoint Agent continuously monitors processes running on those computers, active network connections, and the files that are modified. In recent versions of EPP applications it was replaced by the built-in functionality.
- Kaspersky Network Agent is a Kaspersky Security Center component that enables interaction between the Administration Server and the Kaspersky applications that are installed on a specific network node (workstation or server). This component is common to all of the company's applications for Microsoft Windows. Separate versions of Network Agent exist for Kaspersky applications developed for Unix-like operation systems and for macOS.
- Kaspersky Security Center is an application aimed at corporate network administrators and employees responsible for the protection of assets in a wide range of organizations.
- Kaspersky Security Network is an infrastructure of cloud services that provides access to the Kaspersky online knowledge base, which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.
- Kaspersky Managed Detection and Response (also referred to as MDR) is a solution that delivers continuous managed protection, enabling organizations to hunt down evasive threats automatically, while freeing up IT security teams to focus on critical tasks that require their involvement.
- MDR Web Console provides a web interface for managing and maintaining the protection system of a client organization's network that is managed by Kaspersky Managed Detection and Response. In addition to MDR Web Console, the Kaspersky Security Center web plug-in was added to allow the management of Kaspersky Managed Detection and Response within a single administration console.
- The MDR API is the Application Programming Interface for managing and supporting the network protection system of a client organization managed by Kaspersky Managed Detection and Response.

# Activating and deploying Kaspersky Managed Detection and Response

This section describes how to activate and deploy Kaspersky Managed Detection and Response.

To activate and deploy Kaspersky Managed Detection and Response, you need one of the following solutions for centralized network security management:

- On-premises: [Kaspersky Security Center Web Console](#) <sup>1</sup>, [Open Single Management Platform](#) <sup>2</sup>.
- Cloud-based: [Kaspersky Next Expert View](#) <sup>3</sup>.

Steps for deploying Kaspersky Managed Detection and Response depend on the specific [EPP applications](#) <sup>4</sup> that are installed on your assets and the usage of [multitenancy](#).

Up-to-date versions of applications, a single tenant

[Activate and deploy MDR using only up-to-date applications and a single tenant](#) if the following conditions are met:

- Up-to-date versions of applications are installed on all your assets:
  - Kaspersky Endpoint Security for Windows version 12.10 or later
  - Kaspersky Endpoint Security for Linux version 12.3 or later
  - Kaspersky Endpoint Security for Mac version 12.2 or later
  - Kaspersky Industrial CyberSecurity for Nodes Windows version 4.5 or later
  - Kaspersky Embedded Systems Security for Windows version 4.0 or later
  - Kaspersky Embedded Systems Security for Linux version 4.0 or later
- You do not plan to configure multitenancy immediately after the deployment.  
You can configure multitenancy later.
- You have any of the following licenses:
  - Kaspersky Next Complete Security
  - Kaspersky Optimum Security
  - Kaspersky Symphony MDR
  - Kaspersky Next MXDR Optimum

- Kaspersky MDR
- Kaspersky Managed Detection and Response

## Up-to-date versions of applications, multitenancy

[Activate and deploy MDR using only up-to-date applications and multitenancy](#) if the following conditions are met:

- Up-to-date versions of applications are installed on all your assets:
  - Kaspersky Endpoint Security for Windows version 12.10 or later
  - Kaspersky Endpoint Security for Linux version 12.3 or later
  - Kaspersky Endpoint Security for Mac version 12.2 or later
  - Kaspersky Industrial CyberSecurity for Nodes Windows version 4.5 or later
- You plan to configure multitenancy immediately after the deployment.
- You have any of the following licenses:
  - 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

## Legacy versions of applications

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

Activate and deploy MDR if your infrastructure includes assets with legacy versions of applications:

- Kaspersky Endpoint Security for Windows version 12.9 and earlier
- Kaspersky Endpoint Security for Linux version 12.2 and earlier
- Kaspersky Endpoint Security for Mac version 12.1 and earlier
- Kaspersky Security for Virtualization Light Agent version 5.2
- Kaspersky Security for Windows Server with Kaspersky Endpoint Agent for Windows

## Components required for MDR operation

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

The table below lists components that are required for sending telemetry from the assets. If any of these components are disabled or missing, Kaspersky Managed Detection and Response stops sending telemetry from the asset.

The Light Agent mode is supported for the following versions:

- Kaspersky Endpoint Security for Windows version 12.8 or later
- Kaspersky Endpoint Security for Linux version 12.1 or later

| Component              | Documentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Behavior Detection     | <a href="#">Kaspersky Endpoint Security for Windows</a> <br><a href="#">Kaspersky Endpoint Security for Linux</a> <br><a href="#">Kaspersky Embedded Systems Security for Windows</a> <br><a href="#">Kaspersky Embedded Systems Security for Linux</a> <br><a href="#">Kaspersky Industrial CyberSecurity for Nodes</a>                                                                                                                                                                                                                                                                                                      |
| File Threat Protection | <a href="#">Kaspersky Endpoint Security for Windows</a> <br><a href="#">Kaspersky Endpoint Security for Linux</a> <br><a href="#">Kaspersky Endpoint Security for Mac</a> <br><a href="#">Kaspersky Security for Virtualization Light Agent</a> <br><a href="#">Kaspersky Embedded Systems Security for Windows</a> <br><a href="#">Kaspersky Embedded Systems Security for Linux</a> <br><a href="#">Kaspersky Industrial CyberSecurity for Nodes</a>  |
| System Watcher         | <a href="#">Kaspersky Security for Virtualization Light Agent</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

The table below lists components that affect the fullness of sent telemetry.

| Component | Documentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall  | <a href="#">Kaspersky Endpoint Security for Windows</a> <br><a href="#">Kaspersky Security for Virtualization Light Agent</a> <br><a href="#">Kaspersky Embedded Systems Security for Windows</a> <br><a href="#">Kaspersky Industrial CyberSecurity for Nodes</a>  |

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Threat Protection | <a href="#">Kaspersky Endpoint Security for Windows</a> <br><a href="#">Kaspersky Endpoint Security for Linux</a> <br><a href="#">Kaspersky Endpoint Security for Mac</a> <br><a href="#">Kaspersky Embedded Systems Security for Windows</a> <br><a href="#">Kaspersky Embedded Systems Security for Linux</a> <br><a href="#">Kaspersky Industrial CyberSecurity for Nodes</a>  |
| Mail Threat Protection    | <a href="#">Kaspersky Endpoint Security for Windows</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Web Threat Protection     | <a href="#">Kaspersky Endpoint Security for Windows</a> <br><a href="#">Kaspersky Endpoint Security for Linux</a> <br><a href="#">Kaspersky Endpoint Security for Mac</a> <br><a href="#">Kaspersky Embedded Systems Security for Linux</a> <br><a href="#">Kaspersky Security for Virtualization Light Agent</a>                                                                                                                                                 |
| Self Defense              | <a href="#">Kaspersky Endpoint Security for Windows</a> <br><a href="#">Kaspersky Security for Virtualization Light Agent</a> <br><a href="#">Kaspersky Embedded Systems Security for Windows</a> <br><a href="#">Kaspersky Industrial CyberSecurity for Nodes</a>                                                                                                                                                                                                                                                                                 |

## Integration with Kaspersky applications and solutions

The table below describes how to configure integration of Kaspersky Managed Detection and Response with other Kaspersky solutions and applications.

| Solution or application                                                                                                                                                                                                                                                                                                                                                | Version                                                                                             | Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kaspersky Endpoint Security for Windows<br>Kaspersky Endpoint Security for Linux<br>Kaspersky Endpoint Security for Mac<br>Kaspersky Security for Virtualization Light Agent<br>Kaspersky Industrial CyberSecurity for Nodes Windows<br>Kaspersky Embedded Systems Security Windows<br>Kaspersky Security for Windows Server with Kaspersky Endpoint Agent for Windows |                                                                                                     | Refer to the following article: <a href="#">Activating the MDR solution in Kaspersky applications</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Kaspersky Endpoint Detection and Response Expert (on-premise)                                                                                                                                                                                                                                                                                                          | 8.0 or later integrated in the Open Single Management Platform with Kaspersky Next XDR 2.1 or later | Requires active license keys for Kaspersky MDR Expert and Kaspersky EDR Expert.<br><br>The MDR Administrator role is required to configure the integration. <ol style="list-style-type: none"> <li>1. <a href="#">Configure the MDR Plug-in</a> in the Open Single Management Platform Console.</li> <li>2. In the MDR section of the OSMP Console interface, click the <b>MDR Usage</b> tab.</li> <li>3. Expand the <b>KPSN configuration file for integration with KEDR Expert</b> block.</li> <li>4. Enable the <b>Accept KPSN Agreement</b> option and click <b>Apply the KPSN configuration file for integration with KEDR Expert</b>.<br/>The MDR solution now receives telemetry that includes KEDR alerts for analysis.</li> </ol> |

| Solution or application                            | Version      | Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kaspersky Unified Monitoring and Analysis Platform | 4.0 or later | Refer to the following article: <a href="#">Kaspersky Managed Detection and Response integration</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Kaspersky Anti Targeted Attack (KATA) Platform     | 7.0–7.1      | <ol style="list-style-type: none"> <li>1. <a href="#">Download the MDR configuration file</a>.</li> <li>2. <a href="#">Enable MDR integration</a>.</li> </ol> <p>Not available in the following <a href="#">region</a>: Kingdom of Saudi Arabia.</p>                                                                                                                                                                                                                                                                                                   |
|                                                    | 8.0 or later | <p>Ensure network access of the server on which integration setup with the MDR solution is performed to the following addresses:</p> <ul style="list-style-type: none"> <li>• *uis.kaspersky.com:443</li> <li>• mdr.kaspersky.com:443</li> </ul> <p>Ensure network access of secondary KATA servers to mdr.kaspersky.com:443.</p> <p>Refer to the following article: <a href="#">Configuring integration with Kaspersky Managed Detection and Response</a>.</p> <p>Not available in the following <a href="#">region</a>: Kingdom of Saudi Arabia.</p> |

## Configuring MDR Plug-in

To manage Kaspersky Managed Detection and Response via MDR Plug-in functionality, you need to install MDR Plug-in in the solution for centralized network security management that you use:

- Kaspersky Security Center Web Console
- Kaspersky Next Expert View  
The MDR Plug-in is pre-installed in Kaspersky Next Expert View.
- Open Single Management Platform

### Prerequisites

Make sure you have access to Kaspersky Security Center Web Console, Kaspersky Next Expert View or Open Single Management Platform, with the following minimum access rights:

- **Read** access right for the [General features: Application integration](#)  functional area
- **Allow** access right for the [Incident access](#) functional area of Kaspersky Managed Detection and Response

## Installing MDR Plug-in in Kaspersky Security Center Web Console

*To install MDR Plug-in in Kaspersky Security Center Web Console:*

1. In the main menu of Kaspersky Security Center Web Console, go to **Settings** → **Web plug-ins**.
2. In the window that opens, click the **Add** button.  
The list of available plug-ins is displayed.
3. In the list of available plug-ins, select the MDR Plug-in.  
The plug-in description page is displayed.
4. On the plug-in description page, click **Install plug-in**.
5. When the installation is complete, click **OK**.

The MDR Plug-in is downloaded with the default configuration and displayed in the list of management web plug-ins.

## Installing MDR Plug-in in Open Single Management Platform

If the Open Single Management Platform operates in a closed network environment, you need to specify proxy settings. Run the following command on the Open Single Management Platform host to add environment variables with proxy settings:

```
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
```

Run the following command to ensure that environment variables have been configured:

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

*To install MDR Plug-in in OSMP:*

1. Move the management web plug-in archive to the administrator host on which the KDT utility is located.
2. On the administrator host with the KDT utility, run the following command to install the plug-in:

```
./kdt apply -k <path to the plug-in archive>
```

3. Reload the OSMP Console interface to display the added plug-in.

The MDR management web plug-in is installed, and you can access MDR functions in the OSMP Console.

You can use the KDT utility to view the list of installed web plug-ins and ensure that the MDR management web plug-in has been successfully installed.

*To view the list of management web plug-ins and other components related to OSMP,*

On the administrator host on which the KDT utility is located, run the following command:

```
./kdt state
```

The list of components integrated in OSMP is displayed in the command line window. You can check the list to ensure that the MDR management web plug-in has been installed.

## Results

Upon completion of this scenario, MDR Plug-in is set up to work with Kaspersky Managed Detection and Response.

# Activating and deploying MDR when using up-to-date application versions and a single tenant

The following instruction for activating and deploying the MDR solution is suitable if the following conditions are met:

- Up-to-date versions of applications are installed on all your assets:
  - Kaspersky Endpoint Security for Windows version 12.10 or later
  - Kaspersky Endpoint Security for Linux version 12.3 or later
  - Kaspersky Endpoint Security for Mac version 12.2 or later
  - Kaspersky Industrial CyberSecurity for Nodes Windows version 4.5 or later
  - Kaspersky Embedded Systems Security for Windows version 4.0 or later
  - Kaspersky Embedded Systems Security for Linux version 4.0 or later
- You do not plan to use [multitenancy](#) immediately after the deployment.  
You will be able to configure multitenancy later by adding MDR configuration (BLOB) files to applications.
- You own any of the following licenses:
  - Kaspersky Next Complete Security
  - Kaspersky Optimum Security
  - Kaspersky Symphony MDR
  - Kaspersky Next MDR Optimum

- Kaspersky MDR
- Kaspersky Managed Detection and Response

## Prerequisites

Ensure that your IT infrastructure meets the [hardware and software requirements of Kaspersky Managed Detection and Response](#).

## Activation and deployment

Follow these steps to activate and deploy the MDR solution:

### Step 1. Authenticating in the MDR Web Console

Perform the following steps:

1. Go to the [MDR Web Console](#).
2. Click **Create Account**. Create a new user account.
3. In the [MDR Web Console](#), log in under the created user account.
4. When prompted, enter the activation code sent to the email address that you specified when creating the user account.
5. Select the region of data processing in accordance to the location of license use.
6. When prompted, accept the agreements and confirm the MDR activation.

### Step 2. Activating the MDR solution on your assets

If you use the MDR solution under any of the following licenses, the MDR solution is automatically activated on your assets, so you can skip this step and proceed to the stage 3:

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

Activate the MDR license on your assets:

## Activation in Kaspersky Security Center Web Console

1. In the main menu, go to **Operations** → **Kaspersky licenses**.

2. Click the **Add** button.

3. Add the key file or apply the activation code:

- **Add key file**

Click the **Select key file** button and browse the .key file that you want to add.

- **Enter activation code**

Enter the activation code and click the **Send** button.

4. Click the **Close** button.

5. On the **Kaspersky licenses** page, click the name of the current license.

The license properties are open.

6. On the **General** tab, enable the **Automatically distribute license key to managed devices** parameter.

7. Click **Save**.

The license key is automatically distributed to assets. If you want to distribute a license key to client devices through the license key distribution task, refer to [the Kaspersky Security Center Online Help](#).

## Activation in Open Single Management Platform

1. In the main menu, click the Administration Server name.

The Administration Server properties window opens.

2. On the **General** tab, select the **License keys** section.

3. Click **Add new license key** and specify a new license key.

4. Click **Save**.

5. On the **License keys** page, click the name of the added license key.

The license key properties are open.

6. On the **General** tab, enable the **Automatically distribute license key to managed devices** parameter.

7. Click **Save**.

The license key is automatically distributed to assets.

The following article describes how to view license keys and activation codes in use in the Administration Server: [Viewing information about license keys and activation codes in use](#).

### Step 3. Enabling KSN usage

In Kaspersky Security Center Web Console, Kaspersky Next Expert View or Open Single Management Platform, go to the **Asset management** → **Policies & profiles** section. Enable KSN usage in politics for all applications used on your assets:

#### Kaspersky Endpoint Security for Windows/Linux

1. Select the application policy. If the application policy has not been created, click **Add** and create the policy.
2. In the application policy settings, go to **Application Settings** → **General Settings** → **Kaspersky Security Network**.
3. Enable the **Use of Kaspersky Security Network** parameter.
4. Enable the **Use extended KSN mode** parameter.
5. If you want to use the Administration Server as proxy, enable the following parameters:
  - **Use Administration Server as a KSN proxy server** to send asset telemetry via KSN proxy.
  - **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** to send asset telemetry via KSN when KSN proxy is not available.
6. Click **Save and Close**.

Client devices can send requests to KSN, obtain information from KSN, and transfer information to KSN even if they do not have direct access to the internet. The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

#### Kaspersky Endpoint Security for Mac

1. Select the application policy. If the application policy has not been created, click **Add** and create the policy.
2. In the application policy settings, go to **Application Settings** → **Advanced Threat Protection** → **Kaspersky Security Network**.
3. Enable the **Kaspersky Security Network** parameter.
4. Enable the **Extended KSN mode** parameter.
5. If you want to use the Administration Server as proxy, enable the following parameters:
  - **Use Administration Server as a KSN proxy server** to send asset telemetry via KSN proxy.
  - **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** to send asset telemetry via KSN when KSN proxy is not available.
6. Click **Save and Close**.

Client devices can send requests to KSN, obtain information from KSN, and transfer information to KSN even if they do not have direct access to the internet. The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

## Step 4. Configuring network settings on your assets

For assets with internet access, allow outgoing non-SSL traffic and disable traffic inspection through ports 443 and 1443 to the following addresses:

\*.ksn.kaspersky-labs.com

ksn-\*.kaspersky-labs.com

ds.kaspersky.com

For assets with no internet access, configure KSN Proxy to access KSN servers. Allow outgoing non-SSL traffic and disable traffic inspection for the following variants:

- Traffic from the asset to KSN Proxy through port 13111 ([default port](#) )
- Traffic from KSN Proxy through ports 443 and 1443 to the following addresses:

\*.ksn.kaspersky-labs.com

ksn-\*.kaspersky-labs.com

ds.kaspersky.com

We recommend configuring direct connection between assets and KSN servers. This approach helps to prevent telemetry losses if the KSN Proxy is unavailable, or for laptop assets that use remote connection.

The MDR solution has been activated and deployed. Assets that are managed by MDR are displayed in MDR Web Console after synchronization (up to 24 hours): [mdr.kaspersky.com/assets](https://mdr.kaspersky.com/assets).

You can now proceed to configuring of the MDR solution:

- [Invite new users in MDR Web Console](#).
- [Configure regular notifications](#).
- [Enable extended notifications](#).

## Activating and deploying MDR when using up-to-date application versions and multitenancy

The following instruction for activating and deploying the MDR solution is suitable if the following conditions are met:

- Up-to-date versions of applications are installed on all your assets:
  - Kaspersky Endpoint Security for Windows version 12.10 or later
  - Kaspersky Endpoint Security for Linux version 12.3 or later

- Kaspersky Endpoint Security for Mac version 12.2 or later
- Kaspersky Industrial CyberSecurity for Nodes Windows version 4.5 or later
- Kaspersky Embedded Systems Security for Windows version 4.0 or later (can only be assigned to the root tenant)
- Kaspersky Embedded Systems Security for Linux version 4.0 or later (can only be assigned to the root tenant)
- You plan to use [multitenancy](#) immediately after the deployment.
- You own any of the following licenses:
  - 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

## Prerequisites

Ensure that your IT infrastructure meets the [hardware and software requirements of Kaspersky Managed Detection and Response](#).

## Activation and deployment

Follow these steps to activate and deploy the MDR solution:

## Step 1. Authenticating in the MDR Web Console

Perform the following steps:

1. Go to the [MDR Web Console](#).
2. Click **Create Account**. Create a new user account.
3. In the [MDR Web Console](#), log in under the created user account.
4. When prompted, enter the activation code sent to the email address that you specified when creating the user account.
5. Select the region of data processing in accordance to the location of license use.
6. When prompted, accept the agreements and confirm the MDR activation.

## Step 2. Creating tenants and downloading configuration files

Follow the instructions below:

1. [Create new tenants in the MDR Web Console](#).
2. For each of the created tenants, [download the MDR configuration file and add the BLOB \(P7\) file to application policies](#).

## Step 3. Activating the MDR solution on your assets

If you use the MDR solution under any of the following licenses, the MDR solution is automatically activated on your assets, so you can skip this step and proceed to the step 4:

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

Activate the MDR license on your assets:

### Activation in Kaspersky Security Center Web Console

1. In the main menu, go to **Operations** → **Kaspersky licenses**.
2. Click the **Add** button.

3. Add the key file or apply the activation code:

- **Add key file**

Click the **Select key file** button and browse the .key file that you want to add.

- **Enter activation code**

Enter the activation code and click the **Send** button.

4. Click the **Close** button.

5. On the **Kaspersky licenses** page, click the name of the current license.

The license properties are open.

6. On the **General** tab, enable the **Automatically distribute license key to managed devices** parameter.

7. Click **Save**.

The license key is automatically distributed to assets. If you want to distribute a license key to client devices through the license key distribution task, refer to [the Kaspersky Security Center Online Help](#).

## Activation in Open Single Management Platform

1. In the main menu, click the Administration Server name.

The Administration Server properties window opens.

2. On the **General** tab, select the **License keys** section.

3. Click **Add new license key** and specify a new license key.

4. Click **Save**.

5. On the **License keys** page, click the name of the added license key.

The license key properties are open.

6. On the **General** tab, enable the **Automatically distribute license key to managed devices** parameter.

7. Click **Save**.

The license key is automatically distributed to assets.

The following article describes how to view license keys and activation codes in use in the Administration Server: [Viewing information about license keys and activation codes in use](#).

## Step 4. Enabling KSN usage

In Kaspersky Security Center Web Console, Kaspersky Next Expert View or Open Single Management Platform, go to the **Asset management** → **Policies & profiles** section. Enable KSN usage in politics for all applications used on your assets:

## Kaspersky Endpoint Security for Windows/Linux

1. Select the application policy. If the application policy has not been created, click **Add** and create the policy.
2. In the application policy settings, go to **Application Settings** → **General Settings** → **Kaspersky Security Network**.
3. Enable the **Use of Kaspersky Security Network** parameter.
4. Enable the **Use extended KSN mode** parameter.
5. If you want to use the Administration Server as proxy, enable the following parameters:
  - **Use Administration Server as a KSN proxy server** to send asset telemetry via KSN proxy.
  - **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** to send asset telemetry via KSN when KSN proxy is not available.
6. Click **Save and Close**.

Client devices can send requests to KSN, obtain information from KSN, and transfer information to KSN even if they do not have direct access to the internet. The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

## Kaspersky Endpoint Security for Mac

1. Select the application policy. If the application policy has not been created, click **Add** and create the policy.
2. In the application policy settings, go to **Application Settings** → **Advanced Threat Protection** → **Kaspersky Security Network**.
3. Enable the **Kaspersky Security Network** parameter.
4. Enable the **Extended KSN mode** parameter.
5. If you want to use the Administration Server as proxy, enable the following parameters:
  - **Use Administration Server as a KSN proxy server** to send asset telemetry via KSN proxy.
  - **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** to send asset telemetry via KSN when KSN proxy is not available.
6. Click **Save and Close**.

Client devices can send requests to KSN, obtain information from KSN, and transfer information to KSN even if they do not have direct access to the internet. The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

## Step 5. Configuring network settings on your assets

For assets with internet access, allow outgoing non-SSL traffic and disable traffic inspection through ports 443 and 1443 to the following addresses:

\*.ksn.kaspersky-labs.com

ksn-\*.kaspersky-labs.com

ds.kaspersky.com

For assets with no internet access, configure KSN Proxy to access KSN servers. Allow outgoing non-SSL traffic and disable traffic inspection for the following variants:

- Traffic from the asset to KSN Proxy through port 13111 ([default port](#) )
- Traffic from KSN Proxy through ports 443 and 1443 to the following addresses:

\*.ksn.kaspersky-labs.com

ksn-\*.kaspersky-labs.com

ds.kaspersky.com

We recommend configuring direct connection between assets and KSN servers. This approach helps to prevent telemetry losses if the KSN Proxy is unavailable, or for laptop assets that use remote connection.

The MDR solution has been activated and deployed. Assets that are managed by MDR are displayed in MDR Console after synchronization (up to 24 hours): [mdr.kaspersky.com/assets](https://mdr.kaspersky.com/assets).

You can now proceed to configuring of the MDR solution:

- [Invite new users in MDR Console](#).
- [Configure regular notifications](#).
- [Enable extended notifications](#).

## Activating and deploying MDR when using legacy application versions

Use the following instruction if your infrastructure includes assets with legacy versions of applications:

- Kaspersky Endpoint Security for Windows version 12.9 and earlier
- Kaspersky Endpoint Security for Linux version 12.2 and earlier
- Kaspersky Endpoint Security for Mac version 12.1 and earlier
- Kaspersky Security for Virtualization Light Agent version 5.2
- Kaspersky Security for Windows Server with Kaspersky Endpoint Agent for Windows

## Prerequisites

Ensure that your IT infrastructure meets the [hardware and software requirements of Kaspersky Managed Detection and Response](#).

## Activation and deployment

Activation and deployment of the MDR solution proceeds in stages:

### Step 1. Authenticating in the MDR Web Console

Perform the following steps:

1. Go to the [MDR Web Console](#).
2. Click **Create Account**. Create a new user account.
3. In the [MDR Web Console](#), log in under the created user account.
4. When prompted, enter the activation code sent to the email address that you specified when creating the user account.
5. Select the region of data processing in accordance to the location of license use.
6. When prompted, accept the agreements and confirm the MDR activation.

### Step 2. Creating tenants and downloading configuration files

Follow the instructions below:

1. If you need multitenancy, [create new tenants in MDR Console](#).
2. For each of the created tenants, [download the MDR configuration file and add the BLOB \(P7\) file to application policies](#).

### Step 3. Configuring KPSN

[Deploy the KPSN configuration file](#).

## Step 4. Enabling KSN usage

In Kaspersky Security Center Web Console, Kaspersky Next Expert View or Open Single Management Platform, go to the **Asset management** → **Policies & profiles** section. Enable KSN usage in politics for all applications used on your assets:

1. Select the application policy. If the application policy has not been created, click **Add** and create the policy.
2. In the application policy settings, go to **Application Settings** → **Advanced Threat Protection** → **Kaspersky Security Network**.
3. Enable the **Kaspersky Security Network** parameter.
4. Enable the **Extended KSN mode** parameter.
5. (Optional) If the Administration Server is used as proxy, enable the following parameters:
  - Enable **Use Administration Server as a KSN proxy server** to send asset telemetry via KSN proxy.
  - Enable **Use Kaspersky Security Network servers if the KSN proxy server is unavailable**.
6. Click **Save and Close**.

Client devices can send requests to KSN, obtain information from KSN, and transfer information to KSN even if they do not have direct access to the internet. The KSN proxy server caches processed data, thus reducing the load on the outbound channel and the time period spent for waiting for information requested by a client device.

## Step 5. Configuring network settings on your assets

For assets with internet access, allow outgoing non-SSL traffic and disable traffic inspection through ports 443 and 1443 to the following addresses:

\*.ksn.kaspersky-labs.com

ksn-\*.kaspersky-labs.com

ds.kaspersky.com

For assets with no internet access, configure KSN Proxy to access KSN servers. Allow outgoing non-SSL traffic and disable traffic inspection for the following variants:

- Traffic from the asset to KSN Proxy through port 13111 ([default port](#) <sup>↗</sup>).
- Traffic from KSN Proxy through ports 443 and 1443 to the following addresses:

\*.ksn.kaspersky-labs.com

ksn-\*.kaspersky-labs.com

ds.kaspersky.com

We recommend configuring direct connection between assets and KSN servers. This approach helps to prevent telemetry losses if the KSN Proxy is unavailable, or for laptop assets that use remote connection.

The MDR solution has been activated and deployed. Assets that are managed by MDR will be displayed in MDR Console after synchronization (up to 24 hours): [mdr.kaspersky.com/assets](https://mdr.kaspersky.com/assets).

You can now proceed to configuring of the MDR solution:

- [Invite new users in MDR Console.](#)
- [Configure regular notifications.](#)
- [Enable extended notifications.](#)

## Deploying a KPSN configuration file

You need to deploy a KPSN configuration file if at least one asset in your infrastructure has a legacy application version installed:

- Kaspersky Endpoint Security for Windows 12.9 and earlier
- Kaspersky Endpoint Security for Linux version 12.2 and earlier
- Kaspersky Endpoint Security for Mac version 12.1 and earlier
- Kaspersky Security for Virtualization Light Agent version 5.2
- Kaspersky Security for Windows Server with Kaspersky Endpoint Agent for Windows

Deploying a KPSN configuration file proceeds in two stages.

### Stage 1. Downloading the MDR configuration file

The instruction for downloading the MDR configuration file depends on whether you have created additional tenants and installed the MDR Plug-in for Kaspersky Security Center.

The MDR configuration file is a ZIP archive containing a KPSN configuration file (.pkcs7) for deployment of EPP applications.

*To download the MDR configuration file in MDR Web Console:*

1. In MDR Web Console, navigate to the **Settings** menu item.
2. Open the **Tenants** tab.

3. Click the line with the tenant for which you want to download the MDR configuration file.

The **Tenant settings** block appears.

4. Click the archive file name to download the archive.

*To download the MDR configuration file in Kaspersky Security Center console:*

1. In the MDR section of Kaspersky Security Center Web Console or Kaspersky Next Expert View, click **Licensing**.

2. Locate the **Archive for asset configuration** column and click **Download** to download the archive.

## Stage 2. Deploying the KPSN configuration file

You can deploy the KPSN configuration file in Kaspersky Security Center Web Console. If you have installed the [MDR Plug-in](#), you can also deploy the KPSN configuration file in the MDR Plug-in menu.

Unpack the MDR configuration file and install the KPSN configuration file (.pkcs7).

*To install the KPSN configuration file in Kaspersky Security Center Web Console:*

1. Move to the properties of the Administration Server by clicking its name in the main menu.

2. On the **General** tab, select the **KSN Proxy settings** section.

3. Enable the **Enable KSN Proxy on Administration Server** parameter.

4. Enable the **Use Kaspersky Private Security Network** parameter.

5. Click **Select file with KSN Proxy settings** and upload the KPSN configuration file (.pkcs7).

The KPSN configuration file details are displayed.

6. Click **Save**.

The KPSN configuration file is installed.

*To install the KPSN configuration file in MDR Plug-in menu of Kaspersky Security Center Web Console or Open Single Management Platform:*

1. In the main menu, open the **MDR** section.

2. Open the **MDR Usage** tab.

3. Expand the **KPSN configuration file for integration with the KSC Administration Server** block.

4. Enable the **Accept KPSN Agreement** parameter and click **Apply the KPSN configuration file on Administration Server**.

The KPSN configuration file is installed.

# Deploying an MDR configuration (BLOB) file

You can use MDR configuration (BLOB) files to activate the MDR solution in applications that support integration with MDR via Kaspersky Security Center policies.

If you use tenants other than the root tenant, you need to download MDR configuration files for each tenant.

Legacy application versions require usage of MDR configuration (BLOB) files:

- Kaspersky Endpoint Security for Windows 12.6 and earlier
- Kaspersky Endpoint Security for Linux version 12.2 and earlier
- Kaspersky Endpoint Security for Mac version 12.1 and earlier
- Kaspersky Security for Virtualization Light Agent version 5.2
- Kaspersky Security for Windows Server with Kaspersky Endpoint Agent for Windows

Activation of the MDR solution via the MDR configuration (BLOB) file proceeds in two stages.

## Stage 1. Downloading the MDR configuration file

The instruction for downloading the MDR configuration file depends on whether you have created additional tenants and installed the MDR Plug-in for Kaspersky Security Center.

The MDR configuration file is a ZIP archive containing a BLOB (P7) file for deployment of EPP applications.

*To download the MDR configuration file in MDR Web Console:*

1. In MDR Web Console, navigate to the **Settings** menu item.
2. Click the **Tenants** tab.
3. Click the line with the tenant for which you want to download the MDR configuration file.  
The **Tenant settings** block appears.
4. Click the archive file name to download the archive.

*To download the MDR configuration file in Kaspersky Security Center console:*

1. In the MDR section of Kaspersky Security Center Web Console or Kaspersky Next Expert View, click **Licensing**.
2. Locate the **Archive for asset configuration** column and click **Download** to download the archive.

## Stage 2. Adding the MDR configuration (BLOB) file to application policies

Unpack the MDR configuration file and use the BLOB (P7) file to activate the MDR solution.

*To activate the MDR solution in the following applications:*

- Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Mac
1. In Kaspersky Security Center Web Console or Open Single Management Platform, go to the **Asset management** → **Policies & profiles** section.
  2. Select the application policy. If the application policy has not been created, click **Add** and create the policy.
  3. Select the **Application settings** tab.
  4. Go to **Built-in Agents** → **Managed Detection and Response**.
  5. Enable the Managed Detection and Response parameter.
  6. Click **Upload** and select the BLOB (P7) file that you extracted from the MDR configuration file.
  7. Close the lock button icon (🔒) to enforce settings.
  8. Click **Save and Close**.

The MDR configuration (BLOB) file is uploaded and automatically deployed to applications.

*To activate the MDR solution in Kaspersky Industrial CyberSecurity for Nodes Windows:*

1. In Kaspersky Security Center Web Console or Open Single Management Platform, go to the **Asset management** → **Policies & profiles** section.
2. Select the Kaspersky Industrial CyberSecurity for Nodes Windows policy. If the application policy has not been created, click **Add** and create the policy.
3. Select the **Application settings** tab.
4. Go to **Telemetry Connection Servers**.
5. In the **Managed Detection and Response** section, click **Configure**.
6. Enable the **Managed Detection and Response** parameter.
7. Click **Upload** and select the BLOB (P7) file that you extracted from the MDR configuration file.
8. Click **Save and Close**.

The MDR configuration (BLOB) file is uploaded and automatically deployed to applications.

# Deployment by capturing and copying the image of a device

If you need to install applications on assets on which an operating system and other software also must be installed (or reinstalled), you can use the mechanism of capturing and copying the image of a reference asset.

Deployment by capturing and copying the image of a device is performed in two steps:

1. Prepare a reference asset that has the necessary software installed.
2. Capture the image of the prepared reference asset and distribute the image to assets through the dedicated task of Kaspersky Security Center.

If your Kaspersky Security Center license provides the Systems management feature, you can [use the Kaspersky Security Center functionality to capture and distribute the image to assets](#)<sup>[2]</sup>. Otherwise, use third-party tools available in the organization.

## Preparing a reference asset

*To prepare a Windows-based reference asset:*

1. Install and configure operating system and other software that you need to distribute.
2. On the reference asset, in the Windows Network Connections settings, disconnect the reference asset from the network where Kaspersky Security Center is installed.
3. On the reference asset, start the local installation of Network Agent by using the setup.exe file.

The Kaspersky Security Center Network Agent setup wizard starts. Follow the instructions of the wizard.

4. On the Administration Server page of the wizard, specify the Administration Server IP address.

If you do not know the exact address of the Administration Server, enter localhost. You can change the IP address later by [using the klmover utility](#)<sup>[2]</sup> with the -address key.

5. On the Start application page of the wizard, disable the Start application during installation option.
6. When the Network Agent installation is complete, do not restart the asset before creating an operating system image.

If you restart the asset, you will have to repeat the whole process of preparing a reference asset for creation of an operating system image.

7. On the reference asset, in the command line, start the sysprep utility and execute the following command:  
sysprep.exe /generalize /oobe /shutdown.

The reference asset is ready for creating an operating system image.

To prepare a Linux-based reference asset:

1. Install and configure operating system and other software that you need to distribute.
2. Ensure that the following conditions have been met:
  - The reference asset does not have Kaspersky Endpoint Security for Linux installed.
  - The reference device has not been connected to Kaspersky Security Center.

If any of these conditions have been violated, the MDR solution may fail to correctly identify assets created by distributing a reference asset image. To resolve this issue, perform the following steps on assets that have Kaspersky Endpoint Security for Linux installed:

- a. Run the following commands to generate new UUID:

```
uuidgen > /var/opt/kaspersky/kesl/common/pcid  
uuidgen > /var/opt/kaspersky/epagent/install_id
```

- b. Uninstall the Kaspersky Endpoint Security for Linux and then reinstall it.

The reference asset is ready for creating an operating system image.

## Capturing and distributing the image of a reference asset

When applying third-party tools for capturing the image of an asset with Network Agent installed, use one of the following methods:

- Recommended method. When installing Network Agent on a reference asset, capture the asset image before the first run of Network Agent service (because unique information identifying the asset is created at the first connection of Network Agent to the Administration Server). After that, it is recommended that you avoid running Network Agent service until the completion of the image capturing operation.

For Windows, refer to the following article: [Preparing a reference asset with Network Agent installed for creating an image of operating system](#).

For Linux, refer to the following article: [Deployment by capturing and copying the image of an asset](#).

- On the reference asset, stop the Network Agent service and run the klmover utility with the -dupfix key. The utility klmover is included in the installation package of Network Agent. Avoid any subsequent runs of Network Agent service until the image capturing operation completes.

Make sure that the klmover utility is run with the -dupfix key before the first run of the Network Agent service on target devices. This is a mandatory requirement and must be done at the first launch of the operating system after image deployment.

- Use the Network Agent disk cloning mode.

For Windows, refer to the following article: [Network Agent disk cloning mode](#).

For Linux, refer to the following article: [Network Agent disk cloning mode](#).

You can also capture the image of an asset without Network Agent installed. To do this, perform image deployment on target assets and then deploy Network Agent. If using this method, provide access to the network folder with stand-alone installation packages from the asset. Follow the instructions:

- For Windows, refer to the following article: [Installing images of operating systems](#) <sup>↗</sup>.
- For Linux, refer to the following article: [About remote installation tasks in Kaspersky Security Center Linux](#) <sup>↗</sup>.

## Activating the MDR solution in Kaspersky applications

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

This section contains reference information on how to activate the MDR solution depending on the license and application versions. For a complete tutorial on how to activate the MDR solution, refer to the following article: [Activating and deploying Kaspersky Managed Detection and Response](#).

The following articles describe how to manage license keys and activation codes in the Administration Server:

- [Automatic distribution of license keys and activation codes](#) <sup>↗</sup>
- [Viewing information about license keys and activation codes in use](#) <sup>↗</sup>

| MDR license                                                                                                                                                                                                                                                                                          | Supported applications for the following methods:<br>Activation code<br>BLOB file                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Supported applications for the following methods:<br>BLOB file                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kaspersky Symphony MDR<br>Kaspersky Next Complete Security<br>Kaspersky Optimum Security<br>Kaspersky Next MXDR Optimum<br>Refer to: <a href="#">Kaspersky Symphony, MDR and NEXT Complete Security licenses</a>                                                                                     | <ul style="list-style-type: none"> <li>• Kaspersky Endpoint Security for Windows version 12.6 or later</li> <li>• Kaspersky Endpoint Security for Windows version 12.8 or later in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Windows version 12.6 or later in the Endpoint Detection and Response Agent mode</li> <li>• Kaspersky Endpoint Security for Linux version 12.3 or later</li> <li>• Kaspersky Endpoint Security for Linux version 12.3 or later in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Mac version 12.2 or later</li> </ul> Installing the BLOB file is required if your organization has multiple tenants.<br><br>Activating with a key file has limited support. We recommend that you use an activation code.                                                                                                                                                               | <ul style="list-style-type: none"> <li>• Kaspersky Endpoint Security for Windows version 12.5 and earlier</li> <li>• Kaspersky Endpoint Security for Windows version 5.2–6.1 in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Windows version 12.3–12.5 in the Endpoint Detection and Response Agent mode</li> <li>• Kaspersky Endpoint Security for Linux version 12.2 and earlier</li> <li>• Kaspersky Endpoint Security for Linux version 12.2 and earlier in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Mac version 12.1 and earlier</li> </ul> Kaspersky Anti Targeted Attack Platform (including EDR) version 4.0–7.1 supports installing the MDR configuration file, which includes the BLOB file and the KPSN configuration file.<br><br>Kaspersky Anti Targeted Attack Platform (including EDR) version 8.0 does not require the MDR configuration file. |
| Kaspersky MDR<br>Kaspersky Managed Detection and Response<br>Refer to: <a href="#">Kaspersky MDR licenses</a>                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• Kaspersky Endpoint Security for Windows version 12.6 or later</li> <li>• Kaspersky Endpoint Security for Windows version 12.8 or later in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Windows version 12.6 or later in the Endpoint Detection and Response Agent mode</li> <li>• Kaspersky Endpoint Security for Linux version 12.3 or later</li> <li>• Kaspersky Endpoint Security for Linux version 12.3 or later in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Mac version 12.2 or later</li> <li>• Kaspersky Embedded Systems Security for Windows version 4.0 or later</li> <li>• Kaspersky Embedded Systems Security for Linux version 4.0 or later</li> </ul> Installing the BLOB file is required if your organization has multiple tenants.<br><br>Activating with a key file has limited support. We recommend that you use an activation code. | <ul style="list-style-type: none"> <li>• Kaspersky Endpoint Security for Windows version 12.5 and earlier</li> <li>• Kaspersky Endpoint Security for Windows version 5.2–6.1 in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Windows version 12.3–12.5 in the Endpoint Detection and Response Agent mode</li> <li>• Kaspersky Endpoint Security for Linux version 12.2 and earlier</li> <li>• Kaspersky Endpoint Security for Linux version 12.2 and earlier in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Mac version 12.1 and earlier</li> </ul> Kaspersky Anti Targeted Attack Platform (including EDR) version 4.0–7.1 supports installing the MDR configuration file, which includes the BLOB file and the KPSN configuration file.                                                                                                                         |
| Kaspersky MDR Optimum Add-on<br>Kaspersky MDR Expert Add-on<br>Kaspersky Managed Detection and Response Basic Add-on<br>Kaspersky Managed Detection and Response Advanced Add-on<br>Kaspersky Managed Detection and Response Prime Add-on<br>Refer to: <a href="#">Kaspersky MDR Add-on licenses</a> | <ul style="list-style-type: none"> <li>• Kaspersky Endpoint Security for Windows version 12.6 or later</li> <li>• Kaspersky Endpoint Security for Windows version 12.8 or later in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Windows version 12.6 or later in the Endpoint Detection and Response Agent mode</li> </ul> Installing the BLOB file is required if your organization has multiple tenants.<br><br>Activating with a key file has limited support. We recommend that you use an activation code.                                                                                                                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• Kaspersky Endpoint Security for Windows version 12.5 and earlier</li> <li>• Kaspersky Endpoint Security for Windows version 5.2–6.1 in the Light Agent mode</li> <li>• Kaspersky Endpoint Security for Windows version 12.3–12.5 in the Endpoint Detection and Response Agent mode</li> </ul> Kaspersky Anti Targeted Attack Platform (including EDR) version 4.0–7.1 supports installing the MDR configuration file, which includes the BLOB file and the KPSN configuration file.                                                                                                                                                                                                                                                                                                                                                                             |
| Kaspersky Managed Detection and Response for Industrial CyberSecurity<br>Refer to: <a href="#">Kaspersky MDR for Industrial CyberSecurity Add-on license</a>                                                                                                                                         | Kaspersky Industrial CyberSecurity for Nodes Windows version 4.5 or later.<br><br>Installing the BLOB file is required if your organization has multiple tenants.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Installing the BLOB file is required if your organization has multiple tenants. In this scenario, a file key or an activation code is still necessary.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

# Activating the MDR solution in Kaspersky applications. Kaspersky MDR Add-on licenses

The tables below describe methods of activating the MDR solution in Kaspersky applications for the following licenses:

- 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 for Windows

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.10 or later      | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"><li>• You currently use MDR tenants.</li><li>• You have ever created MDR tenants, even if additional tenants have been deleted.</li></ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>To activate both the Endpoint Detection and Response Optimum solution and the MDR solution, apply the activation code for Endpoint Detection and Response Optimum and an MDR configuration (BLOB) file for the MDR solution.</p>                                                          | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"><li>1. Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li><li>2. Configure the policy to install the BLOB file on your assets.</li></ol> |
| 12.9                | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"><li>• You currently use MDR tenants.</li><li>• You have ever created MDR tenants, even if additional tenants have been deleted.</li></ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>To activate both the Endpoint Detection and Response Optimum solution and the MDR solution, apply the activation code for Endpoint Detection and Response Optimum and an MDR configuration (BLOB) file for the MDR solution.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"><li>1. Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li><li>2. Configure the policy to install the BLOB file on your assets.</li></ol> |

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.6–12.8           | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>To activate both the Endpoint Detection and Response Optimum solution and the MDR solution, apply the activation code for Endpoint Detection and Response Optimum and an MDR configuration (BLOB) file for the MDR solution.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 12.5 and earlier    | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent mode

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.10 or later      | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>To activate both the Endpoint Detection and Response Optimum solution and the MDR solution, apply the activation code for Endpoint Detection and Response Optimum and an MDR configuration (BLOB) file for the MDR solution.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 12.9                | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p>                                                                                                                                                                            | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 12.6–12.8           | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p>                                                                                                                                                                            | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 12.3–12.5           | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Security for Virtualization Light Agent

| Application version                                                                            | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.3 or later<br>Kaspersky Endpoint Security for Windows 12.10 or later in the Light Agent mode | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>To activate both the Endpoint Detection and Response Optimum solution and the MDR solution, apply the activation code for Endpoint Detection and Response Optimum and an MDR configuration (BLOB) file for the MDR solution.</p>                                                          | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 6.2<br>Kaspersky Endpoint Security for Windows 12.8–12.9 in the Light Agent mode               | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>To activate both the Endpoint Detection and Response Optimum solution and the MDR solution, apply the activation code for Endpoint Detection and Response Optimum and an MDR configuration (BLOB) file for the MDR solution.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 6.0–6.1 Kaspersky Security for Virtualization Light Agent                                      | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 5.2 Kaspersky Security for Virtualization Light Agent                                          | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 6.3 or later<br>Kaspersky Endpoint Security for Linux 12.3 or later in the Light Agent mode    | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol>                                                                                                                                                           |
| 6.2<br>Kaspersky Endpoint Security for Linux 12.2 in the Light Agent mode                      | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

# Activating the MDR solution in Kaspersky applications. Kaspersky MDR licenses

The tables below describe methods of activating the MDR solution in Kaspersky applications for the following licenses:

- Kaspersky MDR
- Kaspersky Managed Detection and Response

## Kaspersky Endpoint Security for Windows

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                           | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.10 or later      | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"><li>• You currently use MDR tenants.</li><li>• You have ever created MDR tenants, even if additional tenants have been deleted.</li></ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"><li>1. Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li><li>2. Configure the policy to install the BLOB file on your assets.</li></ol> |
| 12.9                | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"><li>• You currently use MDR tenants.</li><li>• You have ever created MDR tenants, even if additional tenants have been deleted.</li></ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p>             | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"><li>1. Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li><li>2. Configure the policy to install the BLOB file on your assets.</li></ol> |

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.6–12.8           | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>To activate both the Endpoint Detection and Response Optimum solution and the MDR solution, apply the activation code for Endpoint Detection and Response Optimum and an MDR configuration (BLOB) file for the MDR solution.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 12.5 and earlier    | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent mode

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.10 or later      | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p>                                                          | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 12.9                | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 12.6–12.8           | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 12.3–12.5           | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                            | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Security for Virtualization Light Agent

| Application version                                                                            | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.3 or later<br>Kaspersky Endpoint Security for Windows 12.10 or later in the Light Agent mode | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p>                                                                                                                                                                                                                                                                                              | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 6.2<br>Kaspersky Endpoint Security for Windows 12.8–12.9 in the Light Agent mode               | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>To activate both the Endpoint Detection and Response Optimum solution and the MDR solution, apply the activation code for Endpoint Detection and Response Optimum and an MDR configuration (BLOB) file for the MDR solution.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 6.0–6.1 Kaspersky Security for Virtualization Light Agent                                      | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 5.2 Kaspersky Security for Virtualization Light Agent                                          | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 6.3 or later<br>Kaspersky Endpoint Security for Linux 12.3 or later in the Light Agent mode    | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p>                                                                                                                                                                                                                                                                                              | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 6.2<br>Kaspersky Endpoint Security for Linux 12.2 in the Light Agent mode                      | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Endpoint Security for Linux

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                          | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.3 or later       | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 12.2 and earlier    | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                   | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Endpoint Security for Mac

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                      | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2 or later       | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>An expired MDR configuration (BLOB) must be replaced with a new one.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 12.1 and earlier    | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                               | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Embedded Systems Security for Windows

| Application version | Activation method                                                                                                                                                                                   | KPSN configuration file requirement                                            |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 4.0                 | <p>Apply an activation code or key file to activate the MDR solution.</p> <p>It's not necessary to use an MDR configuration (BLOB) file, all assets are assigned to the root tenant by default.</p> | The application supports MDR usage with and without a KPSN configuration file. |

## Kaspersky Embedded Systems Security for Linux

| Application version | Activation method                                                                                                                                                                        | KPSN configuration file requirement                                            |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 4.0                 | Apply an activation code or key file to activate the MDR solution.<br>It's not necessary to use an MDR configuration (BLOB) file, all assets are assigned to the root tenant by default. | The application supports MDR usage with and without a KPSN configuration file. |

## Activating the MDR solution in Kaspersky applications. Kaspersky Symphony MDR, Kaspersky Next Complete Security, Kaspersky Optimum Security and Kaspersky Next MXDR Optimum licenses

The tables below describe methods of activating the MDR solution in Kaspersky applications for the following licenses:

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

## Kaspersky Endpoint Security for Windows

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.10 or later      | You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases: <ul style="list-style-type: none"><li>• You currently use MDR tenants.</li><li>• You have ever created MDR tenants, even if additional tenants have been deleted.</li></ul> It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.                                                          | The application supports MDR usage with and without a KPSN configuration file.<br><br>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.<br><br>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files: <ol style="list-style-type: none"><li>1. Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li><li>2. Configure the policy to install the BLOB file on your assets.</li></ol> |
| 12.9                | Activating the MDR solution with a key file is not supported.<br><br>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases: <ul style="list-style-type: none"><li>• You currently use MDR tenants.</li><li>• You have ever created MDR tenants, even if additional tenants have been deleted.</li></ul> It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code. | The application supports MDR usage with and without a KPSN configuration file.<br><br>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.<br><br>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files: <ol style="list-style-type: none"><li>1. Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li><li>2. Configure the policy to install the BLOB file on your assets.</li></ol> |

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.6–12.8           | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 12.5 and earlier    | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                            | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Security for Virtualization Light Agent

| Application version                                                                            | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.0–6.1 Kaspersky Security for Virtualization Light Agent                                      | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 5.2 Kaspersky Security for Virtualization Light Agent                                          | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 6.3 or later<br>Kaspersky Endpoint Security for Windows 12.10 or later in the Light Agent mode | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>Light Agent cannot be activated under the NEXT Complete Security license.</p>                                                          | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 6.2<br>Kaspersky Endpoint Security for Windows 12.8–12.9 in the Light Agent mode               | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> <p>Light Agent cannot be activated under the NEXT Complete Security license.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |

| Application version                                                                         | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                          | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.3 or later<br>Kaspersky Endpoint Security for Linux 12.3 or later in the Light Agent mode | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 6.2<br>Kaspersky Endpoint Security for Linux 12.2 in the Light Agent mode                   | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                   | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Endpoint Security for Linux

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                          | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.3 or later       | <p>You must have an MDR configuration (BLOB) file installed before applying an activation code or key file in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 12.2 and earlier    | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                   | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Kaspersky Endpoint Security for Mac

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | KPSN configuration file requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.2 or later       | <p>Activating the MDR solution with a key file is not supported.</p> <p>You must have an MDR configuration (BLOB) file installed before applying an activation code in the following cases:</p> <ul style="list-style-type: none"> <li>You currently use MDR tenants.</li> <li>You have ever created MDR tenants, even if additional tenants have been deleted.</li> </ul> <p>It's not necessary to change expired MDR configuration (BLOB) installed before when you apply an activation code.</p> | <p>The application supports MDR usage with and without a KPSN configuration file.</p> <p>To use the MDR solution without a KPSN configuration file, specify the activation code even if you have an MDR configuration (BLOB) file deployed.</p> <p>When you already have MDR configuration (BLOB) files installed on your assets, and the MDR solution was activated before January 2024, you need to re-download and re-install BLOB files:</p> <ol style="list-style-type: none"> <li>Download the MDR configuration (BLOB) file for the required tenant <a href="#">in MDR Web Console</a>.</li> <li>Configure the policy to install the BLOB file on your assets.</li> </ol> |
| 12.1 and earlier    | The MDR solution can be activated with an MDR configuration (BLOB) file.                                                                                                                                                                                                                                                                                                                                                                                                                            | The MDR solution can only operate when the KPSN configuration file is installed in the Kaspersky Security Center.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

# Activating the MDR solution in Kaspersky applications. Kaspersky Managed Detection and Response for Industrial CyberSecurity Add-on license

The table below describes methods of activating the MDR solution in Kaspersky applications for the Kaspersky Managed Detection and Response for Industrial CyberSecurity Add-on license.

## Kaspersky Industrial CyberSecurity for Nodes Windows

| Application version | Activation method                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | KPSN configuration file requirement                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| 4.5                 | <p>Apply an activation code or key file to activate the MDR solution:</p> <ul style="list-style-type: none"><li>• If you do not use and have never created MDR tenants, using an MDR configuration (BLOB) file is not required.</li></ul> <p>If you use MDR tenants, you must install an MDR configuration (BLOB) file, even it has expired. The application supports MDR usage with and without a KPSN configuration file.</p> <p>Use the MDR Plug-in version 3.0.0 or later to apply multiple activation codes for the Kaspersky Industrial CyberSecurity for Nodes license. You can use the MDR Web Console if you only have a single activation code for the Kaspersky Industrial CyberSecurity for Nodes license.</p> <p>Applying new activation codes for Kaspersky Industrial CyberSecurity for Nodes is not available in the Kingdom of Saudi Arabia <a href="#">region</a>, if you have any of the following licenses:</p> <ul style="list-style-type: none"><li>• Kaspersky Managed Detection and Response Basic Add-on</li><li>• Kaspersky Managed Detection and Response Advanced Add-on</li><li>• Kaspersky Managed Detection and Response Prime Add-on</li></ul> | The application supports MDR usage with and without a KPSN configuration file. |

# Licensing

A *license* is a time-limited right to use the application, granted under the Terms and Conditions.

You can only operate a single license in the MDR Web Console and MDR Plug-in version 2.4.1 and earlier. When you enter a new activation code, it replaces the previous one.

Starting with MDR Plug-in version 2.4.2, [you can operate multiple MDR licenses simultaneously](#).

A license grants you the following kinds of services:

- Use of the application in accordance with the Terms and Conditions
- Getting technical support

The scope of services and validity period depend on the type of license under which the application was activated.

The following license types are provided:

- *Trial*—A free license intended for trying out the application.

A trial license usually has a short term. When the trial license expires, all Kaspersky Managed Detection and Response features become disabled. To continue using the application, you need to purchase a commercial license.

You can activate the application under the trial license only once.

- *Commercial*—A paid license granted upon purchase of the application.

When the commercial license expires, the application continues running with limited functionality (telemetry is not provided). To continue using all of the features of Kaspersky Managed Detection and Response, you must renew your commercial license.

We recommend renewing the license before its expiration, to ensure maximum protection against all security threats.

- *Subscription*—A paid license that enables the application usage for a monthly or annual billing period, with auto-renewal, until canceled or expired.

The subscription license can be of two types:

- *Limited*—Automatically renewed at the end of each billing period up until the defined expiration date.
- *Open-ended*—Auto-renewed at the end of each billing period until canceled by the customer.

You can manage the subscription license via the Kaspersky License Management Portal (LMP).

If you change your license scope, for example change the number of assets, the license details are updated in MDR Web Console within 24 hours.

When the subscription license is canceled or expired, the application continues running with limited functionality (telemetry is not provided). To continue using all of the features of Kaspersky Managed Detection and Response, you must renew your subscription license.

We recommend renewing the license before its expiration, to ensure maximum protection against all security threats.

# Comparison of commercial license tiers

The set of features available in Kaspersky Managed Detection and Response depends on the tier of your commercial license (see the table below).

Comparison of Kaspersky Managed Detection and Response commercial license tiers

| Feature                                                                                                            | MDR / MDR Expert* | MDR Optimum* /MDR Basic* | MDR Advanced*                                                                                                                                        | MDR Prime*                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------|-------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 24x7 monitoring, incident detection and management                                                                 | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Automatic threat hunting                                                                                           | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Response playbooks and automatic incident response                                                                 | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Asset status and visibility check                                                                                  | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| MDR Web Console with dashboards and reports                                                                        | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Ability to receive advanced incident information                                                                   | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Incident history retention period                                                                                  | 1 year            | 1 year                   | 1 year                                                                                                                                               | 1 year                                                                                                                                                                             |
| Raw data retention period                                                                                          | 3 months          | 1 month                  | 3 months                                                                                                                                             | 3 months                                                                                                                                                                           |
| Managed threat hunting and incident investigation                                                                  | ✓                 | —                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Extended expert support for incident management                                                                    | ✓                 | —                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Access to Kaspersky Threat Intelligence Portal (for licenses with start date earlier than July 12, 2024)           | ✓                 | —                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| API for exporting Kaspersky MDR data                                                                               | ✓                 | —                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Customers can create a custom incident to be processed by the Kaspersky MDR solution**                             | ✓                 | —                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Localized data storage*                                                                                            | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Multitenancy                                                                                                       | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Adding and editing comments to incidents                                                                           | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Adding and editing attachments to incidents                                                                        | ✓                 | ✓                        | ✓                                                                                                                                                    | ✓                                                                                                                                                                                  |
| Advanced incident investigation: analysis to establish the background, circumstances and detailed attack mechanism | —                 | —                        | <div> <div>✓</div> <div>Customers cannot choose the incidents for advanced investigation; there is no guaranteed incident response time</div> </div> | <div> <div>✓</div> <div>Customers can choose the incidents for advanced investigation (within the purchased time limit); there is a guaranteed incident response time</div> </div> |

\*This tier or feature is available for some regions only and may be unavailable for purchase by new customers. Contact your Kaspersky Managed Detection and Response solution provider for details about the commercial license tiers available to you.

\*\*Kaspersky Managed Detection and Response solution ensures processing of three requests per week in accordance with [performance targets of the solution delivery](#). The number of requests processed in accordance with performance targets of the solution delivery is increased proportionally: for every 10,000 connected endpoints, the number of requests is increased by 1.

## About the activation code

An *activation code* is a unique sequence of 20 letters and numbers. You have to enter an activation code in order to [activate Kaspersky Managed Detection and Response](#). You receive the activation code at the email address that you provided when you bought Kaspersky Managed Detection and Response.

To activate the solution by using the activation code, you need internet access in order to connect to Kaspersky activation servers.

If you have lost your activation code, contact the Kaspersky partner from whom you purchased the license.

## Providing a new activation code

### Initial activation of Kaspersky Managed Detection and Response

Refer to these articles:

- [Activating Kaspersky Managed Detection and Response in Kaspersky Security Center \(recommended\)](#)
- [Activating Kaspersky Managed Detection and Response in MDR Web Console](#)

### Entering a new activation code

You must provide a new activation code for Kaspersky Managed Detection and Response, for example, when you want to upgrade the solution or when you need to renew your expiring license.

This feature is only available if you have the **Application integration** access right set in [Kaspersky Security Center Web Console](#) <sup>2</sup> or [Kaspersky Next Expert View](#) <sup>2</sup>.

For details on how to manage multiple licenses in Kaspersky Managed Detection and Response in Kaspersky Security Center with MDR Plug-in 2.4.2 or later, refer to this article: [Managing licenses in Kaspersky Security Center](#).

If you use a single license for the MDR solution, you can renew this license in the MDR Web Console. The **MDR Administrator** role is required.

If your organization has multiple current licenses, you can only manage them in Kaspersky Security Center. Using the MDR Web Console for license renewal in this scenario stops telemetry from being sent from assets.

We recommend that you use the MDR Plug-in for Kaspersky Security Center to enter a new activation code.

*To enter a new activation code for Kaspersky Managed Detection and Response in Kaspersky Security Center with MDR Plug-in:*

1. In the **MDR** section of Kaspersky Security Center, click the **Licensing** tab.
2. Click the **Activate the solution** button and enter the activation code in the invoked panel.
3. Select the tenants to which the users of this Administration Server will have access.

The new activation code is applied. Kaspersky Managed Detection and Response works under the license provided.

*To replace the current activation code with a new one in MDR Web Console:*

1. Click the **Licensing** tab.
2. Click the **Enter a new activation code** link.
3. Enter a new activation code and click **Continue**.
4. Select your region and click **Confirm and activate**.

## Managing licenses in Kaspersky Security Center

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

If your organization has multiple current licenses, you can only manage them in Kaspersky Security Center.

The **MDR Administrator** role is required to manage licenses.

*To view licenses,*

In the **MDR** section of Kaspersky Security Center, click the **Licensing** tab.

The **Licenses in your organization** list appears. The top panel lists general information about licenses:

- Region
- [Commercial license tier](#)
- Total number and limit of connected assets

The **Current** tab only shows current licenses. Click the **All** tab to view all licenses in your organization.

The table shows the following information about licenses:

## License name

License name that includes details like the license tier and the limit of assets.

## Connected assets / limit

The number of assets that use this license and the limit.

The limit of assets for the license is highlighted with red when exceeded.

This number does not include hosts with BLOB configuration files that were created before January 1, 2024. To fix this issue, update the BLOB file in the tenant settings and apply it to the tenant's assets. Refer to the following topic for details: [About the MDR configuration file](#).

## ID

The license identifier.

## Expiration date

License expiration date is highlighted with red if the license is expired or expires in 14 days or sooner.

## Status

One of the following statuses:

- Current
- Expired
- Rejected
- Not used
- Replaced

## Client name

Hidden by default. You can enable this column in the table menu.

*To download a CSV file that shows licenses by tenants (MDR Plug-in version 2.4.2),*

On the **Current** tab, click **Export by tenants to CSV**.

The CSV file includes the distribution of assets by tenant for each license.

*To display licenses by tenants (MDR Plug-in version 2.5.0 or later),*

On the **Current** tab, click **Display license usage by tenants**.

The table shows distribution of assets by tenant for each license.

*To download the [MDR configuration file](#) for a license,*

Select the **Archive for asset configuration** column and click **Download**.

To enter a new activation code,

Click the **Enter a new activation code** button and enter the activation code in the invoked panel.

The [license tier](#) and region of the new license must match the license tier and region of other activation codes in your organization.

To remove an activation code:

1. Select the radio button next to the activation code that you want to delete and click the  icon.
  2. In the windows that opens, confirm deletion of the activation code.
- The license status changes to **Not used**. You can re-enter the deleted activation code.

## Licensing troubleshooting

If you have activated the MDR solution on your assets, and the **Licensing** section in the MDR Web Console displays fewer assets than are connected to the MDR solution, refer to the following list of possible causes and their respective solutions.

The MDR solution is activated under multiple licenses

Solution:

Activate all license keys in the MDR plug-in. The MDR Web Console does not support activating multiple MDR license keys.

The MDR solution was activated on the assets prior to 01.01.2024 using the MDR configuration (BLOB) file

Solution 1:

1. [Download a new MDR configuration \(BLOB\) file.](#)
2. Apply the new MDR configuration (BLOB) file on your assets.

Solution 2:

[Apply an activation code](#)  to activate the MDR solution on your assets.

Some of your assets use the Kaspersky Endpoint Security for Windows version 12.9 or earlier, and the MDR solution on these assets is activated with a key file

Solution:

[Apply an activation code](#) to activate the MDR solution on your assets. Activating with a key file on such assets has limited support and is not recommended.

You have used a key file for the Kaspersky Next Complete Security, Kaspersky Optimum Security, Kaspersky Next MXDR Optimum or Kaspersky Symphony MDR license to activate the Kaspersky Endpoint Security for Windows version 12.9 or earlier

Solution:

[Apply an activation code](#) to activate the MDR solution on your assets.

## About the MDR Agreement

*The MDR Agreement* is a binding agreement between you and AO Kaspersky Lab, stipulating the terms of how you may use the solution.

Carefully read the MDR Agreement before you start using the solution.

You can view the MDR Agreement:

- During the activation of Kaspersky Managed Detection and Response.
- By clicking the **Terms of Use for the MDR solution** link in the **Terms of Use for the MDR solution** block: the **MDR** section of Kaspersky Security Center → **MDR Usage** → **Terms of Use for the MDR solution**.

You accept the terms of the MDR Agreement by confirming that you agree with the MDR Agreement when activating the solution. If you do not accept the MDR Agreement, cancel the activation of Kaspersky Managed Detection and Response, and do not use the solution.

# Data provision

In order for some components of Kaspersky Managed Detection and Response to work, it's necessary for Kaspersky to process the user's data. Components do not send data without the permission of the Kaspersky Managed Detection and Response administrator.

The list of user's data depends on the region where the solution is used. For your region, the list of user data may differ from that listed in this section.

Kaspersky protects any information received in accordance with law and applicable Kaspersky rules. Data is transmitted over a secure channel.

## List of data on events occurring on User devices

In order to identify new and challenging data security threats and their sources, as well as threats of intrusion, and to take prompt measures to increase the protection of the data stored and processed with a computer by the Customer, the Customer agrees to automatically provide the following information in order to receive the Service:

- The date of software installation and activation, full name and version of the software, including information on installed updates and the language localization of the software.
- Information about the software installed on the computer, including the operating system version and the date of its download and installed updates, and about kernel objects, drivers, services, Autostart entries, programs that are automatically launched in the event of various system events (e.g. operating system startup, user login, etc.) and their configurations, browser extensions, Microsoft Internet Explorer extensions, print system extensions, Windows Explorer extensions, operating system shell extensions, loaded object checksums (MD5), Active Setup elements, control panel applications, browser and mail client versions.
- Information about file system permissions, the effective bit for file system permissions, file system permission versions, environment variables, and names of system calls.
- Information about inherited permissions for a system file.
- Information about the computer's name, IP addresses, default gateways, MAC addresses and hardware, including a checksum of the HDD's serial number, the last 12 bytes of the computer security ID (SID), and the security zone identifier contained in the NTFS data stream, Active Directory attributes of the computer account including the content of msDS-AllowedToActOnBehalfOfOtherIdentity, dNSHostName, distinguishedName, sAMAccountName, userAccountControl.
- Information about software tools used to fix problems in the software installed on the User's computer, or to change its functionality, and the return codes received after the installation of each piece of software.
- Information about the state of the computer's anti-virus protection, including the versions and release dates and times of the anti-virus databases in use, statistics about updates and connections to Kaspersky Lab's services, job identifiers, and the identifiers and versions of the software components performing the scan, flags denoting the internal Kaspersky testing environment, the primary error codes for a specific event, the secondary error codes for a specific event, and the ordinal numbers of events.
- License key and serial number of Kaspersky Lab's products, names and versions of these products. Identifiers of Kaspersky Lab's product installations, the client description from the license information file.

- Information about Customer user accounts: user account name, name of the user, operating system identifier, logon information, privileges, group memberships, types of logon session to the system, name of the authentication packet, domain names, DNS names used for authentication system logon sessions, the server name used for authentication, the user principal name (UPN) for the account, the SID, Active Directory attributes of the account, including mail, altSecurityIdentities, sAMAccountName.
- Full content of operating system logs.
- Information about call systems.
- Information about detection from Kaspersky Lab's programs that support Kaspersky Managed Detection and Response.
- Information about received emails, including: sender and recipient email addresses, subject, attachment information: attachment file name, size, hash (MD5), file format analysis results.
- Information about coordinates of the screen area where the screenshot was taken.
- Information about network connections, including sender and receiver IP addresses and ports, IPv6 zone indices, information about the direction of the network connection (inbound/outbound), the types and masks of DNS queries made, error codes for a DNS query operation, response to a DNS query, and information about the requested DNS server.
- HTTP connection data and methods, including visited web addresses, referrer URLs, user agents, information about TLS handshake: version of TLS protocol, encrypted server name from SNI extension, MD5-hash and SHA1-hash of the certificate, common name of main subject and list of additional subjects' DNS-names, name of the certificate authority, serial number of the certificate issued by the certificate authority, certificate verification result, used cipher suite, validation period of the certificate, JA3 decimal values of client and server hello packets and their MD5-hashes and network authentication protocol data: MD5 hash of data for Kerberos authentication, account or computer name, the name of the Kerberos realm name to which the server name belongs, the domain to which the client name belongs, the UPN for the account, the cryptography package that was used for the issued Kerberos ticket, the flag mask for the Kerberos ticket in hexadecimal format, the Kerberos ticket issue time, the Kerberos ticket expiration time, the expiration date of the ticket (after which the ticket cannot be renewed), and the name of the domain controller used to issue the Kerberos ticket.
- Information about application layer protocols: LDAP search request size, LDAP search request filter, unique name of the LDAP search request, list of attributes for the LDAP search request.
- .Net information: full name of the downloaded .NET build, assembly flags for the downloaded .NET build, module flags for the downloaded .NET module, the domain name for the downloaded .NET build, modules for the generated MSIL stub, information about the managed method: the namespace of the managed method of interoperation, name of the managed method of interoperation, signature of the managed method of interoperation, signature of native method, signature of the method stub.
- Information about files processed in the operating system: file name and path, size, attributes, file and object types, results of file format analysis, checksum (MD5), web address of the file download, sender email address from which the file was received and the subject of the email, the contents of the file system of the VERSIONINFO structure in the file metadata, information about the publisher if the file is signed, the user ID of the file owner, the group ID of the file owners, the timestamp of the last file access, the timestamp that the file metadata was last modified, file creation, the digital signature verification flag masks, the timestamps and codes of operations on files and objects, the number of executable file launches, the file format identifier, the full path to the object and path to the object container, the contents of the autorun file, the file name and path to the file on the remote network resource that is being accessed.
- Contents of the \etc\ directory.
- Command output data.

- Auditd data: operation result, operation description, event type, operation user.
- Information about the process: process identifier (PID), process call tracing, information about the process executable file and its command line, information about the parent process, MD5 hash of the executable file computation error code, primary error codes, process integrity information, session logon information, command line, command line arguments for the process, environment variables for the target process, unique identifier of the process activity log, name and/or address of the code injection site, information about access rights for the process, error codes for calculating the MD5 hash for an object from the process command line, a list of file wrappers that encapsulate the object, the initial working directory for the target process, the array of identifiers (PIDs) for processes that are complete.
- Registry information: names, sections, and values.
- Information about remote operations: the name of the remote computer and the fully qualified (FQDN) name of the remote computer on which the remote operation was performed, the name of the user account that initiated the remote operation, the system-provided identifier of the remote process that initiated the remote operation, the start time of the remote process that initiated the remote operation, the name of the namespace for the user of the WMI events, the name of the user's WMI events filter, the name of the created user of WMI events, and the source code of the user of the WMI events.
- Error information: error code for MD5 calculation, file access error code, primary error codes, and secondary error codes.
- Information about response event tasks created by Kaspersky Lab's specialists and the User's specialists: event name and type, date and time when the event occurred, settings and results of the response task (information about the object [path to the object, object name and size, MD5 and SHA256 checksums], information about quarantining the object, information about deleting the object, information about process termination, information about deleting a registry key/branch, information about process startup, information about objects requested by Kaspersky Lab's specialists for detailed analysis upon the User's consent [name, path, size and type of the object, MD5 and SHA256 checksums, object description, date and time of file request processing, file contents], information about installation and removal of network isolation of the device, information about errors resulting from the response task), results of the IOC Scan task: IP address and physical address from the ARP table, name and type of DNS resource record, IP address, history and browser info, record ID and name of the data source in the event log, name of the event log, user name, event time, hash, full name, and size of the file, remote IP address and port connected at the moment of scan, local adapter IP address, port open on local adapter, protocol as a number, process name, process arguments, path to the process file, Windows PID of the process and parent process, date and time of process start, service name and description, path and name of the service DLL (for svchost), path and name of the executable file of the service, Windows PID, type, status, and run mode of the service, volume label, letter, and type, Windows Registry value, registry hive value, path to the registry key, registry parameter, physical address of the device, name and version of the operating system, network name of the device, domain or workgroup.
- Data about scripts running on the computer: command line arguments, contents of the script or part of the script running on the computer, contents of the object or part of the object received by AMSI.
- Data about commands received by the console application, including the command-line interpreters, using input redirection via a pipe or file, as well as commands executed by the user in console applications, including the command-line interpreters.

If the MDR solution integrates with Kaspersky Endpoint Detection and Response Expert, the additional data is listed below:

- Information about scanned files:
- Checksum (MD5) of the object being processed; checksum (SHA256) of the object being processed; name of the object being processed; size of the object being processed; date and time of creating an object being processed; indicator showing that the digital signature of the loaded module is present and valid; information on who signed the file being processed; trust indicator of the processed object according to KSN; format of the object being processed; information about file signature check results; trust indicator of the module which integrity is checked by the Software.
- Information about alerts and detection technologies:
- Release date and time of the Software's databases; Software verdict on the object being processed; debug detection indicator; ID of the triggered record in the Software's anti-virus databases; vulnerability danger class; detect ID that was generated by the Software for the user; name of the detected malware or legitimate software that can be used to damage the user's device or data; Kaspersky Sandbox guest OS image ID; data of the internal log, generated by the anti-virus Software module for an object being processed; MD5 hash of the Kaspersky Sandbox node IP address; order number of an object being processed rescan; Software database record ID; value of level of the detected malware or legitimate software that can be used to damage the computer or user data; operating status of the Software component; date and time of the detect.
- Information about the results of checking the telemetry data after the attack Indicator rule (IOA) is triggered:

- Capabilities assigned to an object being processed (for Unix-based OS); information about system log events: event time, name of the log where the event has been detected, type and category of event, name of the event source and event description; ID of the event recorded in the Windows Event Log; timestamp of the Software databases; size of the object being processed; information about user group; date and time of creating an object being processed; name of the object being processed; checksum (MD5) of the object being processed; binary mask of the parameters for the object being processed; ID of the triggered record in the Software's anti-virus databases; unique ID of the logon session; indicator showing that the digital signature of the object being processed is present and valid; attributes of the process that attacked Software Self-Defense; current Software settings; Software vendor name; Software name; ID of the device that established remote connection to the system; path to the object being processed; value of the Windows registry element; type of the object detected by the Software; ID of the account under which the controlled process was started; process system ID (PID); controller type of the USB device; system function type recalled to fork new process (for Unix-based OS); start type of the Windows service; checksum (SHA256) of the object being processed; date and time of the last modification of the object being processed; web address being processed; sender email address or email address parts being processed; file operation code; user device name; attributes of executable file being processed; OS version, OS build number, OS update number, OS edition, extended information about the OS edition; operating system family; command line; information on who signed the file being processed; http request method; Software verdict on the object being processed; command line arguments for the process; IP addresses or IP addresses checksums of the source and the destination of the network connection being processed; name of the MITRE attack technique; release date and time of the Software's databases; format of the object being processed; description of an object being processed as defined in the object properties; HTTP referrer; name and version of the OS; date and time of signing the file; DNS server response; volume of outbound traffic; volume file system type; access rights for the object being processed; open flags for an object being processed; type of user account under which the potentially malicious object was started; data received date and time; checksum (SHA1) of an object being processed; result of action with the object being processed; logon session type; security zone identifier extracted from the NTFS stream; email message ID; detected file operations with the object being processed; DNS address of the web service being accessed; object distinguished name; integrity level for the object being processed; header of the http request being processed; data about a third-party application that had caused an error: the application image file name and path, the application image file size and checksum (MD5, SHA256, SHA-1), the application process identifier (PID), date and time of the application process image file compiling and creation, application process memory stack and application process memory address where an error had occurred, application uptime before the error had occurred, names, versions and checksums (MD5, SHA256, SHA-1) of the application components' files; HTTP/HTTPS network request indicators: request URL, open-source library type, request domain name, CND provider, request method, request start time, request packet size, total request duration, status code, response packet size, response content type, request header start time, request header end time, request body start time, request body end time, response header start time, response header end time, response body start time, response body end time, number of redirections, number of DNS resolution failures, total number of DNS resolutions, number of hosts resolved at a time, result of a single resolution, start time of a single resolution, end time of a single resolution, whether the resolution is successful, number of socket connection failures, total number of socket connections, destination address of a single connection, start time of a single connection, end time of a single connection, start time of a single handshake, end time of a single handshake, HTTP type, HTTP version, SSL type, cipher suite type, whether the connection is successful, connection failure information, request exception information and stack information when the response is abnormal; date and time when the certificate expires; full version of the Software; number of objects transferred; drive type; operating system task scheduler tasks parameters; total disk space and amount currently used; port numbers of the source and the destination of the network connection being processed; value of confidence of detecting malware or legitimate software that can be used to damage the computer or user data; date and time when the certificate was issued; ID of the MITRE attack technique; service ID; name of the Windows registry key; subject of the email message being processed; date and time when the process being processed ended; namespace name for the WMI event consumer; event time; name of the filter used by the WMI event consumer; Software protection component operating mode; certificate issuer name; environment variables assigned to an object being processed (for Unix-based OS); notification type, that triggered the statistic sending; WMI event consumer; fragment content of the object being processed; object transfer task parameters; name of network protocol used in the detected network attack; version of the object being processed; name and path to the Windows registry element; event counter; object transfer task ID; binary mask of options of the DNS query; binary mask of options of the DNS query; name of the indicator of attack (IOA); severity of the window prompting for user action; local IP address; query search area; shortened serial

number of the hard drive; query string; the proxy server used; source of the object being processed; name of the created WMI event consumer; certificate serial number; version of the indicator of attack (IOA); ID of controller mode for the USB device; receiver email address or email address parts being processed; ID of the indicator of attack (IOA); device ID; direction of a network connection; source of the web-traffic being processed: local host or remote host; IP address of the DNS server; type of the Windows registry value; ID of the MITRE attack tactic; location where code was injected in process; error that occurred on the detect processing; the host to which a connection has been established to transfer objects.

- File attributes of an object being processed; security parameters from Windows Event Log events; reason for moving the file to the category; name of the domain used to authenticate the owner of the logon session; Active Directory objects parameters; operation parameters from Windows Event Log events; user session parameters from Windows Event Log events; object type code; version of the Software's component; smart card device settings and properties; version of the statistics being sent; parent process system ID (PID); local IP address; task parameters recorded in the Windows Event Log events; DNS address of the web service being accessed; web address being processed; network connection parameters from Windows Event Log events; name of the detected malware or legitimate software that can be used to damage the user's device or data; Active Directory objects parameters; operation parameters from Windows Event Log events; Windows Event Log events additional parameters; user session parameters from Windows Event Log events; name of the domain used to authenticate the owner of the logon session; user account security identifier (SID); error type; text of the error message.

## List of data about events detected as a result of network traffic analysis

In order to identify new and challenging data security events and their sources, as well as threats of intrusion, and to take prompt measures to increase the protection of the data stored and processed with a computer by the Customer, the Customer agrees to provide the following information automatically in order to receive the Service:

- Information about scanned files:  
Checksum (MD5) of the object being processed; checksum (SHA256) of the object being processed; name of the object being processed; size of the object being processed; date and time of creating an object being processed; indicator showing that the digital signature of the loaded module is present and valid; information on who signed the file being processed; trust indicator of the processed object according to KSN; format of the object being processed; information about file signature check results; trust indicator of the module which integrity is checked by the Software.
- Information about alerts and detection technologies:  
Release date and time of the Software's databases; Software verdict on the object being processed; debug detection indicator; ID of the triggered record in the Software's anti-virus databases; vulnerability danger class; detect ID that was generated by the Software for the user; name of the detected malware or legitimate software that can be used to damage the user's device or data; Kaspersky Sandbox guest OS image ID; data of the internal log, generated by the anti-virus Software module for an object being processed; MD5 hash of the Kaspersky Sandbox node IP address; order number of an object being processed rescan; Software database record ID; value of level of the detected malware or legitimate software that can be used to damage the computer or user data; operating status of the Software component; date and time of the detect.
- Information about the source of processed objects and network connections:  
Source of the object being processed; web address being processed; accessed IPv4 address of the web service; web address of the source of the web service request (referrer); host source; name of the domain used to authenticate the owner of the logon session; local IP address; information about the client that uses a network protocol (user agent), sender email address or email address parts being processed; receiver email address or email address parts being processed; subject of the email message being processed; IP addresses or IP addresses checksums of the source and the destination of the network connection being processed; port numbers of the source and the destination of the network connection being processed; name of network protocol used in the detected network attack; name of network protocol used in the detected network attack.

- Data sent to technical support:  
If a problem is detected on the User side that affects the quality of the Solution and requires the involvement of technical support, information including the name of the organization and contact email address, a description of the problem and related materials that may assist in understanding and resolving the problem will be passed to the technical support team. Contact email address may either be: the address to which the Solution is registered, or the address of a specific employee of the User if that employee has requested assistance from the experts who provide the Solutions.  
The technical support service automatically creates an account in the technical support systems, if there was not previously an account associated with the email address transmitted by the experts.  
Creating a User's employee account is necessary to ensure communication between the User and technical support to resolve issues related to the Solution.  
This account will only be used by the Technical Support to resolve issues related to the Service until the account owner creates a request not related to the Service.
- Data sent when sending notifications and incident reports:  
The User can use the Service to send notifications upon occurrence of information security incidents occur, and summary reports on information security incidents, to recipients specified by the User.  
If the Service is configured to send notifications and reports via email, the Processor will process the following data: the User ID and email address of the Recipient.  
If the Service is configured to send notifications via the Telegram bot, the Processor will process the following data: the User ID, the notification recipient ID, a flag showing whether the notification recipient subscribes to the Telegram bot, a link to the notification recipient's chat with the Telegram bot.

## Data provision while using Kaspersky Endpoint Agent

For details about the provision of data while using Kaspersky Endpoint Agent, refer to [Kaspersky Endpoint Agent for Windows](#).

## Regions of data processing

The table below lists the regions in which user data is processed in accordance with the Kaspersky Managed Detection and Response Data Processing Agreement.

Regions of data processing

| Region of license use                               | Region of data processing |
|-----------------------------------------------------|---------------------------|
| Europe, Canada                                      | Europe                    |
| Kingdom of Saudi Arabia                             | Kingdom of Saudi Arabia   |
| Russia and other regions, except those listed above | Russia                    |

The region of data processing depends on the region you select when [activating](#) Kaspersky Managed Detection and Response to ensure compliance with legal requirements regarding the processing of user data.

## About the Data Processing Agreement

*The Data Processing Agreement (DPA)* is an integral part of the Kaspersky Managed Detection and Response Agreement. The Data Processing Agreement applies to the processing of user data by AO Kaspersky Lab on behalf of a user.

The content of the *Data Processing Agreement* (DPA), its availability in the solution interfaces, and the list of user's data depends on the region where the solution is used.

You can view the Data Processing Agreement:

- During the activation of Kaspersky Managed Detection and Response (for some regions only).
- In the **About** section of MDR Web Console: <https://mdr.kaspersky.com/about>  (for some regions only).

The **About** section is available only for logged-in users.

- In the set of documents you get when you buy Kaspersky Managed Detection and Response solution (for some regions only).

Carefully read the Data Processing Agreement before you start using the solution.

You confirm that you have fully read and understood the Data Processing Agreement when you activate the solution, or when you purchase the Kaspersky Managed Detection and Response solution. If you do not agree that your data will be processed as described in the Data Processing Agreement, cancel the activation of Kaspersky Managed Detection and Response, and do not use the solution.

# Interfaces of Kaspersky Managed Detection and Response

This section provides information about the Kaspersky Managed Detection and Response user interfaces.

You can work with Kaspersky Managed Detection and Response by using the following interfaces:

- Kaspersky Managed Detection and Response portal (hereinafter also referred to as MDR Web Console).  
MDR Web Console is available at <https://mdr.kaspersky.com/> after logging in. To log in, use the email address and password of the [Kaspersky website](#) account created [during the activation](#) of Kaspersky Managed Detection and Response.
- The **MDR** section in [Kaspersky Security Center Web Console](#) or in Kaspersky Next Expert View.  
In order to use Kaspersky Security Center Web Console with Kaspersky Managed Detection and Response, you must [download and configure](#) MDR Plug-in in Kaspersky Security Center Web Console. In Kaspersky Next Expert View, MDR Plug-in is pre-installed.  
To access Kaspersky Managed Detection and Response functions, in Kaspersky Security Center Web Console or Kaspersky Next Expert View, click **Monitoring & reporting** → **MDR**.

The capabilities and available functions in these interfaces are basically the same, but we recommend performing some tasks in one of the interfaces, since there is a wider set of functions or data available. The recommended interface is specified in the description of the tasks and usage scenarios.

The Kaspersky Security Center interface is intended mainly to accomplish the following tasks:

- [Activating the Kaspersky Managed Detection and Response solution](#)
- Checking the status of assets

The MDR Web Console interface is intended mainly to accomplish the following tasks:

- Security officer tasks: managing incidents
- Administrator tasks: managing MDR users
- Viewing and managing assets

## MDR section in Kaspersky Security Center

You can work with Kaspersky Managed Detection and Response by using the **MDR** section in [Kaspersky Security Center Web Console](#) or in Kaspersky Next Expert View. To access Kaspersky Managed Detection and Response functions, in Kaspersky Security Center, click **Monitoring & reporting** → **MDR**.

The **MDR** section in the [Kaspersky Security Center](#) web interface contains the following tabs:

- **Incidents.** Contains the link to MDR Web Console, where you can manage your incidents.
- **Settings.** Allows enabling extended notifications and switching the language for incident data, notifications, and reports.

- **Licensing.** Allows you to manage MDR licenses.
- **API.** Contains the list of API connections and the functions to manage them.
- **Tenants.** Contains the list of tenants and the functions to manage them.
- **MDR Asset statuses.** Contains the lists of malfunctioning assets and all assets ever seen.
- **Getting Started.** Contains instructions for setting up the MDR solution.
- **MDR Usage.** Contains information about the solution activation status, license, telemetry storage region, KPSN configuration file, and Terms of Use acceptance status.

You can also [add](#) the **MDR assets by status** widget on the **Monitoring & reporting** → **Dashboard** pane in Kaspersky Security Center.

## Setting up MDR Plug-in in Kaspersky Security Center

This section contains information about the initial configuration of MDR Plug-in in Kaspersky Security Center, for work with Kaspersky Managed Detection and Response.

## Setting access rights in Kaspersky Security Center

You must set access rights for every user of Kaspersky Security Center Web Console or Kaspersky Next Expert View who will use MDR functions in Kaspersky Security Center. Access rights depend on the actions that you want users to be able to perform.

You can create MDR roles with predefined access rights automatically by clicking the link in the first step on the **Getting Started** tab of **MDR** section in Kaspersky Security Center.

*To set access rights:*

1. In Kaspersky Security Center, go to the **Users & roles** → **Roles** section, and then create a new role. For details on how to create roles, refer to [Kaspersky Security Center Windows Help](#), [Kaspersky Security Center Linux Help](#), or [Kaspersky Next Expert View Help](#).
2. On the **Access rights** tab of a new role, set the **Allow** right for the following functional areas:

- **Kaspersky Security Center Administration Server** → **General features** → **Application integration**  
**Kaspersky Security Center Administration Server** → **General features** → **Basic functionality**  
**Kaspersky Security Center Administration Server** → **General features** → **Access objects regardless of their ACLs**

These access rights allow users to activate, configure, use, and terminate the use of Kaspersky Managed Detection and Response

- **Kaspersky Managed Detection and Response** → **Incident access**

It is required to set the **Allow** right for the **Incident access** functional area for users to have access to the **MDR** section in Kaspersky Security Center. If the **Incident access** functional area has the **Deny** right set, users can see only the **Getting Started** tab of the **MDR** section in Kaspersky Security Center.

- **Kaspersky Managed Detection and Response → Tenant management**

Permits users to create, view, and edit tenants.

- **Kaspersky Managed Detection and Response → REST API access**

Permits users to manage Kaspersky Managed Detection and Response through the REST API.

3. Assign the created role to all users who will use MDR functions in Kaspersky Security Center.

The following table shows the minimum set of access rights.

Minimum set of access rights

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Application Integration     | —     | ✓    |
| Incident access             | ✓     | —    |
| Auto-accept settings        | —     | ✓    |
| Response management         | —     | ✓    |
| Tenant management           | —     | ✓    |
| Incident summary scheduling | —     | ✓    |
| REST API access             | —     | ✓    |

The access rights are set.

## Viewing and editing the MDR settings in Kaspersky Security Center

You can view and edit settings of MDR Plug-in installed in Kaspersky Security Center.

*To view and edit settings:*

1. In the **MDR** section of Kaspersky Security Center, click the **Settings** tab.
2. If you want to enable [extended notifications](#) via email, turn on the **Enable extended notifications via email** option, and then select the check box to confirm that you have read and understand the terms of sending extended notifications.
3. You can use the **Language** setting to select English or Russian for displaying reports and notifications.
4. Click the **Save** button in the lower part of the window to save the settings.

The **Save** button becomes active only if you changed the settings.

## Using MDR Plug-in functions on a virtual Administration Server

To use MDR functions in Kaspersky Security Center on a virtual Administration Server:

- If you use Kaspersky Security Center Windows:
  1. Download the [MDR configuration file](#) in Kaspersky Security Center Web Console or in [MDR Web Console](#).
  2. In Kaspersky Security Center Web Console, select the main (physical) Administration Server where your virtual Administration Server is located.
  3. Enable the [Kaspersky Private Security Network](#)  switch in the main (physical) Administration Server properties.
  4. Click the **Select file with KSN Proxy settings** button, and select the MDR configuration file you have downloaded.
- If you use Kaspersky Next Expert View:
  1. Activate Kaspersky Managed Detection and Response on the main (physical) Administration Server.
  2. On the main (physical) Administration Server, click **Monitoring & reporting** → **MDR**, open the **MDR Usage** tab, and make sure that the **KPSN configuration file for integration with the KSC Administration Server** section contains the correct status and version of the KPSN configuration file. Example of correct status and version:

To send telemetry data to the Kaspersky MDR infrastructure, the KPSN configuration file with version is used

If the file status or version is incorrect, please [contact Technical Support](#).

## Using MDR functions in Kaspersky Security Center through a proxy server

If a proxy server is used on the network where Kaspersky Security Center is running, you must set two environment variables with proxy server settings for the HTTP and the HTTPS protocols, for the MDR functions in Kaspersky Security Center to work properly. These environment variables must be set on the host where Kaspersky Security Center Web Console is installed.

The environment variables have the following format:

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

where:

- `<protocol>` is http or https.
- `<proxy_user_name>` is the user name for authorization on the proxy server.
- `<proxy_user_password>` is the password for authorization on the proxy server.
- `<host>:<port>` are the name or IP address of the proxy server, and its port number.

Example of environment variables:

```
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
```

You can set the environment variables in two ways:

- If you want to apply the proxy settings to all applications on the host where Kaspersky Security Center Web Console is installed, add these environment variables by using the **Edit the system environment variables** component of the Windows operating system. For information on using this component, refer to the documentation for the version of the operating system that you are using.
- If you want to apply these proxy settings only to Kaspersky Security Center Web Console, add these environment variables in the .env file located in the Kaspersky Security Center Web Console installation folder (by default, C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\). If the .env file is missing in the installation folder, create it.

After setting the environment variables, you need to restart the host where Kaspersky Security Center Web Console is installed for the changes to be applied.

## Changing the certificates to use MDR functions in Kaspersky Security Center with a proxy server or anti-virus software

You need to redefine the certificate chain for connection between Kaspersky Security Center Web Console with MDR Plug-in and the MDR solution infrastructure in the following cases:

- A proxy server with a TLS connection is used on the network where Kaspersky Security Center is running.
- Anti-virus software with TLS traffic encryption is running on a host where Kaspersky Security Center Web Console is installed.

*To redefine the certificate chain:*

1. Save the necessary certificates as files on your computer.
  - To save the certificate file of the software encrypting traffic, on the host with Kaspersky Security Center Web Console open <https://mdr-ksc.kaspersky.com/> in the Chrome browser, click the lock icon in the address bar next to the site address, click **Connection is secure**, click **Certificate is valid**, go to the **Details** tab, and then click the **Export** button. For instructions for other browsers, refer to the documentation for these browsers.
  - To get the certificate used to connect to the proxy server, contact your network administrator.
2. Add the saved certificates to the file with the .PEM extension (for example, KL\_Root.pem).
3. Place the created .PEM file in the Kaspersky Security Center Web Console installation folder (by default, C:\Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\).
4. Add the NODE\_EXTRA\_CA\_CERTS environment variable to the .env file located in the Kaspersky Security Center Web Console installation folder. If the .env file is missing in the installation folder, create it.

Example of the variable:

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

To apply the changes after you set the environment variable, restart the host where Kaspersky Security Center Web Console is installed.

# Hiding and showing the MDR features in Kaspersky Security Center

By default, the interface elements related to Kaspersky Managed Detection and Response are displayed in the interface of Kaspersky Security Center. If you do not use Kaspersky Managed Detection and Response, you can hide its features from the interface. Later, you can [change the interface settings](#) to show the hidden elements again.

*To hide the MDR features in Kaspersky Next Expert View:*

1. In Kaspersky Security Center Web Console or Kaspersky Next Expert View, hover the mouse pointer over your username, which is located on the left panel at the bottom. The interface settings menu appears.
2. Click **Interface options**.
3. Turn off or turn on the **Show MDR features**.
4. Click the **Save** button.

Kaspersky Security Center saves the value of this option only for your user account. Other users can set a different value.

The **MDR** section is hidden or shown.

## MDR Web Console

You can work with Kaspersky Managed Detection and Response in the web interface named [MDR Web Console](#).

The MDR Web Console window contains the following items:

- Main menu in the left pane of the window
- Work area in the right pane of the window

### Main menu

The main menu contains the following sections:

- **Monitoring**. Contains the widgets that provide summary information about active incidents, assets, and responses.
- **Incidents**. Contains detailed information about your incidents, and the tools to work with them.
- **Assets**. Contains detailed information about assets, and the tools to work with them.

- **Settings.** Contains the tabs to work with the user accounts, notifications, incident settings, summary reports, API, tenants, and general settings.
- **About.** Contains the information about the solution, links to the MDR Agreement, Data Processing Agreement, this online help, and the Technical Support website.

In the lower part of the left pane there is an **Account settings** control that allows you to access the *Getting started page*, change the interface language, access your user profile page, and sign out of MDR Web Console.

## Work area

The work area displays the information you choose to view in the MDR Web Console. The work area also contains control elements that you can use to configure how the information is displayed.

# Switching the interface language in Kaspersky Security Center

The MDR interface in Kaspersky Security Center is available in the following languages:

- English
- Russian
- German
- Spanish
- French
- Italian

*To switch the interface language in Kaspersky Security Center:*

1. In Kaspersky Security Center Web Console or Kaspersky Next Expert View, In the main menu, go to **Settings** → **Language**.
2. Select one of the supported localization languages.

The language is switched.

You can switch to another language at any time in the future.

# Switching the language for notifications and reports in Kaspersky Security Center

In Kaspersky Security Center you can select English or Russian for displaying incident data, notifications, and reports.

*To switch the language for notifications and reports in Kaspersky Security Center:*

1. In Kaspersky Security Center Web Console or Kaspersky Next Expert View, click **MDR** → **Settings**.
2. In the **Language** area, select **Russian** or **English**.
3. Click the **Save** button.

The language is switched.

You can switch to another language at any time in the future.

Changing the language only applies to new notifications and reports. Already generated notifications and reports retain the old language.

## Switching the interface language in MDR Web Console

The MDR Web Console interface is available in the following languages:

- English
- Russian

*To change the MDR Web Console interface language:*

1. In MDR Web Console, navigate to the **Account settings** section located on the left panel at the bottom. This section contains the **Language** area.
2. In the **Language** area, click the language that you want to apply to the MDR Console interface.

The language is changed. You can change it to another language at any time in the future.

# About the MDR configuration file

Kaspersky Managed Detection and Response uses an MDR configuration file to enable the solution on Kaspersky EPP applications for workstations (such as Kaspersky Endpoint Security for Windows) installed on [assets](#).

The MDR configuration file is generated automatically by Kaspersky Managed Detection and Response when you activate the solution via an activation code. The MDR configuration file is a ZIP archive containing the following files:

- [KPSN](#) configuration file.
- BLOB (P7) file for deployment of EPP applications that support integration with MDR via Kaspersky Security Center policies.

Once generated, the BLOB file expires in 5 years, even if the license is perpetual or issued for a longer term.

You may not need the BLOB (P7) file on the following conditions:

Note that even if you do not use the MDR configuration file, it is required to activate the solution using the MDR Web Console or MDR Plug-in in Kaspersky Security Center.

- You are only using the following EPP applications:
  - Kaspersky Endpoint Security for Windows 12.6 or later
  - Kaspersky Endpoint Security for Windows 12.8 or later in the Light Agent mode
  - Kaspersky Endpoint Security for Linux 12.3 or later
  - Kaspersky Endpoint Security for Mac 12.2 or later
- Your organization only uses the root tenant and never created additional tenants.
- You are not using Kaspersky Endpoint Detection and Response Optimum solution simultaneously with Kaspersky MDR solution. For details, refer to [Activating the MDR solution in Kaspersky applications](#).

In this case Kaspersky Endpoint Security for Windows applies the license from Kaspersky Security Center. If you use tenants other than the root tenant, you need to download MDR configuration file for each tenant.

[Download the MDR configuration file](#) and use it according to the instructions for the EPP applications installed on your assets:

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

# About Kaspersky Security Network

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

The MDR solution uses Kaspersky Security Network (KSN) for the following tasks:

- Sending telemetry from the assets.
- Integration with the Kaspersky Anti Targeted Attack Platform (EDR) server.
- Integration with Kaspersky Endpoint Detection and Response Expert within the Open Single Management Platform.

A KPSN configuration file is installed when you configure the integration with Kaspersky Anti Targeted Attack Platform (EDR) or with Kaspersky Endpoint Detection and Response Expert within the Open Single Management Platform.

We recommend to not use a KPSN configuration file to send telemetry from the assets. However, if your configuration does not meet [requirements for operation without KPSN configuration files](#), you need to install a KPSN configuration file on the Administration Server. For details on configuring KSN, refer to [Kaspersky Security Center documentation](#). To ensure secure transmission of customer telemetry to Kaspersky Managed Detection and Response, Kaspersky periodically updates the encryption keys for MDR telemetry data. Refer to the following article for details: [Periodic update of KPSN configuration files](#).

If you install a KPSN configuration file on the Kaspersky Security Center Administration Server, KSN is automatically disabled when you [revoke your consent with the terms of using the MDR solution](#).

If you have manually added a KPSN configuration file on the Administration Server and have not activated the MDR Plug-in for Kaspersky Security Center, you need to manually replace or remove the KPSN configuration file from the Administration Server.

## Periodic update of KPSN configuration files

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

We recommend that you switch the MDR solution to operation without KPSN configuration files. Refer to this article for details: [Switching the MDR solution to operation without KPSN configuration files](#). If you have assets that use KPSN configuration files, you must update KPSN configuration files once a year. Otherwise, telemetry data from these assets will stop being sent to Kaspersky Managed Detection and Response.

If you can't currently switch to operation without KPSN configuration files, see the information below and follow the instructions.

## Why updating configuration files is required

To ensure secure transmission of customer telemetry to Kaspersky Managed Detection and Response, Kaspersky periodically updates the encryption keys for MDR telemetry data. The public key is transmitted as part of the KPSN configuration file.

If you are using MDR Plug-in for Kaspersky Next Expert View or on-premises Kaspersky Security Center, in some cases (please check the details in the table below) the KPSN configuration file will be updated automatically. However, in many cases you have to replace the installed KPSN configuration file manually.

No later than one month before the expiration of the current KPSN configuration file, Kaspersky will notify you about the imminent expiration of the KPSN configuration file. There are two notification options:

- An incident will be created, notifying you about the upcoming expiration of the current KPSN configuration file.
- A notification about the upcoming expiration of the current KPSN configuration file will be published in MDR Web Console. Any user logging in MDR Web Console will see this notification.

### Actions required to update the KPSN configuration file

| The solution you use to manage your assets | The interface your SOC analysts use                                                                            | Actions required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kaspersky Next Expert View                 | MDR Plug-in installed in Kaspersky Next Expert View                                                            | <p>Log in to Kaspersky Next Expert View. When you log in, MDR Plug-in prompts you to accept the new KPSN Agreement. The KPSN configuration file will be updated automatically after the administrator accepts the KPSN Agreement.</p> <p>If MDR Plug-in successfully updates the file, you will get a notification about the change of the KPSN configuration file.</p> <p>If MDR Plug-in fails to update the KPSN configuration file, you will get a notification about the cause of the problem:</p> <ul style="list-style-type: none"><li>• Your account does not have sufficient access rights to update the file.</li><li>• An unexpected error occurred while updating the KPSN configuration file.</li></ul> <p>If no notifications are displayed, it is likely that the KPSN configuration file was successfully updated when another specialist connected to the Kaspersky Next Expert View.</p> <p>If you see a notification about insufficient access rights to update the KPSN configuration file, contact your Kaspersky Next Expert View administrator (<b>Main administrator</b> role) for help:</p> <p>Ask the administrator to connect to Kaspersky Next Expert View. When the administrator connects, the KPSN configuration file will be updated.</p> <p>You can check if the KPSN configuration file is up to date at any time. To do so, in the <b>MDR</b> section of Kaspersky Security Center click the <b>MDR Usage</b> tab. Information about the current version of the KPSN configuration file will be shown. If a new version of the KPSN configuration file is available, you can use a button to update the KPSN configuration file.</p> <p>If an unexpected error occurs while updating, contact Kaspersky technical support.</p> |
| Kaspersky Next Expert View                 | MDR Web Console<br>OR<br>You use the API to download the incidents in order to process them in your own system | <p>Log in to Kaspersky Next Expert View.</p> <p>Start the Initial Configuration Wizard to activate the MDR Plug-in.</p> <p>If your account does not have sufficient access rights to activate MDR Plug-in, contact your Kaspersky Next Expert View server administrator for help.</p> <p>Then, follow the instructions for the Kaspersky Next Expert View server and MDR Plug-in above.</p> <p>If an unexpected error occurs while updating, contact Kaspersky technical support.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| The solution you use to manage your assets                 | The interface your SOC analysts use                            | Actions required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Open Single Management Platform                            | MDR Plug-in installed in Open Single Management Platform       | <p>When an MDR Administrator logs in to the Open Single Management Platform, they must accept the new KPSN Agreement. The KPSN configuration file is updated automatically after the administrator accepts the KPSN Agreement.</p> <p>If the agreement has not been accepted, users with the MDR Administrator role can accept it later in the OSMP console.</p> <p><i>To accept the agreement and update the KPSN configuration file:</i></p> <ol style="list-style-type: none"> <li>1. In the MDR section of the OSMP Console interface, click the <b>MDR Usage</b> tab.</li> <li>2. Expand the <b>KPSN configuration file for integration with the KSC Administration Server</b> block.</li> <li>3. Enable the <b>Accept KPSN Agreement</b> option and click <b>Apply the KPSN configuration file on Administration Server</b>.</li> <li>4. Additionally, if you have configured integration with Kaspersky Endpoint Detection and Response Expert (on-premise), do the following: <ol style="list-style-type: none"> <li>a. Expand the <b>KPSN configuration file for integration with KEDR Expert</b> block.</li> <li>b. Enable the <b>Accept KPSN Agreement</b> option and click <b>Apply the KPSN configuration file for integration with KEDR Expert</b>.</li> </ol> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| On-premises Kaspersky Security Center version 14 and later | MDR Plug-in installed in on-premises Kaspersky Security Center | <p>Log in to Kaspersky Security Center.</p> <p>When you log in, depending on the MDR Plug-in version, the KPSN configuration file is updated either automatically or after a user with the MDR Administrator role accepts the new KPSN Agreement.</p> <p>If MDR Plug-in successfully updates the file, you will get a notification about the change of the KPSN configuration file.</p> <p>If MDR Plug-in fails to update the KPSN configuration file, you will get a notification about the cause of the problem:</p> <ul style="list-style-type: none"> <li>• Your account does not have sufficient access rights to update the file.</li> <li>• An unexpected error occurred while updating the KPSN configuration file.</li> </ul> <p>If no notifications are displayed, it is likely that the KPSN configuration file was successfully updated when another specialist connected to Kaspersky Next Expert View.</p> <p>If you see a notification about missing access rights to update the KPSN configuration file, contact your Kaspersky Security Center server administrator for help. Ask the administrator to connect to the Kaspersky Security Center server. When the administrator connects, the KPSN configuration file will be updated.</p> <p>If the administrator does not get the notification about the change of the KPSN configuration file, the administrator should check the version of the installed MDR Plug-in, and update it to the current version if necessary (MDR Plug-in version 2.1.17 or later is required).</p> <p>You can check if the KPSN configuration file is up to date at any time. To do so, in the <b>MDR</b> section of Kaspersky Security Center, click the <b>MDR Usage</b> tab.</p> <p>The information about the current version of the KPSN configuration file will be shown. If a new version of the KPSN configuration file is available, you can use a button to update the KPSN configuration file.</p> <p>If an unexpected error occurs while updating, contact Kaspersky technical support.</p> |

| The solution you use to manage your assets                    | The interface your SOC analysts use                                                                                                                                             | Actions required                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| On-premises Kaspersky Security Center version 14 or later     | MDR Web Console (MDR Plug-in not installed in on-premises Kaspersky Security Center OR<br>You use the API to download the incidents in order to process them in your own system | Ask the MDR Web Console administrator to: <ol style="list-style-type: none"> <li>1. Download the MDR ZIP archive from the <b>Licensing</b> page.</li> <li>2. Extract the KPSN configuration file from the ZIP archive.</li> <li>3. Send this file to the Kaspersky Security Center Administration server administrator.</li> </ol> |
| On-premises Kaspersky Security Center version 13.* or earlier | MDR Plug-in installed in on-premises Kaspersky Security Center OR<br>You use the API to download the incidents in order to process them in your own system                      | Ask the Kaspersky Security Center server administrator to upload the KPSN configuration file by clicking <b>Administration Server properties → KSN proxy server settings → KSN proxy server settings file</b> .<br>If an unexpected error occurs while updating, contact Kaspersky technical support.                              |

If there are multiple Kaspersky Security Center servers installed in your network, you have to update the KPSN configuration file on each server.

## Updating the KPSN configuration file on KATA servers

If there are KATA servers that are connected to Kaspersky Managed Detection and Response in your network, you have to update the MDR configuration file on these KATA servers.

The steps to update the MDR configuration file depend on the KATA version.

*To update the MDR configuration file on KATA servers version 8.0–8.1:*

1. Log in to the KATA web interface with the administrator account.
2. Select the **Settings** section, **KSN/KPSN and MDR** subsection.
3. Under **MDR integration**, click **Log in again**.
4. In the window that opens, enter your Kaspersky Account credentials.

After successful verification of credentials, the MDR configuration file is automatically updated on the server.

*To update the MDR configuration file on KATA servers version 7.1 and earlier:*

1. Log in to the MDR Console with the MDR Administrator account.
2. Download the MDR configuration ZIP archive from the **Getting Started** page: <https://mdr.kaspersky.com/guide>.
3. Log in to the KATA web interface with the administrator account.
4. Select the **Settings** section, **KSN/KPSN and MDR** subsection.

5. Under **MDR integration**, click **Upload** to upload the configuration file.

This opens the file selection window.

6. Select the archive downloaded from the MDR Web Console and click **Open**.

The MDR configuration file is updated on the server.

In case of problems during an MDR configuration file update, the KATA server administrator should contact Kaspersky Technical Support for instructions on how to update the MDR configuration file on the KATA server.

## Switching the MDR solution to operation without KPSN configuration files

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

The MDR solution must use KPSN configuration in the following scenarios:

- To ensure that KSN query and statistics data is never sent to another region. Without KPSN configuration, Kaspersky only ensures that data is routed to the specified region. Refer to this article for details: [Periodic update of KPSN configuration files](#).
- To ensure operation of the MDR solution when an obsolete EPP application is installed on any of your devices.

You can switch the MDR solution to operation without KPSN configuration files if the following requirements are met:

1. EPP application versions that support KPSN-free operation are installed on all your assets:

- Kaspersky Endpoint Security for Windows version 12.6 or later
- Kaspersky Endpoint Security for Windows version 12.6 or later in Endpoint Detection and Response Agent configuration
- Kaspersky Endpoint Security for Windows Light Agent version 12.8 or later
- Kaspersky Endpoint Security for Linux 12.3 or later
- Kaspersky Endpoint Security for Mac 12.2 or later
- Kaspersky Embedded Systems Security for Windows version 4.0 or later
- Kaspersky Embedded Systems Security for Linux version 4.0 or later
- Kaspersky Industrial CyberSecurity for Nodes Windows 4.5

2. MDR solution is activated on all your assets with an activation code or with a BLOB file that has been created no earlier than January 01, 2024.

BLOB files that have been created on or after January 01, 2024 contain data that is necessary for KPSN-free operation.

It is recommended to apply an activation code to activate MDR solution for EPP applications that support it. Certain versions of EPP applications do not support KPSN-free operation if you use a key file to activate the MDR solution. Refer to the following article for details: [Hardware and software requirements](#).

*To switch the MDR solution to KPSN-free operation:*

1. [Generate and review a Report On Kaspersky Software Versions in Kaspersky Security Center](#).
2. Update EPP applications according to the requirements:
  - Kaspersky Endpoint Security for Windows version 12.6 or later
  - Kaspersky Endpoint Security for Windows version 12.6 or later, the Endpoint Detection and Response Agent mode (requires installing a BLOB file)
  - Kaspersky Endpoint Security for Windows Light Agent version 12.8 or later
  - Kaspersky Endpoint Security for Linux 12.3 or later
  - Kaspersky Endpoint Security for Mac 12.2 or later
  - Kaspersky Embedded Systems Security for Windows version 4.0 or later
  - Kaspersky Industrial CyberSecurity for Nodes Windows 4.5
3. Disable KPSN usage in the Administration Server.
  - In Kaspersky Security Center that uses the MDR plug-in:
    1. Ensure that the MDR plug-in is updated to version 2.5.1.
    2. In the MDR section of Kaspersky Security Center window, click the **MDR Usage** tab.
    3. Expand the **KPSN** block and click **Disable KPSN**.
  - In Kaspersky Security Center that does not use the MDR plug-in:
    1. In the main menu, click the settings icon () next to the name of the required Administration Server.
    2. The Administration Server properties window opens.
    3. On the **General** tab, select the KSN Proxy settings section.
    4. Disable the **Use Kaspersky Private Security Network** option.
    5. Enable the **Enable KSN Proxy on Administration Server** option.
4. If you deploy assets from an operating system image, update the image so that the EPP application does not use KPSN configuration.

5. Edit the policies for EPP applications (required for both the activation code usage and the BLOB file usage scenarios).
  1. Disable the usage of Kaspersky Security Network and save the policy. Refer to the article for more information: [Configuring Kaspersky Security Network](#) .
  2. If the EPP application can only be activated with a BLOB file, [download the MDR configuration file](#) and upload the BLOB file to the policy.
  3. Re-enable the usage of Kaspersky Security Network, accept the KSN Agreement. Ensure that the Enforce option is enabled in the policy settings.

# Monitoring dashboards in MDR Web Console

MDR Web Console provides monitoring dashboards to view summary information.

*To view the dashboards:*

1. In MDR Web Console, navigate to the **Monitoring** menu item.

The **Summary** page opens.

2. The following dashboards are present on the **Summary** page:

- **Number of connected assets**

This section shows the number of connected assets versus the target number of assets.

- **Assets by status**

This is a pie chart that shows the distribution of assets by their status.

- **Active incidents**

This is a pie chart that shows the distribution of active incidents, according to their statuses.

- **Responses**

This is a pie chart that shows the distribution of responses, according to their statuses.

The number of connected assets represents assets that were seen in MDR Web Console in the last 7 days. If you want to get the number of connected assets for a specific period of time, navigate to the **Assets** menu item of MDR Web Console.

- **Telemetry statistics**

This is a dashboard that shows the telemetry statistics of the MDR solution for a client, including statistics by specific tenants. You can view data for 1 day, 7, 30, 90, 180 days, for 1 year, or for the entire period a client continuously uses the MDR solution.

This dashboard displays the number of each of the following objects:

- *Telemetry events*\* are all of the events sent from a client's assets to Kaspersky Managed Detection and Response.
- *Suspicious events* are telemetry events that Kaspersky Managed Detection and Response determines as events that require additional check.
- *Security events* are telemetry events that the detection rules determine as potential incidents.
- *Incidents* are actions that the detection technology determines as critical. Incidents require immediate reaction (response action) from Kaspersky Managed Detection and Response.
- *Detection rules triggered* is a number of unique detection rules triggered on specified telemetry events for a specified time period.

Dashboards are updated with every refresh of the **Summary** page.

*To switch dashboards to tenant-specific statistics:*

1. At the top of the **Summary** page, click **Filter**.
2. In the invoked menu, select one or multiple tenants.
3. Click **Save**.

Tenant-specific statistics are available for the following widgets:

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

# Receiving summary information

Kaspersky Managed Detection and Response provides several types of summary information that you can receive via email. This section describes how to configure receiving summary information.

## Receiving a summary of all assets in a CSV file (MDR Web Console)

You can receive a summary as a CSV file that contains all the assets from your account. No filters are applied to the summary, i.e., the number of the assets in this summary represents all assets that were seen in MDR Web Console.

You can hide assets with the **Absent** status in the summary by selecting the corresponding check box in the **Settings**.

*To receive a CSV summary:*

1. In the MDR Web Console, navigate to the **Assets** menu item.

The asset list opens.

2. Click the **Receive a CSV summary by email** button in the upper part of the window.

The summary is sent to the email address that was specified during the activation of Kaspersky Managed Detection and Response.

## Receiving incident information as a PDF (MDR Web Console)

You can receive a summary information about a particular incident as a PDF.

*To receive a PDF summary:*

1. In MDR Web Console, navigate to the **Incidents** menu item.

The incident list opens.

2. Click the incident whose summary you want to receive.

The incident card appears.

3. Click the **Receive a PDF by email** link in the upper part of the window.

The summary is sent to the email address that was specified during the activation of Kaspersky Managed Detection and Response.

# Setting up regular report delivery in MDR Web Console

This feature is only available in MDR Web Console.

You can schedule receiving a summary report that contains data about open incidents. Each set of delivery settings is saved as a schedule. You can create no more than 50 schedules for an organization, and no more than 10 schedules for each tenant.

To create or edit report delivery schedules, you must have the [MDR Administrator user role](#).

The report is sent by email in an open, unencrypted PDF format to the addresses you specified and according to the defined schedule.

The report always contains data for the last seven days, and the report generation day is not included. In other words, if you configure to receive the summary report every day, your daily report will contain data for the previous seven days, excluding the current day. If you configure receiving the summary report every Wednesday, report will contain data from the previous Wednesday to the following Tuesday.

*To set up receiving the summary report as a PDF file:*

1. In the **Settings** section of the MDR Web Console, click the **Schedules** tab.
2. Click the **Add** button.  
The **Add new schedule** window opens.
3. Turn on the toggle switch to the **Enabled** position.
4. Carefully read the notification below regarding the terms and conditions of sending the summary reports. Then, select the check box to confirm that you have read and understand the terms and conditions. If the check box is not selected, you cannot save the changes you make.
5. Specify the following settings:
  - In the **Schedule name** field, specify an arbitrary, human-readable name of the summary report. The name should contain Latin letters, digits, and special characters; it cannot be longer than 1000 characters.
  - In the **Tenant** field, select the tenant for which you want to receive a summary report. The report will contain data from the selected tenant only. Alternatively, if you want to receive a summary report about all of the tenants, select **All tenants**.
  - In the **To emails** field, specify an email address or comma-separated list of email addresses of users who will be receiving the summary.

Double check the email addresses entered, since they will be added without further confirmations. The summary reports can contain sensitive data, and will be sent in an open, unencrypted PDF format.

- In the **Sending day** field, select the days of the week when the summary should be sent to the specified email addresses. You can choose one day or **Every day**.

- In the **Time, UTC** field, specify time in 24-hour UTC format. For example, 15:00.

The schedule only affects the time when the report is received, but does not affect the period of data in the report.

The report always contains data for the last seven days, and the report generation day is not included. In other words, if you configure to receive the summary report every day, your daily report will contain data for the previous seven days, excluding the current day. If you configure receiving the summary report every Wednesday, report will contain data from the previous Wednesday to the following Tuesday.

6. Click the **Save** button.

The summary report will be sent to the specified email addresses on a weekly or daily basis.

# Receiving notifications

You can configure the delivery of notifications about events occurring with incidents and responses as they are being processed in Kaspersky Managed Detection and Response.

Kaspersky Managed Detection and Response sends notifications to clients via Telegram or email, depending on the settings that you specify. The notification body contains a description of the event and a link to the object where the event has occurred.

You can configure the notifications in MDR Web Console.

## Setting up notifications in MDR Web Console

*To configure the delivery of notifications in the MDR Web Console:*

1. In the **Settings** section of MDR Web Console, click the **Notification settings** tab.
2. Select the check boxes corresponding to the events that you want to receive email or Telegram notifications for.  
Available check boxes are:
  - **All**—All events that Kaspersky Managed Detection and Response sends notifications about.
  - **Incidents**—Notifications about creating, updating, resolving, and closing incidents.
    - **Extended notifications**—A description of the attack detected as the incident, and the response recommendations. This check box is available if the extended notifications feature is [enabled on the General settings tab](#). These notifications can be enabled only in MDR Web Console, but not in the MDR Plug-in.
  - **Comments**—Notifications on creating, updating, and deleting comments within incidents.
  - **Responses**—Notifications on creating, accepting, and rejecting responses.
  - **Information on license expiration**—Notifications about the following events: less than 30 days left before the license expires, the license has expired. Kaspersky Managed Detection and Response sends these notifications every day but not after the license has expired or the license is renewed.
3. Click the **Subscribe** button located above the check boxes, to subscribe to notifications from the Telegram chatbot. When you click the **Subscribe** button, the application generates and displays a unique link to activate the chatbot in Telegram. You can use this link for one Telegram account.

Use this link only on a device (desktop or mobile) where the Telegram app is installed. The link cannot activate the chatbot in the web version of Telegram.

If you want to receive notifications to another Telegram account, click the **Unsubscribe** button, and then repeat the subscription procedure to generate a new link and use it to activate the chatbot for another account.

4. Click the **Save** button in the lower part of the window to save settings. The **Save** button becomes active only if you changed the settings.

The delivery of notifications is configured.

## Asset status notifications

You can configure the delivery of notifications when a number of assets with a specific status exceeds a threshold.

Asset status notifications allow you to receive timely information about the following issues:

- Decrease in MDR monitoring coverage
- Asset connection problems with MDR
- Mass transition of assets to warning or critical states

For details on asset statuses, refer to the following article: [Asset statuses](#).

### How automatic notifications work

For each of the statuses listed below, you can set a threshold value as a percentage of the total number of assets. When the threshold is exceeded, a notification is sent.

| Status   | Condition                                |
|----------|------------------------------------------|
| OK       | Number of assets is below the threshold. |
| Warning  | Number of assets is above the threshold. |
| Critical | Number of assets is above the threshold. |
| Offline  | Number of assets is above the threshold. |

Automatic asset checks are performed at an interval of 1 hour.

Notifications are sent separately for each tenant that exceeds its thresholds. A notification for a given status is sent no more than once per day per tenant.

Only users who have access to the tenant with exceeded thresholds and have enabled notifications in their user settings receive the notifications.

### Configuring notification rules by the MDR Administrator

Setting up asset status notifications requires the MDR Administrator role.

*To configure asset status notification rules:*

1. In the MDR console, go to **Settings** → **General Settings**.

2. Enable one or both of the following options:

- **Receive extended email notifications**
- **Receive extended Telegram notifications**

3. Enable the **Enable notifications for asset status changes** parameter.

The **Base Rule** panel becomes editable, containing the notification rule settings. You can add additional rules (e.g., for another set of tenants) by clicking the **Add Rule** button below the **Base Rule** panel.

4. In the panel, select the tenants for which the rule will apply, or enable **Apply to all tenants**.

5. Set threshold values for asset statuses, or keep the default values.

6. Click **Save**.

The rule is now created and active. To receive notifications, MDR users need to configure asset status notifications as described below.

## Configuring asset status notifications by MDR users

*To receive asset status notifications:*

1. In the MDR console, go to **Settings** → **Notification Settings**.

2. Enable **Asset status notifications**.

3. Click **Save**.

You will now receive asset status notifications for the tenants you have access to, according to the configured rules.

## Receiving extended notifications

You can configure the delivery of extended incident notifications via email or Telegram to MDR users. Extended notifications contain a description of the attack detected as the incident, and the response recommendations. The attack description includes some data that the MDR solution receives as telemetry from devices connected to the MDR solution, so the description can include the following sensitive information:

- Host names
- Host IP addresses
- Account names
- Account passwords (if a script containing a password was run on a device)

- Service URLs
- Filenames
- Email addresses
- Names of the departments and tenants

The complete list of data received by the MDR solution is contained in the [Data provision](#) section.

## Enabling extended notifications in MDR Web Console

*To enable the delivery of the extended notifications:*

1. In the **Settings** section of MDR Web Console, click the **General settings** tab.
2. Turn on one or both of the options:
  - **Enable extended email notification**
  - **Enable extended Telegram notification**
3. Select the check box at the bottom of the panel to confirm that you have read and understand the terms of sending extended notifications.
4. Click the **Save** button.

Now, you can [subscribe](#) to extended notifications in **Notification settings** of MDR Web Console.

# Managing users

Kaspersky Managed Detection and Response users can have different roles, with a different functionality available for each role. The *role model* is a set of rules that specify user roles.

The following roles are present in Kaspersky Managed Detection and Response:

## MDR Administrator

The superuser who has access to all Kaspersky Managed Detection and Response functions granted by the license. The MDR Administrator can grant access to client data sources to other users. When you activate Kaspersky Managed Detection and Response, you become the MDR Administrator automatically, which is why we recommend using a corporate email address for the activation process instead of a personal email address. Having the MDR Administrator created with a personal email address can pose security risks, such as theft of the MDR Administrator account.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | ✓     | —    |
| Response management         | ✓     | —    |
| Tenant management           | ✓     | —    |
| Incident summary scheduling | ✓     | —    |
| REST API access             | ✓     | —    |

## Senior Security Officer

An employee who has access to the Kaspersky Managed Detection and Response functions granted by the license, but who does not have access to the REST API. The Senior Security Officer has the right to accept and reject [responses](#) <sup>2</sup>.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | ✓     | —    |
| Response management         | ✓     | —    |
| Tenant management           | —     | ✓    |
| Incident summary scheduling | —     | ✓    |
| REST API access             | —     | ✓    |

## Security Officer

An employee who has access to the Kaspersky Managed Detection and Response functions granted by the license, but who does not have access to the REST API. The Security Officer cannot accept and reject [responses](#) <sup>2</sup>.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area      | Allow | Deny |
|----------------------|-------|------|
| Incident access      | ✓     | —    |
| Auto-accept settings | —     | ✓    |

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Response management         | —     | ✓    |
| Tenant management           | —     | ✓    |
| Incident summary scheduling | —     | ✓    |
| REST API access             | —     | ✓    |

## Inviting new users in MDR Web Console

*To invite a new user to Kaspersky Managed Detection and Response:*

If your previously created [Kaspersky Account](#) (i.e. your email) has previously been used to access Kaspersky Managed Detection and Response, it may be associated with another organization's MDR data and can be unavailable to apply a new activation code. To use your existing Kaspersky Account for the new activation, contact [Technical Support](#).

Please note: when Technical Support staff remove the association of your existing Kaspersky Account with another organization's data in MDR, your existing Kaspersky Account can no longer be used to access the other organization's data for which it was previously used.

1. In the MDR Console window, navigate to the **Settings** menu item.

The user list opens.

2. Click the **Add** button located above the user list.

The invitation card appears.

3. In the **Email** field, specify an email address.

4. In the **User role** field, specify a role for the new user.

The following user roles are available:

### MDR Administrator

The superuser who has access to all Kaspersky Managed Detection and Response functions granted by the license. The MDR Administrator can grant access to client data sources to other users. When you activate Kaspersky Managed Detection and Response, you become the MDR Administrator automatically, which is why we recommend using a corporate email address for the activation process instead of a personal email address. Having the MDR Administrator created with a personal email address can pose security risks, such as theft of the MDR Administrator account.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | ✓     | —    |
| Response management         | ✓     | —    |
| Tenant management           | ✓     | —    |
| Incident summary scheduling | ✓     | —    |
| REST API access             | ✓     | —    |

Only a user with the **MDR Administrator** [role](#) assigned can assign the **MDR Administrator** role to a new user.

## Senior Security Officer

An employee who has access to the Kaspersky Managed Detection and Response functions granted by the license, but who does not have access to the REST API. The Senior Security Officer has the right to accept and reject [responses](#) <sup>2</sup>.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | ✓     | —    |
| Response management         | ✓     | —    |
| Tenant management           | —     | ✓    |
| Incident summary scheduling | —     | ✓    |
| REST API access             | —     | ✓    |

## Security Officer

An employee who has access to the Kaspersky Managed Detection and Response functions granted by the license, but who does not have access to the REST API. The Security Officer cannot accept and reject [responses](#) <sup>2</sup>.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | —     | ✓    |
| Response management         | —     | ✓    |
| Tenant management           | —     | ✓    |
| Incident summary scheduling | —     | ✓    |
| REST API access             | —     | ✓    |

5. If necessary, select the value (or values) in the **Tenant** drop-down list.

Tenants that already exist and the **Root tenant** value are suggested.

The user can view only the assets and incidents related to the specified tenants. If you have assets and incidents not assigned to any tenants, the user can view them if you select the **Root tenant** value.

You can select the **Root tenant** value, in addition to specifying tenant names.

6. Click **Invite**.

The invitation card disappears.

Enter the email address. The email address must first be registered and verified on the [auth.hq.uis.kaspersky.com](https://auth.hq.uis.kaspersky.com) web portal.

A message with the invitation link is sent from noreply@mail.account.uis.kaspersky.com to the specified email address.

The invited user must verify his or her email address by following the link from the message. The user cannot log in and use Kaspersky Managed Detection and Response until their email is verified. Permissions corresponding to the user role will be granted after the first login of the user.

# Changing user roles in MDR Web Console

You can change the role for an existing user. For example, an employee with the Security Officer role is assigned additional responsibilities that require the Senior Security Officer role to be assigned.

*To change a role for an existing user:*

1. In the MDR Console window, navigate to the **Settings** menu item.

The user list opens.

2. Click the string containing the user whose role you want to change.

The user card appears.

3. In the user card, change the role for the existing user by selecting another role from the drop-down list of roles.

4. Click **Save**.

The role for the existing user is changed.

# Editing user notification methods in MDR Web Console

Editing user notification methods is available only for the user who has the MDR Administrator [role](#) assigned. The user with that role can edit notification settings for all users with the active status, including themselves.

Users with the active status can receive notifications from Kaspersky Managed Detection and Response via email and/or Telegram.

*To edit the user notification methods for an existing user:*

1. In the MDR Console window, navigate to the **Settings** menu item.

The user list opens.

2. Click the string containing the user whose notification methods you want to change.

The user card appears.

3. In the user card, specify the following options:

- **Email notifications enabled**

The user receives notifications to the email address specified when this user was invited.

- **Telegram notifications enabled**

The user receives notifications from the Telegram chatbot.

If a user has lost access to their Telegram account, select the **Unsubscribe Telegram account from notifications** check box. Then, ask the user to log in to MDR Web Console, go to **Settings → Notification settings**, and then repeat the subscription procedure to generate a new link in order to activate a Telegram subscription for another Telegram account.

4. In the lower part of the user card, click the **Save** button to close the card.

The user notifications methods are edited and saved.

## Editing user access to tenants in MDR Web Console

You can change user access to the tenants in your account, for example, if you add a new tenant and want an existing user to have access to it.

*To change access to tenants:*

1. In the MDR Console window, navigate to the **Settings** menu item.

The user list opens.

2. Click the string containing the user whose access rights you want to change.

The user card appears.

3. In the user card, change the value (or values) in the **Tenant** drop-down list.

4. In the lower part of the user card, click the **Save** button to close the card.

User access to tenants is changed.

## Deleting user accounts

Deleting user accounts is available in the MDR Console and on the Kaspersky website.

### Deleting MDR user accounts in the MDR Console

The MDR Administrator account is required to delete MDR user accounts.

The email associated with a deleted account stops receiving notifications and reports. To restore access to the MDR Console, [a new invite must be sent to the email](#).

When you only have a single MDR Administrator account, this account cannot be deleted.

*To delete an MDR user account:*

1. In the MDR Console window, navigate to the **Settings** menu item.

The user list opens.

2. In the user list, hover the mouse pointer over the user you want to delete, and click the trash bin icon on the right.

The **Confirm user deletion** window appears.

3. Click the **Delete** button to delete the user.

## Deleting Kaspersky Accounts

Users can delete their own Kaspersky Account on the Kaspersky website regardless of the assigned user rights.

Deleting a Kaspersky Account automatically deletes the corresponding MDR user account. The email associated with the deleted Kaspersky account stops receiving MDR notifications and reports.

If all MDR Administrator user accounts are deleted, adding new users and configuring the MDR Console can no longer be done. In this scenario, [contact Technical Support](#).

If you delete the Kaspersky Account that was used to configure the MDR Plug-in on the Administration Server or Open Single Management Platform, the MDR Plug-in needs to be reconfigured.

# Managing assets

An *asset* is a device with a Kaspersky EPP application installed (for example, Kaspersky Endpoint Security for Windows). This section provides information about viewing, sorting, and filtering assets.

## Viewing and searching assets in MDR Web Console

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

You can view and search through available assets by using the asset list.

*To view assets:*

1. In the MDR Web Console window, navigate to the **Assets** menu item.

The asset list opens. Each line represents one asset. You can click anywhere on the line to view asset information.

The following asset attributes are available to show above the list:

### **Asset name**

Network name of a computer.

You can click **Asset name** to view the asset information in Kaspersky Security Center Web Console.

### **Asset ID**

A unique identifier of an asset. An asset ID is generated automatically by Kaspersky Managed Detection and Response before the asset sends telemetry for the first time.

### **Applications**

An Endpoint Protection Platform (EPP) application that is installed on the asset and configured for use with Kaspersky Managed Detection and Response.

### **Interfaces**

Number of all available network interfaces of the device.

### **Operating system**

Operating system that is installed on the asset.

### **Domain**

Network domain that the asset belongs to.

### **Tenant**

Name of the [tenant](#), if the asset belongs to one of the tenants. If the asset does not belong to a tenant, this field is blank.

### **Last seen**

Number of days since the asset was last seen in MDR Web Console.

Assets are sorted according to this attribute, in descending order.

By default, assets that were seen in the last 30 days are shown. You can extend the time range by filtering assets.

## Status

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

The status reflects the current asset state. For assets in the *OK*, *Warning*, or *Critical* statuses, the application additionally lists the problems (if any) for the last 72 hours.

The assets have one of the following statuses:

- **OK** (green)

Telemetry is being sent, protection is fully operational.

- **Warning** (yellow)

Possible reasons of the **Warning** status:

- Minor telemetry losses. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- Anti-virus databases are outdated by more than 7 days.
- At least one of the following EPP application components on the asset is disabled or not installed:

### Firewall

The following articles describe how to enable or configure this component:

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

### Network Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) <sup>↗</sup>
- [Kaspersky Endpoint Security for Linux](#) <sup>↗</sup>
- [Kaspersky Endpoint Security for Mac](#) <sup>↗</sup>
- [Kaspersky Embedded Systems Security for Windows](#) <sup>↗</sup>
- [Kaspersky Embedded Systems Security for Linux](#) <sup>↗</sup>
- [Kaspersky Industrial CyberSecurity for Nodes](#) <sup>↗</sup>

### Mail Threat Protection and Additional Microsoft Office Outlook Extension

The following article describes how to enable or configure this component: [Kaspersky Endpoint Security for Windows](#) <sup>↗</sup>.

## Web Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) <sup>↗</sup>
- [Kaspersky Endpoint Security for Linux](#) <sup>↗</sup>
- [Kaspersky Endpoint Security for Mac](#) <sup>↗</sup>
- [Kaspersky Security for Virtualization Light Agent](#) <sup>↗</sup>
- [Kaspersky Embedded Systems Security for Linux](#) <sup>↗</sup>

## Product Self Defense

The following articles describe how to enable or configure this component:

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

These components affect the fullness of sent telemetry. If a component is disabled or missing, Kaspersky Managed Detection and Response does not send the telemetry events related to this component. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring. The application displays the expiration date. Consider [updating the KPSN configuration file](#). If you keep working with the current configuration file, the status changes to **Critical** few days before the expiration date.

The **Warning** status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization Light Agent 5.2 or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#) <sup>↗</sup>, this status is not displayed.

- **Critical** (red)

Possible reasons of the **Critical** status:

- Major telemetry losses, telemetry data is insufficient for analysis. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- At least one of the following EPP application components on the asset is disabled or not installed:
  - **System Watcher or Behavior Detection**

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) <sup>↗</sup>
- [Kaspersky Endpoint Security for Linux](#) <sup>↗</sup>

- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- **File Threat Protection**

The following articles describe how to enable or configure this component:

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

If any of these components are disabled or missing, Kaspersky Managed Detection and Response stops sending telemetry from the asset. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring soon or is already expired. The application displays the expiration date. Consider [updating the KPSN configuration file](#).

This status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization 5.2 Light Agent or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#) , this status is not displayed.

- **Offline** (black)

No telemetry for more than 7 days (default value). You can change the number of days of absence of telemetry, after which the **Offline** status is displayed for the asset, in the **Settings** section. The available range is 2–29 days.

If you see the **Offline** status for your assets:

- Make sure the EPP application components listed with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

**Offline** status is not applicable for VDI assets (temporary virtual machines).

- **Absent** (black)

No telemetry for more than 30 days for physical assets or for more than 24 hours for VDI assets (temporary virtual machines).

If you see the **Absent** status for your assets:

- Make sure the EPP application components with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

You can hide assets with the **Absent** status in the [asset list](#), in the [reports](#), and in the data received via the [API interface](#).

At the top of the incidents list, there are the following buttons:

- The **Columns** button with a gear icon, to select which columns to show on the **History** tab.
- The **Filter** button with a funnel icon, to show changes related only to the selected check boxes.
- The **Search** button with loupe icon, to show changes related only to the entered words or characters.

2. If you want to change the number of assets shown per page of the list, select the number by clicking the **entries per page** option at the bottom of the page.

You can select 10, 20, or 50 assets per page.

You can hide assets with the **Absent** status in the asset list by selecting the check box in the **Settings** → **General settings** tab.

If you want to navigate the list of assets, select the page from below the list. You can use the **Previous** and **Next** options to switch between adjacent pages.

By default, the asset list contains assets that were seen in MDR Web Console in the last 30 days.

To change this period:

1. Click the funnel icon above the list.
2. On the **Filter** panel on the right, select the period in the **Last seen** field.
3. Click **Save**.

You can search through the assets by clicking the magnifying glass icon located next to the funnel icon above the asset list.

## Filtering assets in MDR Web Console

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

You can create and apply filters to the asset list.

To create a filter for the asset list:

1. In MDR Web Console, navigate to the **Assets** menu item.

The asset list opens.

2. Click the funnel icon located above the asset list.

The **Filter** menu appears.

Parameters available for filtering are:

- **Last seen**

The moment when the asset was last seen in MDR Web Console.

- **Asset name**

Available asset names.

An asset name is the network name of a computer.

- **Tenant**

Available tenant names.

You can select the **Root tenant** value to view assets that are not assigned to any of your tenants.

You can select the **Root tenant** value in addition to specifying tenant names.

- **Status**

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

The status reflects the current asset state. For assets in the *OK*, *Warning*, or *Critical* statuses, the application additionally lists the problems (if any) for the last 72 hours.

The assets have one of the following statuses:

- **OK** (green)

Telemetry is being sent, protection is fully operational.

- **Warning** (yellow)

Possible reasons of the **Warning** status:

- Minor telemetry losses. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- Anti-virus databases are outdated by more than 7 days.
- At least one of the following EPP application components on the asset is disabled or not installed:

**Firewall**

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) <sup>↗</sup>
- [Kaspersky Security for Virtualization Light Agent](#) <sup>↗</sup>

- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

## Network Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

## Mail Threat Protection and Additional Microsoft Office Outlook Extension

The following article describes how to enable or configure this component: [Kaspersky Endpoint Security for Windows](#) .

## Web Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 

## Product Self Defense

The following articles describe how to enable or configure this component:

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

These components affect the fullness of sent telemetry. If a component is disabled or missing, Kaspersky Managed Detection and Response does not send the telemetry events related to this component. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring. The application displays the expiration date. Consider [updating the KPSN configuration file](#). If you keep working with the current configuration file, the status changes to **Critical** few days before the expiration date.

The **Warning** status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization Light Agent 5.2 or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#), this status is not displayed.

- **Critical** (red)

Possible reasons of the **Critical** status:

- Major telemetry losses, telemetry data is insufficient for analysis. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- At least one of the following EPP application components on the asset is disabled or not installed:

- **System Watcher or Behavior Detection**

The following articles describe how to enable or configure this component:

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

- **File Threat Protection**

The following articles describe how to enable or configure this component:

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

If any of these components are disabled or missing, Kaspersky Managed Detection and Response stops sending telemetry from the asset. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring soon or is already expired. The application displays the expiration date. Consider [updating the KPSN configuration file](#).

This status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization 5.2 Light Agent or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#), this status is not displayed.

- **Offline** (black)

No telemetry for more than 7 days (default value). You can change the number of days of absence of telemetry, after which the **Offline** status is displayed for the asset, in the **Settings** section. The available range is 2–29 days.

If you see the **Offline** status for your assets:

- Make sure the EPP application components listed with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

**Offline** status is not applicable for VDI assets (temporary virtual machines).

- **Absent** (black)

No telemetry for more than 30 days for physical assets or for more than 24 hours for VDI assets (temporary virtual machines).

If you see the **Absent** status for your assets:

- Make sure the EPP application components with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

You can hide assets with the **Absent** status in the [asset list](#), in the [reports](#), and in the data received via the [API interface](#).

- **Isolation**

Whether network isolation is enabled or not. The possible filter values are:

- **Isolated**

Network isolation is enabled.

- **Not isolated**

Network isolation is disabled.

3. Click **Save** to apply the created filter.

Only assets that meet the selected parameters of the filter are shown in the asset list after the filter is applied.

You can hide assets with the **Absent** status in the asset list by selecting the check box in the **Settings** → **General settings** tab.

# Viewing detailed information about assets in MDR Web Console

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

*To view detailed information about assets:*

1. In the MDR Web Console window, navigate to the **Assets** menu item.

The asset list opens.

2. Click the string with the asset whose details you want to view.

The asset card appears. The asset card contains two tabs:

- **Properties** has general information about the asset
- **Incidents** has information on incidents that have occurred with the asset

General information on the **Properties** tab contains the following information:

- **Asset name**

Network name of a computer.

You can click **Asset name** to view the asset information in Kaspersky Security Center Web Console.

- **Status**

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

The status reflects the current asset state. For assets in the *OK*, *Warning*, or *Critical* statuses, the application additionally lists the problems (if any) for the last 72 hours.

The assets have one of the following statuses:

- **OK** (green)

Telemetry is being sent, protection is fully operational.

- **Warning** (yellow)

Possible reasons of the **Warning** status:

- Minor telemetry losses. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- Anti-virus databases are outdated by more than 7 days.
- At least one of the following EPP application components on the asset is disabled or not installed:

## Firewall

The following articles describe how to enable or configure this component:

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

## Network Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

## Mail Threat Protection and Additional Microsoft Office Outlook Extension

The following article describes how to enable or configure this component: [Kaspersky Endpoint Security for Windows](#) .

## Web Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 

## Product Self Defense

The following articles describe how to enable or configure this component:

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

These components affect the fullness of sent telemetry. If a component is disabled or missing, Kaspersky Managed Detection and Response does not send the telemetry events related to this component. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring. The application displays the expiration date. Consider [updating the KPSN configuration file](#). If you keep working with the current configuration file, the status changes to **Critical** few days before the expiration date.

The **Warning** status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization Light Agent 5.2 or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#), this status is not displayed.

- **Critical (red)**

Possible reasons of the **Critical** status:

- Major telemetry losses, telemetry data is insufficient for analysis. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- At least one of the following EPP application components on the asset is disabled or not installed:

- **System Watcher or Behavior Detection**

The following articles describe how to enable or configure this component:

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

- **File Threat Protection**

The following articles describe how to enable or configure this component:

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

If any of these components are disabled or missing, Kaspersky Managed Detection and Response stops sending telemetry from the asset. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring soon or is already expired. The application displays the expiration date. Consider [updating the KPSN configuration file](#).

This status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization 5.2 Light Agent or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#)<sup>2</sup>, this status is not displayed.

- **Offline** (black)

No telemetry for more than 7 days (default value). You can change the number of days of absence of telemetry, after which the **Offline** status is displayed for the asset, in the **Settings** section. The available range is 2–29 days.

If you see the **Offline** status for your assets:

- Make sure the EPP application components listed with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

**Offline** status is not applicable for VDI assets (temporary virtual machines).

- **Absent** (black)

No telemetry for more than 30 days for physical assets or for more than 24 hours for VDI assets (temporary virtual machines).

If you see the **Absent** status for your assets:

- Make sure the EPP application components with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

You can hide assets with the **Absent** status in the [asset list](#), in the [reports](#), and in the data received via the [API interface](#).

- **IP address**

The IP address of the asset.

- **Physical address**

- **Tenant**

Name of the [tenant](#), if the asset belongs to one of the tenants. If the asset does not belong to a tenant, this field is blank.

- **First seen**

- **Last seen**

- **Operating system**

Operating system that is installed on the asset.

- **Kaspersky applications that work with MDR**

- **Domain**

The **Incidents** tab contains the list of incidents. The **ID/Created** column of the list contains an incident identifier and time the incident was created. The **Status** column of the list contains information on the incident status.

## Asset statuses

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

The status reflects the current asset state. For assets in the *OK*, *Warning*, or *Critical* statuses, the application additionally lists the problems (if any) for the last 72 hours.

The assets have one of the following statuses:

- **OK** (green)

Telemetry is being sent, protection is fully operational.

- **Warning** (yellow)

Possible reasons of the **Warning** status:

- Minor telemetry losses. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- Anti-virus databases are outdated by more than 7 days.
- At least one of the following EPP application components on the asset is disabled or not installed:

### Firewall

The following articles describe how to enable or configure this component:

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

### Network Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) <sup>↗</sup>
- [Kaspersky Endpoint Security for Linux](#) <sup>↗</sup>

- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Embedded Systems Security for Windows](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

### Mail Threat Protection and Additional Microsoft Office Outlook Extension

The following article describes how to enable or configure this component: [Kaspersky Endpoint Security for Windows](#) .

### Web Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 

### Product Self Defense

The following articles describe how to enable or configure this component:

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

These components affect the fullness of sent telemetry. If a component is disabled or missing, Kaspersky Managed Detection and Response does not send the telemetry events related to this component. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring. The application displays the expiration date. Consider [updating the KPSN configuration file](#). If you keep working with the current configuration file, the status changes to **Critical** few days before the expiration date.

The **Warning** status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization Light Agent 5.2 or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#) , this status is not displayed.

- **Critical** (red)

Possible reasons of the **Critical** status:

- Major telemetry losses, telemetry data is insufficient for analysis. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- At least one of the following EPP application components on the asset is disabled or not installed:
  - **System Watcher or Behavior Detection**

The following articles describe how to enable or configure this component:

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

- **File Threat Protection**

The following articles describe how to enable or configure this component:

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

If any of these components are disabled or missing, Kaspersky Managed Detection and Response stops sending telemetry from the asset. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring soon or is already expired. The application displays the expiration date. Consider [updating the KPSN configuration file](#).

This status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization 5.2 Light Agent or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#) , this status is not displayed.

- **Offline** (black)

No telemetry for more than 7 days (default value). You can change the number of days of absence of telemetry, after which the **Offline** status is displayed for the asset, in the **Settings** section. The available range is 2–29 days.

If you see the **Offline** status for your assets:

- Make sure the EPP application components listed with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

**Offline** status is not applicable for VDI assets (temporary virtual machines).

- **Absent** (black)

No telemetry for more than 30 days for physical assets or for more than 24 hours for VDI assets (temporary virtual machines).

If you see the **Absent** status for your assets:

- Make sure the EPP application components with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

You can hide assets with the **Absent** status in the [asset list](#), in the [reports](#), and in the data received via the [API interface](#).

## Checking assets status in Kaspersky Security Center

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

You can check the status of your assets by using the MDR asset statuses functionality. It enables you to check which assets are currently protected by Kaspersky Managed Detection and Response and which ones never sent [telemetry](#) to Kaspersky Managed Detection and Response.

For assets with Kaspersky Endpoint Security for Windows 12.3 or later working in the [Endpoint Detection and Response Agent \(EDR Agent\) configuration](#), the displayed status in MDR does not reflect the actual status.

Statuses of the assets that have sent telemetry at least once

*To check the assets status:*

1. In the **MDR** section of Kaspersky Security Center, navigate to the **MDR Asset statuses** tab.
2. Select the **All assets ever seen** tab.

A list of all assets that have sent telemetry to Kaspersky Managed Detection and Response at least once is displayed.

The following details are displayed for each asset:

## Status

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

The status reflects the current asset state. For assets in the *OK*, *Warning*, or *Critical* statuses, the application additionally lists the problems (if any) for the last 72 hours.

The assets have one of the following statuses:

- **OK** (green)

Telemetry is being sent, protection is fully operational.

- **Warning** (yellow)

Possible reasons of the **Warning** status:

- Minor telemetry losses. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- Anti-virus databases are outdated by more than 7 days.
- At least one of the following EPP application components on the asset is disabled or not installed:

### Firewall

The following articles describe how to enable or configure this component:

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

### Network Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) <sup>↗</sup>
- [Kaspersky Endpoint Security for Linux](#) <sup>↗</sup>
- [Kaspersky Endpoint Security for Mac](#) <sup>↗</sup>
- [Kaspersky Embedded Systems Security for Windows](#) <sup>↗</sup>
- [Kaspersky Embedded Systems Security for Linux](#) <sup>↗</sup>
- [Kaspersky Industrial CyberSecurity for Nodes](#) <sup>↗</sup>

### Mail Threat Protection and Additional Microsoft Office Outlook Extension

The following article describes how to enable or configure this component: [Kaspersky Endpoint Security for Windows](#) <sup>↗</sup>.

### Web Threat Protection

The following articles describe how to enable or configure this component:

- [Kaspersky Endpoint Security for Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security for Mac](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security for Linux](#) 

## Product Self Defense

The following articles describe how to enable or configure this component:

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

These components affect the fullness of sent telemetry. If a component is disabled or missing, Kaspersky Managed Detection and Response does not send the telemetry events related to this component. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring. The application displays the expiration date. Consider [updating the KPSN configuration file](#). If you keep working with the current configuration file, the status changes to **Critical** few days before the expiration date.

The **Warning** status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization Light Agent 5.2 or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#) , this status is not displayed.

- **Critical** (red)

Possible reasons of the **Critical** status:

- Major telemetry losses, telemetry data is insufficient for analysis. Refer to this article: [How to avoid loss of telemetry data from assets](#).
- At least one of the following EPP application components on the asset is disabled or not installed:

- **System Watcher or Behavior Detection**

The following articles describe how to enable or configure this component:

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

- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security for Virtualization Light Agent](#) 

- **File Threat Protection**

The following articles describe how to enable or configure this component:

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

If any of these components are disabled or missing, Kaspersky Managed Detection and Response stops sending telemetry from the asset. The installed EPP application may not include all of the listed components.

- KPSN configuration file is expiring soon or is already expired. The application displays the expiration date. Consider [updating the KPSN configuration file](#).

This status is applicable for assets with Kaspersky Endpoint Security for Windows 11 or later, Kaspersky Endpoint Security for Linux 11.2 or later, Kaspersky Endpoint Security for Mac 11.2 or later, or Kaspersky Security for Virtualization 5.2 Light Agent or later installed. For assets with the [Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent \(EDR Agent\) configuration](#) , this status is not displayed.

- **Offline** (black)

No telemetry for more than 7 days (default value). You can change the number of days of absence of telemetry, after which the **Offline** status is displayed for the asset, in the **Settings** section. The available range is 2–29 days.

If you see the **Offline** status for your assets:

- Make sure the EPP application components listed with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

**Offline** status is not applicable for VDI assets (temporary virtual machines).

- **Absent** (black)

No telemetry for more than 30 days for physical assets or for more than 24 hours for VDI assets (temporary virtual machines).

If you see the **Absent** status for your assets:

- Make sure the EPP application components with **Warning** and **Critical** statuses are installed and enabled on the assets.
- Make sure Kaspersky Managed Detection and Response is [properly deployed](#) in your infrastructure.

You can hide assets with the **Absent** status in the [asset list](#), in the [reports](#), and in the data received via the [API interface](#).

### Asset name

Network name of a computer.

You can click **Asset name** to view the asset information in Kaspersky Security Center Web Console.

### Asset ID

A unique identifier of an asset. An asset ID is generated automatically by Kaspersky Managed Detection and Response before the asset sends telemetry for the first time.

### Domain

Network domain that the asset belongs to.

### OS version

Operating system that is installed on the asset.

### EPP applications

An Endpoint Protection Platform (EPP) application that is installed on the asset and configured for use with Kaspersky Managed Detection and Response.

### Interfaces

Number of all available network interfaces of the device.

### Tenant

Name of the [tenant](#), if the asset belongs to one of the tenants. If the asset does not belong to a tenant, this field is blank.

### Last seen

Number of days since the asset was last seen in MDR Web Console.

Assets are sorted according to this attribute, in descending order.

By default, assets that were seen in the last 30 days are shown. You can extend the time range by filtering assets.

3. Use the following sorting and filtering options to work with this list:

- Click any column header to sort the list by the selected column values.
- Click the **Status** column, and then select the required statuses. The list will be filtered to show only the assets with the selected statuses.
- Click **Filter** and then select the time period to view only those assets that were last seen during the selected time period. You can also specify a custom time period.

- Click **Export** above the asset list to make a CSV export.
- Use the **Search** field to search for assets by name.

## Statuses of the assets that never sent telemetry

This feature is working properly in Kaspersky Security Center 15.1 Windows or later versions, Kaspersky Security Center 15.1 Linux or later versions, and Kaspersky Next Expert View.

*To view the assets that never sent telemetry:*

1. In the **MDR** section of Kaspersky Security Center, navigate to the **MDR Asset statuses** tab.
2. Select the **Failed to get the state of assets** tab.

The MDR Web Console displays a list of the assets that have been added to Kaspersky Security Center, but never sent telemetry to Kaspersky Managed Detection and Response.

The following details are displayed for each asset:

- **Asset name**

Network name of a computer.

You can click **Asset name** to view the asset information in Kaspersky Security Center Web Console.

- **EPP applications**

An Endpoint Protection Platform (EPP) application that is installed on the asset and configured for use with Kaspersky Managed Detection and Response.

- **MDR state**

The MDR component of an EPP application installed on an asset can have one of the following statuses:

- *Unknown*—Unlike other statuses, the *Unknown* status is not sent by applications. This option shows that the applications have no information about the selected component status. For example, this can happen when the selected component does not belong to any of the applications installed on the device, or when the device is turned off.
- *Stopped*—The component is disabled and not working at the moment.
- *Paused*—The component is suspended, for example, after the user has paused protection in the managed application.
- *Starting*—The component is currently in the process of initialization.
- *Running*—The component is enabled and working properly.
- *Failed*—An error has occurred during the component operation.

- *Not installed*—The user did not select the component for installation when configuring custom installation of the application.

- *No license*—The license that covers the MDR functionality is missing or expired.

- **KSC Server**

Name of the Kaspersky Security Center Administration Server that manages the selected asset.

- **State of critical components**

A list of EPP application components critical for MDR operation. Each component has color indication depending on the component status:

- Yellow indication is used when the component has one of the following statuses: **Paused**, **Starting**, or **Unknown**.
- Red indication is used when the component has one of the following statuses: **Stopped**, **Failed**, **No license**, or **Not installed**.

Also, the [Self-Defense feature](#) is listed along with the EPP application components. If this feature is disabled, it has red indication too.

- The components that have the **Running** status are not listed in the table and have no indication.

To view the complete list of components, including those not critical for MDR operation, click the asset name. The components and their statuses will be displayed in the asset details window.

3. If necessary, you can filter the assets by MDR status. To do so, click **Filter**, and then select the required MDR statuses. The MDR Web Console will display only those assets on which the MDR component has one of the selected MDR statuses. Alternatively, select one of the following options:

- **Installed and activated**—The list will be filtered to display the assets that have one of the following MDR statuses: *Unknown*, *Stopped*, *Paused*, *Starting*, *Running*, or *Failed*.
- **License is missing or expired**—The list will be filtered to display the assets that have the *No license* MDR status.

4. If necessary, click the **Export** button to export the asset list to a CSV file.

## How to avoid loss of telemetry data from assets

We recommend using the latest versions of Kaspersky applications and solutions to ensure the best protection and get full access to new features and updates.

Assets [send telemetry data](#) to Kaspersky Managed Detection and Response to detect and analyze security incidents in your infrastructure. If you see that there are telemetry losses in the [asset status](#), make sure the following instructions are completed:

1. The recommended versions of Kaspersky applications are installed on your assets (see *Recommended versions and their term of support* column in the *Compatible Kaspersky applications versions* section of [Hardware and software requirements](#)).

2. Your network channel throughput meets the specifications provided in the *Network channel* section of [Hardware and software requirements](#).

3. Your [KSN proxy server](#) <sup>↗</sup> provides sufficient throughput capacity.

If there are issues with the KSN proxy server throughput capacity, disable the KSN proxy in the [KSC policy](#) <sup>↗</sup>, to force the assets to connect to KSN directly:

a. In the Kaspersky Security Center main menu, go to **Devices** → **Policies & profiles**.

b. Click the policy for Kaspersky Endpoint Security for Windows, Linux, or Mac. The properties window of the selected policy opens.

c. In the policy properties, click **Application settings** → **Advanced Threat Protection** → **Kaspersky Security Network**.

d. Enable the **Use KSN servers when KSN Proxy is not available** option (if applicable for the policy).

e. Click **OK**.

4. KSN Proxy is enabled on the distribution point side in [Kaspersky Next Expert View](#) <sup>↗</sup> or Kaspersky Security Center [Web Console](#) <sup>↗</sup> to optimize the network load.

5. Your Kaspersky Security Center Administration Server workload does not exceed the [limitations](#) <sup>↗</sup>.

6. The recommended version of Kaspersky Security Center specified in [Hardware and software requirements](#) is used, latest available hotfixes and patches are installed.

# Managing incidents

An *incident* is an activity evaluated as critical by the detection technology and which requires immediate reaction from the online service. This section provides information about managing existing incidents and adding new incidents.

You can manage incidents in [MDR Web Console](#).

To manage the incidents in MDR Web Console, you should create a [Kaspersky Account](#) and ask your [MDR administrator](#) (the user of MDR Web Console with **MDR Administrator** role) to [invite you in MDR Web Console](#) by using the email address you use for your Kaspersky Account. Then, you receive the invitation email containing the link to MDR Web Console.

The MDR solution offers response actions, which you can [process manually](#) or [configure auto-acceptance](#).

You can configure integrations with [KUMA](#) and [XDR](#), which allows MDR to process data from these platforms.

## About the incidents

### What is an incident

In the context of information security, an incident is any unforeseen or undesirable event that could disrupt normal activity or information security.

An event is the identified external signs of a particular state of a system, service, or network.

Within the framework of the Kaspersky MDR solution, the main criterion for deciding whether the observed activity is an incident is the ability to implement efficient measures to counter, prevent, or reduce possible damage resulting from this activity. See the table below for examples of possible incident criteria and responsive measures depending on the event source.

Examples of incident detection criteria and response measures

| Event source              | Possible incident criteria                                                                                                                                                                                                                                                                                                                                   | Possible incident responses                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Endpoint device           | <ul style="list-style-type: none"><li>• The active phase of an attack that was not prevented automatically</li><li>• Evidence of malicious persistence in the system</li><li>• Indicators of past incidents</li><li>• Indicators of internal intruder activity on the customer's side (including cases when the attack was successfully prevented)</li></ul> | <ul style="list-style-type: none"><li>• Issue detection by means of AO Kaspersky Lab solutions installed on endpoint devices, and assessment of automatic response efficiency (if technically possible)</li><li>• Recommended manual response actions</li><li>• Requested automatic response actions</li><li>• Recommendations for raising the users' information security awareness</li></ul>                        |
| Endpoint device + network | Security event from a supported network detection technology that has been confirmed on the endpoint device                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"><li>• Issue detection by means of AO Kaspersky Lab solutions installed on endpoint devices, as well as AO Kaspersky Lab solutions for network traffic monitoring, and assessment of automatic response efficiency (if technically possible)</li><li>• Recommended manual response actions</li><li>• Requested automatic response actions</li><li>• Informing the customer</li></ul> |

## Incident detection scenarios

### *Scenario 1. Incident detection by the Kaspersky MDR solution*

In this scenario, an information security incident is detected as a result of the Kaspersky MDR operation. The incident is logged automatically in the incidents tracking system. The default incident priority level can be changed later, but it will require to specify the reason of the change according to the incident priority level table (see below). Kaspersky MDR processes the logged incidents to promptly obtain information about the status of the customer's IT infrastructure.

If root causes of the incident are identified as a result of the analysis, then response recommendations are provided to the customer. If there is not enough information to identify the root cause of the incident, all the available information and the results of analysis are provided to the customer for independent research.

### *Scenario 2. Incident detection by the customer (creating custom incidents is not available in some of the [commercial license tiers](#))*

In this scenario, an information security incident is detected by the customer, independently from the Kaspersky MDR operation. If the incident needs to be processed by Kaspersky MDR, the customer may log the incident manually and provide all the available information about the detected incident by using the Kaspersky MDR features. By default, the incident priority level is set to **Low**, unless specified otherwise by the customer while logging the incident.

Further processing of the incident is similar to Scenario 1.

## Incident priority levels

Incident priority levels and their descriptions

| Incident priority level | Description                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>High</b>             | Incidents that, in AO Kaspersky Lab expert opinion, may result in major disruptions or unauthorized access to the customer's assets monitored by Kaspersky MDR.<br>For example, identified traces of a targeted attack or of an unknown threat, requiring further investigation by using digital forensic methods. |
| <b>Medium</b>           | Incidents that, in AO Kaspersky Lab expert opinion, may affect the efficiency or performance of the customer's assets monitored by Kaspersky MDR, or may result in a one-time data corruption.                                                                                                                     |
| <b>Low</b>              | Incidents that, in AO Kaspersky Lab expert opinion, do not significantly affect the efficiency or performance of the customer's assets monitored by Kaspersky MDR.<br>For example, identified potentially unwanted software such as adware or riskware.                                                            |

The default incident priority level is **Low**.

## Performance targets of the solution delivery

Target reaction time and value of Kaspersky MDR delivery depending on the incident priority

| Incident priority level | Reaction time* | Target value** |
|-------------------------|----------------|----------------|
| High                    | 1 hour         | 90%            |
| Medium                  | 4 hours        | 90%            |
| Low                     | 24 hours       | 90%            |

The incident is considered as resolved if recommendations of response measures were provided to the customer.

\*Reaction time is the time between incident detection (creation time) and publishing it to MDR Web Console (update time).

\*\*Target value is the percentage of incidents where the reaction time meets the objective specified in the table.

## Viewing and searching incidents in MDR Web Console

*To view incidents:*

1. In the MDR Web Console, navigate to the **Incidents** menu item.

The incident list opens. Each line represents one incident. You can click anywhere on the line to view incident information.

The following incident attributes are present above the list:

- **ID/Created**—Numeral identifier of the incident in the Console / date the incident was created.
- **Status**—One of the following incident statuses:
  - **Open**—The incident has to be processed by the security team.
  - **Resolved**—The incident received a response created by the security team.
  - **On hold**—The incident has temporarily stopped being processed by the security team.
  - **Closed**—The incident was processed by the security team and no more work needs to be done on it.
- **Summary**—Brief commentary about the whole incident.
- **Tenant**—A tenant that an incident is assigned to.
- **Updated**—Date and time when the incident was updated.

Incidents are sorted according to their update time in descending order.

At the top of the incidents list, there are the following buttons:

- The **Columns** button with a gear icon, to select which columns to show on the **History** tab.
- The **Filter** button with a funnel icon, to show changes related only to the selected check boxes.
- The **Search** button with loupe icon, to show changes related only to the entered words or characters.

2. If you want to change the number of incidents shown per page of the list, select a number by clicking the **entries per page** option in the lower part of the page. You can select 10, 20, or 50 incidents per page.

To navigate the list of incidents, select a page from below the list. You can use the **Previous** and **Next** options to switch between adjacent pages.

In order to [filter the incidents](#), click the funnel icon above the list.

You can search through the incidents by clicking the magnifying glass icon located next to the funnel icon above the incident list.

## Filtering incidents in MDR Web Console

To view specific incidents, you can create and apply filters to the incident list.

*To create a filter for the incident list:*

1. In MDR Web Console, click the **Incidents** menu item.

The incident list opens.

2. Click the funnel icon located above the incident list.

The **Filter** block appears.

Parameters available for filtering are:

- **Created**  
Time period for incident creation.
- **Updated**  
Time period for incident update.
- **Priority**  
Incident priority. Available priorities are Low, Medium, and High.
- **Status**  
Incident status.
- **Resolution**  
Resolution for incident.
- **Assets**  
Available assets.

- **Tenant**

Available tenant names.

You can select the **Root tenant** value to view incidents that are not assigned to any of your tenants.

You can select the **Root tenant** value in addition to specifying tenant names.

- **Tactics**

Available MITRE tactics for incident response.

- **Response statuses**

Show only incidents with the selected statuses of corresponding responses.

3. Click **Save** to apply the created filter. Click **Clear** to discard the created filter.

Only incidents that meet the selected parameters of the filter are shown in the incident list after the filter is applied.

## Creating custom incidents in MDR Web Console

Creating custom incidents is not available in some of the [commercial license tiers](#).

If you consider some activity in your infrastructure to be a threat but Kaspersky Managed Detection and Response did not create an incident automatically, you can add a new incident manually.

According to the terms of the service level agreement (SLA), the number of manually created incidents that are eligible for processing by the security team is limited. Information about the limitations is available on the [MDR Usage tab in Kaspersky Security Center](#). On this tab, you can track the usage of the manually created incidents for the current period (for example, for the current week):

- The total number incidents that you can create for the current period. These incidents are to be processed by the security team, according to the SLA. You can create more incidents than specified in the MDR Agreement, but compliance with the SLA time frames is not guaranteed for processing of such incidents.
- The remaining number of incidents that you can create for the current period.

*To add a new incident:*

1. In the MDR Web Console window, navigate to the **Incidents** menu item.

The incident list opens.

2. In the upper part of the window, click the **Add** button.

The new incident block appears.

3. Fill in the following fields:

- **Summary**

A brief commentary about the incident.

- **Description**

Free-form detailed information about the incident. Markdown is supported

- **Assets**

The asset(s) compromised in the incident. For this field, assets that already exist in MDR Web Console and Kaspersky Security Center are suggested.

4. If necessary, fill in the **Tenant** field.

For the **Tenant** field, tenants that already exist and the **Root without tenants** value are suggested.

5. Click the **Send** button.

The new incident block disappears.

The new incident is added to the incident list in MDR Web Console. You can view detailed information about this incident and the processing responses to it.

## Viewing detailed information about incidents in MDR Web Console

*To view detailed information about incidents:*

1. In the MDR Web Console window, navigate to the **Incidents** menu item.

The incident list opens.

2. Click the string with the incident whose details you want to view.

The incident page opens.

The page title contains an incident identifier. Below the title there are four tabs:

- **Summary**

Contains general information on the incident.

- **Responses**

Contains information on responses to the incident.

- **Communication**

Contains information on communication and files related to the incident.

- **History**

Contains information on the incident changes.

General information on the **Summary** tab starts with a brief incident summary. Additional information listed in this section includes:

- Incident priority
- Incident status
- Incident resolution

- Timestamps of the incident create time and update time
- MITRE Tactics
- MITRE Techniques
- Detection technology

Below the incident summary, the following information is listed:

- **Affected assets**
- **Asset-based IOCs**
- **Network-based IOCs**

General information on the **Summary** tab concludes with a client description and a **Close incident** button.

3. If you know that the incident is a duplicate or you are not going to solve it, click the **Close incident** button.
4. If necessary, [send the incident to IR Retainer](#) for investigation and elimination of possible consequences.
5. Refer to the **Responses** tab to view information on response requests.

The information on the **Responses** tab is presented as a list. The columns of the list are:

- **Status**
- **Asset ID**
- **Type**
- **Details**
- **Comment**
- **Changed by**
- **Update time**

6. If you want to add a comment to an incident:

- a. On the **Communication** tab of the incident details page, type your comment in the text field.  
Markdown and attaching files are supported. The maximum file size is 10 MB.

- b. Click the **Send** button.

The comment is added to the **Communication** tab on the incident details page. You can edit or delete your comment within 10 minutes after you post it.

7. Refer to the **History** tab to view information on the incident changes.

Below the title there is a switch for showing changes related to:

- **All events**
- **Only incidents**

- **Only responses**
- **Only communication**

Next to this switch, there are the following buttons:

- The **Columns** button with a gear icon, to select which columns to show on the **History** tab.
- The **Filter** button with a funnel icon, to show changes related only to the selected check boxes.
- The **Search** button with loupe icon, to show changes related only to the entered words or characters.

## Processing responses to incidents in MDR Web Console

You can view, accept, and reject [responses](#) to incidents.

*To view responses to an incident:*

1. In the MDR Web Console window, navigate to the **Incidents** menu item.

The incident list opens.

2. Click the string with the incident whose details you want to view.

The incident page opens.

3. On the incident page, click the **Responses** tab.

The response list opens.

Each line represents one response. The following information about the response is displayed:

- **Status**  
Status of the response.
- **Asset ID**  
Identifier of the asset for the response to be executed.
- **Type**  
Type of the object that makes up the response.
- **Parameters**  
OS-specific local path to get the response file and expected file size in MB. The maximum file size is 10 MB.
- **Comment**  
Last comment to the response.
- **Changed by**  
Last user who modified the response description.

To view the response description, click on the string with the response.

*To accept or reject responses to an incident:*

1. In the Console window, navigate to the **Incidents** menu item.

The incident list opens.

2. Click the string with the incident whose details you want to view.

The incident page opens.

3. On the incident page, click the **Responses** tab.

The response list opens.

4. Select a response that you want to approve or reject by selecting the check box at the left end of the string that contains response.

You can also select several responses by selecting their check boxes at the left. To select all responses, select the check box at the left part of response table heading.

5. To approve or reject a response or responses, select either the **Accept** or **Reject** button located below the response list. The comment box appears. Enter your comment, and then click the **Send** button.

You can also click a response on the **Responses** tab to check its details and either accept or reject it in the side pane that appears. To reject the response, you have to enter your comment in the field on the side pane.

The response status is changed.

## Response types

The MDR solution examines incidents and creates responses that you can either accept or reject. This is the default way of how incidents are handled in Kaspersky Managed Detection and Response.

However, you can manually create responses by [using the Kaspersky Endpoint Detection and Response Optimum features](#).

This article only describes the types of responses created by the MDR solution.

Each response can have a set of parameters that are present on the **Responses** tab of an incident.

The available response types are:

- **Get file**

Copying a file from your infrastructure to Kaspersky SOC. If you accept this response, the specified file will be copied to Kaspersky SOC.

Note that this response type can obtain files containing personal and/or confidential data.

The possible parameters are:

- **Infected file path**

The absolute file path. For example, C:\\file.exe.

- **Maximum file size**

The maximum file size, in MB.

If the infected file exceeds the specified maximum file size, the attempt to accept the response will fail and the response will not be performed, but will appear on the **History** tab of an incident.

- **Isolate**

Isolating the specified asset from the network.

In case you need to disable network isolation urgently, please [contact technical support](#) or write a request on the **Communication** tab of the incident.

The possible parameters are:

- **Password for disabling isolation**

The password for disabling isolation. Once technical support receives your request for disabling network isolation, they will send you the procedure with details on using the password.

- **Task ID**

The unique task identifier that is used in conjunction with **Password for disabling isolation**, for disabling network isolation manually.

- **Password details**

You can check the **Password** validity by generating a derived key from it and comparing the resulting value with the value in the **Derived key** parameter.

- **Version**

The numeric version of the password creation rules. A version of 1 means that the following parameters of PBKDF2 are applied for creating a derived key:

- HMACSHA256 hash algorithm
    - 10,000 iterations
    - Key length of 32 bytes

- **Salt**

The salt in HEX format for obtaining a derived key via PBKDF2.

- **Derived key**

The derived key in HEX format.

- **Exclude rules**

Array of rules with the custom ports, protocols, IP addresses, and processes that isolation is not applied to.

- **Direction**

The traffic direction. The possible values are: **Inbound**, **Outbound**, **Both**.

- **Protocol**

The protocol number according to the [IANA specification](#) <sup>1</sup>.

The possible values are:

- **1** (ICMP)
- **6** (TCP)
- **17** (UDP)
- **58** (IPv6-ICMP)

- **Remote port range**

The range of remote ports specified in the nested **From** and **To** fields.

- **Remote IPv4 address**

The remote IPv4 address or subnet mask.

- **Remote IPv6 address**

The remote IPv6 address or subnet mask.

- **Local port range**

The range of local ports specified in the nested **From** and **To** fields.

- **Local IPv4 address**

The local IPv4 address or subnet mask.

- **Local IPv6 address**

The local IPv6 address or subnet mask.

- **Process**

The path to the process image specified in the nested **Image** → **Path** field.

- **Disable isolation**

Disable network isolation of the specified asset.

- **Delete registry key**

Delete a registry key or a registry branch on the specified asset.

This action cannot be undone.

The possible parameters are:

- **Key**

The absolute key path, which starts with HKEY\_LOCAL\_MACHINE or HKEY\_USERS. For example, HKEY\_LOCAL\_MACHINE\\SYSTEM\\WebClient.

If the key is a symbolic link, only this key will be deleted while the link's target key will remain intact.

- **Value**

The key value.

If this parameter is not specified, the key will be deleted recursively. During recursive deleting, each subkey that is a symbolic link will be deleted while its target key will remain intact.

If the key value is an empty string, the default value will be deleted.

- **Memory dump**

Creating a memory dump and sending it to Kaspersky SOC.

The possible parameters are:

- **Dump type**

A memory dump can be one of two types:

- **Full memory dump**

A dump of the entire memory of an asset.

- **Process dump**

A dump of a specified process.

- **Maximum file size**

The maximum file size for the dump in ZIP format, in MB. The default value is 100 MB.

- **Process**

The process ID and image details.

- **Image**

- **Path**

The absolute file path. For example, %systemroot%\system32\svchost.exe.

- **SHA-256**

The SHA256 checksum in HEX format.

- **MD5**

The MD5 checksum in HEX format.

- **Unique ID**

The unique process identifier.

- **Process count limit**

The maximum number of processes that can be contained within the dump file.

- **Terminate process**

Terminate a process on the specified asset with Kaspersky Endpoint Security for Windows. The process to be terminated can be specified by its name or process identifier (PID).

- **Run process**

Run a script on the specified asset with Kaspersky Endpoint Security for Windows.

For this response to work, the PowerShell component must be installed on the asset. You can view the script to be run and its description in [MDR Web Console](#).

- **Quarantine file**

Places a potentially dangerous file in a special local storage. The files in this storage are stored encrypted and do not threaten the security of the device. The confirmation request specifies the asset, the path to the file and the hash of the file (MD5 or SHA256).

- **Restore file from quarantine**

Restores the previously quarantined file to its original location. If there is a file with the same name in the original location, restoring is not performed.

- **Get artefacts**

In this type of response action, files containing personal and confidential data may be transmitted.

Available if you have configured integration with Kaspersky Anti Targeted Attack version 8.0 or later

Copies files related to Kaspersky Anti Targeted Attack alerts from the Kaspersky Anti Targeted Attack infrastructure to Kaspersky SOC. The copied files are used by MDR SOC analysts to investigate Kaspersky Anti Targeted Attack alerts.

The possible parameters are:

- Kaspersky Anti Targeted Attack solution node ID.
- Kaspersky Anti Targeted Attack alert ID.
- File categories to copy to Kaspersky SOC that are related to the alerts:
  - PCAP and Payload files related to an IDS alert.
  - Report on the result of file scanning in Sandbox. Includes screenshots of object execution, activity log, and other scan data.
  - The infected file that was sent to Sandbox.
  - File that contains alert details.

Available if you have configured integration with Kaspersky Next XDR Expert 2.1

Copies files related to alerts or incidents from Kaspersky Endpoint Detection and Response Expert within the Open Single Management Platform infrastructure to Kaspersky SOC. The copied files are used by MDR SOC analysts to investigate Kaspersky Endpoint Detection and Response Expert alerts and incidents.

The possible parameters are:

- Solution node ID.
- XDR alert or incident ID.
- File categories to copy to Kaspersky SOC that are related to the alerts or incidents:
  - Files uploaded to the XDR alert or incident.
  - Report on the result of file scanning in Sandbox. Includes screenshots of object execution, activity log, and other scan data.
  - The infected file that was sent to Sandbox.
  - Files related to user response actions for the alert or incident:
    - File retrieval
    - Forensic collection
    - Registry key acquisition
    - NTFS filesystem service file retrieval
    - Process memory dump acquisition
    - File quarantining
- Details about all files related to the alert.
- Names and ids of copied files.

## Auto-accepting responses in MDR Web Console

You can enable auto-acceptance of the offered responses. In this case, the actions offered within responses, for example, deleting an infected file, will be performed automatically. When this feature is disabled, the [measures offered within responses](#) need to be accepted or rejected manually.

If you use tenants, you can enable the auto-acceptance of responses for all tenants or only for the tenants that you select. If you do not use tenants, you enable or disable this feature for your current organization.

*To enable auto-acceptance of responses:*

1. In the MDR Web Console window, navigate to the **Settings** menu item.
2. Click the **Incidents** tab.
3. Select one of the following options:

- **Enabled for all tenants**

When this option is selected, the auto-acceptance of responses is enabled both for the existing and newly created tenants.

- **Enabled for the tenants selected below**

Select the tenants for which you want to enable the auto-acceptance of responses. For newly created tenants, the auto-acceptance of responses is disabled by default.

4. Click the **Save** button.

Auto-acceptance of responses is enabled and the actions offered within responses will be performed automatically for all tenants or the tenants that you selected. You can disable this option at any time.

## Access rights to view or change the auto-acceptance settings

The [user roles of Kaspersky Managed Detection and Response](#) have the following access rights to the auto-acceptance settings:

| Operation                                             | MDR Administrator | Senior Security Officer                            | Security Officer |
|-------------------------------------------------------|-------------------|----------------------------------------------------|------------------|
| Access the <b>Incidents</b> tab                       | ✓                 | ✓                                                  | —                |
| Change the currently selected option                  | ✓                 | —                                                  | —                |
| View the currently selected option                    | ✓                 | ✓                                                  | —                |
| Enable auto-acceptance for all tenants                | ✓                 | —                                                  | —                |
| Enable auto-acceptance for specific tenants           | ✓                 | ✓<br>(only for the tenants the user has access to) | —                |
| View the auto-acceptance setting of a specific tenant | ✓                 | ✓<br>(only for the tenants the user has access to) | —                |

## Auto-accepting responses in Kaspersky Security Center

You can enable auto-acceptance of the offered responses. In this case, the response actions offered within responses, for example, deleting an infected file, will be performed automatically. When this feature is disabled, the [measures offered within responses](#) need to be accepted or rejected manually.

If you use tenants, you can enable the auto-acceptance of responses for all tenants or only for the tenants that you select. If you do not use tenants, you enable or disable this feature for your current organization.

You can change the auto-acceptance settings if you have the MDR Administrator user role. Users with the Security Officer role are not allowed to change the settings. Users with the Senior Security Officer role are allowed to perform the following operations:

- View the currently selected option
- Enable or disable the auto-acceptance of responses for specific tenants if the **Allow changing the response auto-acceptance option for each tenant** option is selected

*To configure auto-acceptance of responses:*

1. In the **MDR** section of Kaspersky Security Center, click the **Settings** tab.
2. In the **Auto-acceptance of responses** group of parameters, select the required option:

- **Disable auto-acceptance of responses for all tenants**

Select this option, if you want to accept or reject response actions manually.

- **Allow changing the response auto-acceptance option for all tenants**

Select this option, if you want to enable the auto-acceptance of responses for all the tenants in your organization, including the existing and newly created tenants.

- **Allow changing the response auto-acceptance option for each tenant**

Select this option, if you want to configure the auto-acceptance of responses for each tenant individually. Then, select the check boxes for those tenants for which you want the response actions to be performed automatically. For newly created tenants, the auto-acceptance of responses is disabled by default.

If you select the **All tenants** option, the auto-acceptance of responses is enabled for the newly created tenants by default.

3. Click the **Save** button.

The **Save** button becomes active only if you changed the settings.

## Closing incidents in MDR Web Console

You can close an incident if you know that it is a duplicate or you are not going to solve it. In other cases, you must not close incidents, as they need to be solved by the MDR solution. The MDR solution resolves an incident if the recommended measures within this incident are applied. A resolved incident automatically closes after 72 hours.

*To close an incident:*

1. In MDR Web Console, navigate to the **Incidents** menu item.

The incident list opens.

2. Click the string with the incident whose details you want to view.

The incident page opens.

3. On the **Summary** tab of the page, click the **Close incident** button in the lower part of the window.

There is no **Close incident** button for incidents with the **Closed** status.

The **Close incident** block appears.

4. In the **Reason why you are closing this incident** field, specify any additional information that you want to communicate to Kaspersky Managed Detection and Response SOC analysts. For example, you can give details why you consider this incident to be a standard, non-threatening situation for your infrastructure. You can leave this field empty.

5. Below the comment field, select the **True positive** or **False positive** option, depending on the closure reason.

Select the **True positive** option if Kaspersky Managed Detection and Response detected a threat, but you do not want MDR SOC analysts to investigate and solve the incident.

Select the **False positive** option if Kaspersky Managed Detection and Response detected a non-threatening activity as a threat. Kaspersky Managed Detection and Response uses this information for improving the automated detection algorithms.

6. In the lower part of the block, click the **Close** button.

The **Share your feedback** form appears.

7. In the **Share your feedback** form, select a rating from 1 to 5. You can leave a text comment about the handling of this incident. The feedback is processed by Kaspersky experts to improve the performance of the MDR solution.

8. Click **Submit**.

The **Close incident** block disappears.

The incident is closed. From now on, Kaspersky Managed Detection and Response will perform no actions in relation to this incident.

## Sending an incident to the Incident Response team for additional investigation

You can [send an incident to the Incident Response team](#) for investigation. This service involves the complete set of response actions, starting from initial analysis and early response actions up to detecting additional attack signs and preparing a plan for elimination of possible consequences.

When you pay for the subscription to the service, you obtain a number of investigation hours. You spend the investigation hours when you send an incident to the Incident Response team. If you do not have available investigation hours, you still can send an incident for investigation by purchasing a commercial service and creating a request manually.

You receive investigation results in the incident's **Communication** tab.

Users with MDR Administrator or Senior Security Officer roles are allowed to send incidents to the Incident Response team.

*To send an incident to the Incident Response team:*

1. In the MDR Web Console window, navigate to the **Incidents** menu item.

The incident list opens.

2. Click the string with the incident that you want to send to Incident Response team.

The incident page opens.

3. On the **Summary** tab, in the **Actions** section, do one of the following:

- If you have investigation hours, click the **Escalate incident to the IR team** button, and then confirm that you want to send the incident to the Incident Response team.
- If you do not have investigation hours, click the link, and then fill out the request creation form to purchase a commercial service.

The incident is sent. The Incident Response team experts will contact you through MDR Web Console as soon as possible after they receive the incident.

# Kaspersky Unified Monitoring and Analysis integration

Kaspersky Unified Monitoring and Analysis Platform (KUMA) is an integrated software solution that combines the following functionality:

- Receiving, processing, and storing information security events
- Analyzing and correlating incoming data
- Searching in received events
- Creating notifications about detected indicators of information security threats

You can configure the Kaspersky Managed Detection and Response integration in KUMA version 4.0 or later to automatically import KUMA data to MDR.

The following article describes how to configure the integration: [Kaspersky Endpoint Managed Detection and Response integration](#).

## Creating Managed Detection and Response incidents from XDR incidents

You can create an MDR incident from an XDR incident if the Managed Detection and Response integration is enabled in Open Single Management Platform and the XDR incident's alerts meet the following conditions:

- The detection source is endpoint.
- At least one related asset is included in the alert.
- The detection technology is any of the following:
  - Kaspersky IOA rules
  - SB (Sandbox)
  - AM (Anti-Malware Engine)
  - IOC
  - YARA

We recommend that you activate the MDR solution on all managed assets to ensure continuous managed protection and automate threat detection, freeing up IT security employees to address tasks that require their involvement.

*To export an XDR incident to MDR:*

1. In the main menu of the OSMP Console interface, go to **Monitoring → Incidents**.
2. In the incident table, click the ID of the required incident. The window with incident details is displayed.
3. Click the three-dots icon on the toolbar and select **Create MDR incident**.
4. In the **Create MDR incident** panel, specify the incident name and description and click **Create**.

If the incident is created successfully, an appropriate message is displayed. You can now access the incident in the MDR Web Console. The link to the incident is available in the **Summary** section of the XDR incident.

# Kaspersky Digital Footprint Intelligence integration for MDR

The MDR solution can use compromised credentials identified by Kaspersky Digital Footprint Intelligence (DFI) to enhance threat detection, investigation, and threat hunting workflows.

Customers do not need to have an active Kaspersky DFI license to use this capability. Kaspersky DFI data is available as part of the corresponding MDR functionality.

The MDR solution analyzes credential leaks relevant to the customer organization and the assets that are associated with it and are covered by MDR monitoring. The primary focus is on infostealer-related credential leaks, which may indicate a potential compromise of an employee's device.

Kaspersky DFI data is used by MDR for the following functionality:

- Alert enrichment with credential leak context;
- Correlation of leaked credentials with security events;
- Threat hunting and detection of potential compromise based on credential information.

Kaspersky DFI integration helps the MDR solution identify potentially compromised accounts faster, better prioritize related incidents, and reduce the risk of unauthorized access.

In addition to infostealer-related leaks, Kaspersky DFI can analyze publicly available credential exposures from third-party resources where employee credentials may also appear. Its monitoring scope can also extend to partners and other entities associated with the organization.

To summarize, Kaspersky DFI provides MDR with credential compromise intelligence, while MDR applies this data within SOC workflows through alert enrichment, correlation, and threat hunting.

# Using Kaspersky Endpoint Detection and Response Expert features

Kaspersky Endpoint Detection and Response Expert integration within the Open Single Management Platform enables the following functionality:

- Kaspersky Endpoint Detection and Response sends alert data to MDR, which allows you to process Endpoint Detection and Response telemetry and alerts in the MDR solution.
- [The ability to create MDR incidents from XDR incidents.](#)
- The Get artefacts [response type](#).

## Enabling the Kaspersky Endpoint Detection and Response Expert integration

The MDR Administrator role is required to configure the integration.

*To enable the integration:*

1. [Configure the MDR Plug-in](#) in the Open Single Management Platform Console.
2. In the MDR section of the OSMP Console interface, click the **MDR Usage** tab.
3. Expand the **KPSN configuration file for integration with KEDR Expert** block.
4. Enable the **Accept KPSN Agreement** option and click **Apply the KPSN configuration file for integration with KEDR Expert**.

The integration is enabled.

## Responses

The [Kaspersky Endpoint Detection and Response Expert](#) solution provides the following response features (hereupon also referred to as EDR responses), which you can run and configure manually.

- Network isolation
- Move file to Quarantine
- Send files to Cloud Sandbox
- Delete file
- Run Critical Areas Scan
- IOC Scan

- Execution prevention
- Start a process
- Terminate process
- Get file

You can find more details about these EDR responses in [Kaspersky Endpoint Detection and Response Expert Online Help](#).

The EDR responses described in this section are available for assets with Kaspersky Endpoint Security for Windows 11.7 or later. If you use Kaspersky Endpoint Security for Windows 11.6 or an earlier version on your assets, Kaspersky Endpoint Agent must be installed on these assets in order to work with EDR responses.

To manage EDR alert responses actions, in [Kaspersky Security Center](#)  go to the **Monitoring & Reporting** → **Alerts** section.

# Managing tenants

Multitenancy is a mechanism allowing you to become a Kaspersky Managed Detection and Response supplier for other organizations. Once you have an MDR account, you can create [tenants](#) in your MDR account.

You can create up to 100 tenants in your organization.

Your account in Kaspersky Security Center Web Console or Kaspersky Next Expert View must have a role with the following [access rights](#): **Incident access** and **Tenant management**, and the ability to view, add, edit, and delete tenants in the **MDR** section in Kaspersky Security Center.

If your organization has multiple licenses, you can only [manage tenants in Kaspersky Security Center](#).

To become an MDR supplier, you must have access to your tenant's infrastructure to be able to perform deployment scenarios.

All tenants are independent and isolated, which means no data from one tenant can be accessed by other tenants.

Assets with Kaspersky Embedded Systems Security for Windows and Kaspersky Embedded Systems Security for Linux can only be assigned to the root tenant.

Only users with the [MDR Administrator role](#) assigned can add, edit, and delete tenants in MDR Web Console.

## Managing tenants in Kaspersky Security Center

This section provides information about managing existing tenants and adding new tenants in Kaspersky Security Center.

## Viewing tenants in Kaspersky Security Center

You can view available tenants by using the tenants list.

Your account in Kaspersky Security Center Web Console or Kaspersky Next Expert View must have a role with the following [access rights](#): **Incident access** and **Tenant management**, and the ability to view, add, edit, and delete tenants in the **MDR** section in Kaspersky Security Center.

*To view tenants:*

1. In the **MDR** section of Kaspersky Security Center, click the **Tenants** tab.

The **Tenants** list appears. Each line represents one tenant. You can click the tenant name to view tenant information.

2. The following tenant attributes are present above the list:

### **Name**

An arbitrary, human-readable name of the tenant that you specify while creating the tenant. The tenant name can contain Latin letters, digits, and special characters. It cannot be more than 100 characters long. Tenants cannot be renamed.

### **Status**

One of the following tenant statuses:

- **Active**

A tenant can use Kaspersky Managed Detection and Response.

- **Inactive**

A tenant cannot use Kaspersky Managed Detection and Response.

You can set the inactive status manually in the tenant card. Also, inactive status is set automatically at the end of the tenant's lifetime.

### **Assets / limit**

Number of assets assigned to a tenant / Asset limit.

The asset limit is specified when creating additional tenants and is for informational purposes only. Exceeding the limit is permitted and does not affect the operation of the MDR solution.

### **Description**

Free-form information that you enter while creating or editing the tenant. You can specify the tenant purpose or the projected number of assets. The description can contain Latin letters, digits, and special characters. It cannot be more than 2000 characters long.

### **Created on**

Date when the tenant was created.

### **Expiration date**

Date when the tenant lifetime expires.

Tenants are sorted according to their expiration date, in descending order.

You can also [view tenants in MDR Web Console](#).

## Viewing tenant settings in Kaspersky Security Center

You can view the settings of every tenant in your account.

Your account in Kaspersky Security Center Web Console or Kaspersky Next Expert View must have a role with the following [access rights](#): **Incident access** and **Tenant management**, and the ability to view, add, edit, and delete tenants in the **MDR** section in Kaspersky Security Center.

To view tenant settings:

1. In the **MDR** section of Kaspersky Security Center, click the **Tenants** tab.

The **Tenants** list appears. Each line represents one tenant. You can click the tenant name to view tenant information.

2. Click the line with the tenant whose details you want to view.

The **Tenant settings** block appears.

The setting starts with the **Active** toggle button showing whether a tenant is active or not. If necessary, you can switch the **Active** toggle button. Below, the following fields are present:

#### **Name**

An arbitrary, human-readable name of the tenant that you specify while creating the tenant. The tenant name can contain Latin letters, digits, and special characters. It cannot be more than 100 characters long. Tenants cannot be renamed.

#### **ID**

A unique automatically generated tenant id.

#### **Description**

Free-form information that you enter while creating or editing the tenant. You can specify the tenant purpose or the projected number of assets. The description can contain Latin letters, digits, and special characters. It cannot be more than 2000 characters long.

#### **Assigned assets**

The number of assets assigned to the tenant.

#### **Limit of assets**

The number of assets planned to be connected to the tenant. Exceeding this limit is permitted and does not affect the operation of the MDR solution.

#### **Configuration files for the tenant**

This section shows information about the [MDR configuration file](#) for the tenant:

- **License**—The [license](#) that corresponds to the tenant.
- **Expiration date**—The tenant life span. You can specify the expiration date manually while creating the tenant. The expiration date cannot be equal to or later than the last day of your MDR license term.
- **Action**—You can click the **Download the configuration file** link to download the ZIP archive that contains the MDR configuration file.

Click the **X** button to delete a configuration file. You can only delete a configuration file if another configuration file is added to the tenant.

Click the **Add** button to add a new configuration file. Specify the license and the expiration date.

3. In the lower part of the **Tenant settings** block, click the **Close** button to close the block.

You can also [view tenant settings in MDR Web Console](#).

# Editing tenant settings in Kaspersky Security Center

You can edit the settings of every tenant in your account.

Your account in Kaspersky Security Center Web Console or Kaspersky Next Expert View must have a role with the following [access rights](#): **Incident access** and **Tenant management**, and the ability to view, add, edit, and delete tenants in the **MDR** section in Kaspersky Security Center.

*To edit tenant settings:*

1. In the **MDR** section of Kaspersky Security Center, click the **Tenants** tab.

The **Tenants** list appears. Each line represents one tenant. You can click the tenant name to view tenant information.

2. Click the line with the tenant whose details you want to edit.

The **Tenant settings** block appears. Here you can perform the following actions:

- Activating or deactivating the tenant by switching the **Active** toggle button.
- Changing the value of the **Description** field.
- Deleting a configuration file by clicking the **X** button. You can only delete a configuration file if another configuration file is added to the tenant.
- Adding a new configuration file by clicking the **Save** button. Specify the license and the expiration date.

3. In the lower part of the **Tenant settings** block, click the **Save** button.

- The **Tenant settings** block disappears. After clicking the **Save** button, Kaspersky Managed Detection and Response generates the new MDR configuration file that complies with the updated tenant settings. You can click the **Download the configuration file** link to download the ZIP archive that contains the MDR configuration file.

The tenant settings are edited. The updated settings are applied to the assets of the selected administration groups.

You can also [edit tenant settings in MDR Web Console](#).

## Adding new tenants in Kaspersky Security Center

If you want to become a Kaspersky Managed Detection and Response supplier for another organization, you need to add a new tenant to your account.

Your account in Kaspersky Security Center Web Console or Kaspersky Next Expert View must have a role with the following [access rights](#): **Incident access** and **Tenant management**, and the ability to view, add, edit, and delete tenants in the **MDR** section in Kaspersky Security Center.

To add a new tenant:

1. In the **MDR** section of Kaspersky Security Center, click the **Tenants** tab.

The **Tenants** list appears.

2. In the upper part of the window, click the **+ Add tenant** button.

The **Tenant settings** block appears.

3. If necessary, switch the **Active** toggle button.

The **Active** toggle button is on by default.

4. Fill in the following fields:

#### **Name**

An arbitrary, human-readable name of the tenant that you specify while creating the tenant. The tenant name can contain Latin letters, digits, and special characters. It cannot be more than 100 characters long. Tenants cannot be renamed.

#### **Description**

Free-form information that you enter while creating or editing the tenant. You can specify the tenant purpose or the projected number of assets. The description can contain Latin letters, digits, and special characters. It cannot be more than 2000 characters long.

#### **Configuration files for the tenant**

This section shows information about the [MDR configuration file](#) for the tenant:

- **License**—The [license](#) that corresponds to the tenant.
- **Expiration date**—The tenant life span. You can specify the expiration date manually while creating the tenant. The expiration date cannot be equal to or later than the last day of your MDR license term.
- **Action**—You can click the **Download the configuration file** link to download the ZIP archive that contains the MDR configuration file.

Click the **X** button to delete a configuration file. You can only delete a configuration file if another configuration file is added to the tenant.

Click the **Add** button to add a new configuration file. Specify the license and the expiration date.

#### **Limit of assets**

The number of assets planned to be connected to the tenant. Exceeding this limit is permitted and does not affect the operation of the MDR solution.

5. In the lower part of the **Tenant settings** block, click the **Save** button.

The **Tenant settings** block disappears. After clicking the **Save** button, Kaspersky Managed Detection and Response generates an [MDR configuration file](#) for the new tenant. You can click the **Download the configuration file** link to download the ZIP archive that contains the MDR configuration file.

The new tenant is added.

You can also [add new tenants in MDR Web Console](#).

# Deleting tenants in Kaspersky Security Center

When you delete a tenant that contains some assets, all its assets are disconnected from MDR solution. To continue managing tenant's assets, you can [move them to the root tenant or a new tenant](#) before deleting the tenant.

Your account in Kaspersky Security Center Web Console or Kaspersky Next Expert View must have a role with the following [access rights](#): **Incident access** and **Tenant management**, and the ability to view, add, edit, and delete tenants in the **MDR** section in Kaspersky Security Center.

*To delete a tenant:*

1. In the **MDR** section of Kaspersky Security Center, click the **Tenants** tab.

The **Tenants** list appears.

2. In the **Tenants** list, point to the tenant that you want to delete, and then click the trash can icon (🗑️) in the **Actions** column.

3. Confirm the deletion.

The selected tenant is deleted.

You can also [delete tenants in MDR Web Console](#).

## Moving assets between tenants

When you delete a tenant that contains some assets, all its assets stop sending telemetry to MDR solution. Before deleting a tenant, move all its assets to the root tenant or a new tenant.

Your account in Kaspersky Security Center Web Console or Kaspersky Next Expert View must have a role with the following [access rights](#): **Incident access** and **Tenant management**, and the ability to view, add, edit, and delete tenants in the **MDR** section in Kaspersky Security Center.

*To move assets to a new tenant:*

1. In the **MDR** section of Kaspersky Security Center, [create a new tenant](#). Later, you will add assets to this tenant.

When you create a new tenant, you download an MDR configuration file.

2. In Kaspersky Security Center Web Console, [create a new administration group](#).

3. [Add the assets](#) that you want to move to the new tenant to the new administration group.

4. [Create a new policy](#) for Kaspersky Endpoint Agent or an EPP application for the created administration group.

5. Apply the MDR configuration file to the created policy.

For details on different deployment scenarios, refer to [Deployment of Kaspersky Managed Detection and Response](#).

After the policy is applied to the assets of the administration group, the assets are moved from the root tenant to the newly created tenant.

*To move assets to the root tenant:*

1. Download an MDR configuration file for root tenant:

- In MDR Web Console (<https://mdr.kaspersky.com/guide>), go to **Getting Started** page and click the **MDR configuration file** link.
- In your Kaspersky Security Center Web Console or Kaspersky Next Expert View, go to **MDR > Getting Started** and click the **Download** link.

2. In Kaspersky Security Center Web Console, [create a new administration group](#).

3. [Add the assets](#) that you want to move to the root tenant to the new administration group.

4. [Create a new policy](#) for Kaspersky Endpoint Agent or an EPP application for the created administration group.

5. Apply the MDR configuration file to the created policy.

After the policy is applied to the assets of the administration group, the assets are moved to the root tenant.

## Managing tenants in MDR Web Console

This section provides information about managing tenants in MDR Web Console.

### Viewing tenants in MDR Web Console

*To view tenants:*

1. In the MDR Web Console window, navigate to the **Settings** menu item.

2. Click the **Tenants** tab.

The **Tenants** list appears. Each line represents one tenant. You can click anywhere on the line to view tenant information.

3. The following tenant attributes are present above the list:

#### **Name**

An arbitrary, human-readable name of the tenant that you specify while creating the tenant. The tenant name can contain Latin letters, digits, and special characters. It cannot be more than 100 characters long. Tenants cannot be renamed.

#### **Status**

One of the following tenant statuses:

- **Active**

A tenant can use Kaspersky Managed Detection and Response.

- **Inactive**

A tenant cannot use Kaspersky Managed Detection and Response.

You can set the inactive status manually in the tenant card. Also, inactive status is set automatically at the end of the tenant's lifetime.

### **Assets / limit**

Number of assets assigned to a tenant / Asset limit.

The asset limit is specified when creating additional tenants and is for informational purposes only. Exceeding the limit is permitted and does not affect the operation of the MDR solution.

### **Description**

Free-form information that you enter while creating or editing the tenant. You can specify the tenant purpose or the projected number of assets. The description can contain Latin letters, digits, and special characters. It cannot be more than 2000 characters long.

### **Created on**

Date when the tenant was created.

### **Expiration date**

Date when the tenant lifetime expires.

Tenants are sorted according to their expiration date, in descending order.

### **Actions**

Shows the trash can icon (🗑️) on hover for non-root tenants. To delete the tenant, click the trash can icon and confirm deletion.

## Viewing tenant settings in MDR Web Console

*To view tenant settings:*

1. In MDR Web Console, navigate to the **Settings** menu item.

2. Click the **Tenants** tab.

The **Tenants** list appears. Each line represents one tenant. You can click anywhere on the line to view tenant information.

3. Click the line with the tenant whose details you want to view.

The **Tenant settings** block appears.

The setting starts with the **Active** toggle button showing whether a tenant is active or not. You can switch the **Active** toggle button to disable the tenant.

Below, the following fields are present:

#### **Tenant name**

An arbitrary, human-readable name of the tenant that you specify while creating the tenant. The tenant name can contain Latin letters, digits, and special characters. It cannot be more than 100 characters long. Tenants cannot be renamed.

### Description

Free-form information that you enter while creating or editing the tenant. You can specify the tenant purpose or the projected number of assets. The description can contain Latin letters, digits, and special characters. It cannot be more than 2000 characters long.

### Assets / limit

The number of assets planned to be connected to the tenant. Exceeding this limit is permitted and does not affect the operation of the MDR solution.

### Configuration file lifetime

Date when the tenant's configuration file expires.

This field is not shown for the root tenant.

In the lower part of the block, there is a button for downloading the [MDR configuration file](#) for the tenant deployment.

4. In the lower part of the **Tenant settings** block, click the **Cancel** button to close the block.

## Editing tenant settings in MDR Web Console

The ability to add, edit, and delete tenants is available only for the user who has the [MDR Administrator role](#) assigned.

*To edit tenant settings:*

1. Open MDR Web Console.
2. In the **Settings** section of MDR Web Console, click the **Tenants** tab.  
The **Tenants** list appears. Each line represents one tenant. You can click anywhere on the line to view tenant information.
3. Click the line with the tenant whose details you want to edit.  
The **Tenant settings** block appears.
4. If necessary, switch the **Active** toggle.
5. If necessary, change the values of the fields.
6. In the lower part of the **Tenant settings** block, click the **Save** button.  
The **Tenant settings** block disappears. After clicking the **Save** button, Kaspersky Managed Detection and Response generates a new MDR configuration file that complies with the updated tenant settings.

7. In the **Tenants** list, click the line with the edited tenant.

The **Tenant settings** block appears. In the lower part of the block, there is a button for downloading the [MDR configuration file](#) for the tenant deployment.

8. In the lower part of the **Tenant settings** block, click the **Cancel** button to close the block.

The tenant settings are edited. Now, you need to deploy the new MDR configuration file on the tenant's assets to apply the edited settings.

## Adding new tenants in MDR Web Console

The ability to add, edit, and delete tenants is available only for the user who has the [MDR Administrator role](#) assigned.

*To add a new tenant:*

1. In the MDR Web Console window, navigate to the **Settings** menu item.

2. Click the **Tenants** tab.

The **Tenants** list appears.

3. In the upper part of the window, click the **Add** button.

The **Tenant settings** block appears.

4. If necessary, switch the **Active** toggle button.

The **Active** toggle button is on by default.

5. Fill in the following fields:

### **Tenant name**

An arbitrary, human-readable name of the tenant that you specify while creating the tenant. The tenant name can contain Latin letters, digits, and special characters. It cannot be more than 100 characters long. Tenants cannot be renamed.

### **Description**

Free-form information that you enter while creating or editing the tenant. You can specify the tenant purpose or the projected number of assets. The description can contain Latin letters, digits, and special characters. It cannot be more than 2000 characters long.

### **Assets / limit**

The number of assets planned to be connected to the tenant. Exceeding this limit is permitted and does not affect the operation of the MDR solution.

### **Configuration file lifetime**

Date when the tenant's configuration file expires.

This field is not shown for the root tenant.

6. In the lower part of the **Tenant settings** block, click the **Save** button.

The **Tenant settings** block disappears. After clicking the **Save** button, Kaspersky Managed Detection and Response generates an [MDR configuration file](#) for the new tenant.

7. In the **Tenants** list, click the line with the new tenant.

The **Tenant settings** block appears. In this block you can download the [MDR configuration file](#) for the tenant deployment.

8. Click the **Configuration archive** button to download the new MDR configuration file.

9. In the lower part of the **Tenant settings** block, click the **Cancel** button to close the block.

The new tenant is added. Now, you can deploy the downloaded MDR configuration file on the tenant's assets.

Please note that the tenants created in MDR Web Console are not available in the **MDR** section of Kaspersky Security Center. Please use MDR Web Console to work with these tenants.

## Deleting tenants in MDR Web Console

When you delete a tenant that contains some assets, all its assets are disconnected from MDR solution. Incidents assigned to a deleted tenant are no longer available. This action is irreversible. Before deleting a tenant, [move all its assets to the root tenant or a new tenant](#).

The ability to add, edit, and delete tenants is available only for the user who has the [MDR Administrator role](#) assigned.

*To delete a tenant:*

1. In MDR Web Console, navigate to the **Settings** menu item.

2. Click the **Tenants** tab.

The **Tenants** list appears.

3. In the tenants list, hover the mouse pointer over the tenant you want to delete, and click the **Delete tenant** button with trash bin icon on the right.

The **Confirm tenant deletion** windows appears.

4. Click the **Delete** button to delete the tenant.

Please note that the tenants created in MDR Console are not available in the **MDR** section of Kaspersky Security Center. Please use MDR Web Console to work with these tenants.

# Managing the solution through the REST API

This feature is available in MDR Expert, MDR Advanced, (available in some regions only), and MDR Prime (available in some regions only). See the comparison of license solutions [in this section](#).

To have access to the REST API in Kaspersky Security Center, your account in Kaspersky Security Center Web Console needs to have the following access rights: Incident access and REST API access.

For some [commercial license tiers](#) it will only be possible to generate a refresh token in MDR Web Console to use it for [setting up MDR Plug-in](#), without access to the REST API in Kaspersky Security Center.

Kaspersky Managed Detection and Response allows you to programmatically get, create, and update MDR entities via the REST API. The REST API operates over HTTP and consists of a set of request/response methods. In other words, you can manage Kaspersky Managed Detection and Response through a third-party solution, not MDR Web Console.

To start working with the REST API, you need to [create a refresh token](#) and [an access token](#).

[OPEN THE REST API REFERENCE](#) 

## Scenario: performing token-based authorization

This scenario explains how to perform a token-based authorization in order to work with the REST API.

### Prerequisites

Make sure that you have an MDR account with one of the following roles assigned:

- The MDR Administrator [role](#)
- A custom role with the following [access rights](#) (applicable only for Kaspersky Security Center):
  - Incident Access
  - REST API access

## Stages

The token-based authorization proceeds in stages:

### 1 Creating a refresh token in MDR Web Console

You need [a refresh token](#) for creating an access token. A refresh token is valid for 24 hours. You can use a refresh token only once.

### 2 Creating an access token via the REST API

You need [an access token](#) to work with the REST API. An access token is valid for 1 hour. You can use an access token multiple times during its lifetime.

When you create an access token, the REST API generates a new refresh token and includes it in the response. When the access token expires, you can create a new access token by using the most recent API-generated refresh token.

An API-generated refresh token is valid for 7 days.

## Results

Upon completion of this scenario, you can [start working with the REST API](#) by sending requests with the access token.

# Creating an API connection in Kaspersky Security Center

When you create a new API connection, a refresh token is generated. A *refresh token* is a unique sequence of letters, digits, and symbols. Once created, a refresh token allows you to create an access token.

*To create an API connection:*

1. In the **MDR** section of Kaspersky Security Center, click the **API** tab.

The **API** list appears.

2. In the upper part of the window, click the **Add connection** button.

The **Add a new API connection** block appears.

3. Specify the following settings:

- **Connection name**

A connection name can contain Latin letters, digits, and special characters. A connection name is specified as `author_name` in REST API responses and displayed as the comment author on the **Communication** tab of an incident.

- **Access rights**

Select which access rights to grant for performing actions via the HTTP API:

- **Full access + API and tenants**

Access rights of the MDR Administrator role. An MDR Administrator is a superuser who has access to all Kaspersky Managed Detection and Response functions granted by the license. The MDR Administrator can grant access to client data sources to other users. When you activate Kaspersky Managed Detection and Response, you become the MDR Administrator automatically, which is why we recommend using a corporate email address for the activation process instead of a personal email address. Having the MDR Administrator created with a personal email address can pose security risks, such as stealing the MDR Administrator account.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | ✓     | —    |
| Response management         | ✓     | —    |
| Tenant management           | ✓     | —    |
| Incident summary scheduling | ✓     | —    |
| REST API access             | ✓     | —    |

- **Incident access, response management, and auto-accept settings**

Access rights of the Senior Security Officer role. A Senior Security Officer is an employee who has access to the Kaspersky Managed Detection and Response functions granted by the license, but does not have access to the REST API. The Senior Security Officer has the right to accept and reject [responses](#) <sup>2</sup>.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | ✓     | —    |
| Response management         | ✓     | —    |
| Tenant management           | —     | ✓    |
| Incident summary scheduling | —     | ✓    |
| REST API access             | —     | ✓    |

- **Incident access**

Access rights of the Security Officer role. A Security Officer is an employee who has access to the Kaspersky Managed Detection and Response functions granted by the license, but does not have access to the REST API. The Security Officer cannot accept and reject [responses](#) <sup>2</sup>.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | —     | ✓    |
| Response management         | —     | ✓    |
| Tenant management           | —     | ✓    |
| Incident summary scheduling | —     | ✓    |
| REST API access             | —     | ✓    |

- **Tenant**

If necessary, select the value (or values) in the **Tenant** drop-down list.

The user can view only the assets and incidents related to the specified tenants.

4. Click the **Generate** button.

The **JWT token** field appears.

5. Click the **Close** button.

The new API connection appears in the **API** list. Now, you can use the refresh token to [create an access token](#).

You can also [create API connections in MDR Web Console](#).

## Creating an API connection in MDR Web Console

A *refresh token* is a unique sequence of letters, digits, and symbols. Once created, a refresh token allows you to create an access token.

*To create a refresh token:*

1. In the MDR Web Console window, navigate to the **Settings** menu item.

2. Click the **API** tab.

The **All tokens** list appears.

3. In the upper part of the window, click the **Add** button.

The **Generate token** block appears.

4. Specify the following settings:

- **Connection name**

The name of a token.

The name of a token can contain Latin letters, digits, and special characters. The name of a token is specified as `author_name` in REST API responses and displayed as the comment author on the **Communication** tab of an incident.

For some [commercial license tiers](#), this is the only available field while creating a refresh token.

- **User role**

The user role to specify permissions that will be granted for performing actions via the HTTP API.

The following user roles are available:

- **MDR Administrator**

The superuser who has access to all Kaspersky Managed Detection and Response functions granted by the license. The MDR Administrator can grant access to client data sources to other users. When you activate Kaspersky Managed Detection and Response, you become the MDR Administrator automatically, which is why we recommend using a corporate email address for the activation process instead of a personal email address. Having the MDR Administrator created with a personal email address can pose security risks, such as theft of the MDR Administrator account.

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | ✓     | —    |
| Response management         | ✓     | —    |
| Tenant management           | ✓     | —    |
| Incident summary scheduling | ✓     | —    |
| REST API access             | ✓     | —    |

- **Senior Security Officer**

An employee who has access to the Kaspersky Managed Detection and Response functions granted by the license, but who does not have access to the REST API. The Senior Security Officer has the right to accept and reject [responses](#).

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | ✓     | —    |
| Response management         | ✓     | —    |
| Tenant management           | —     | ✓    |
| Incident summary scheduling | —     | ✓    |
| REST API access             | —     | ✓    |

- **Security Officer**

An employee who has access to the Kaspersky Managed Detection and Response functions granted by the license, but who does not have access to the REST API. The Security Officer cannot accept and reject [responses](#).

In Kaspersky Security Center, this role corresponds to the following access rights:

| Functional area             | Allow | Deny |
|-----------------------------|-------|------|
| Incident access             | ✓     | —    |
| Auto-accept settings        | —     | ✓    |
| Response management         | —     | ✓    |
| Tenant management           | —     | ✓    |
| Incident summary scheduling | —     | ✓    |
| REST API access             | —     | ✓    |

- **Tenant**

If necessary, select the value (or values) in the **Tenant** drop-down list.

The tenants already existing in Console and the **Root tenant** value are suggested.

The user can view only the assets and incidents related to the specified tenants. If you have assets and incidents not assigned to any tenants, the user can view them if you select the **Root tenant** value.

You can select the **Root tenant** value, in addition to specifying tenant names.

5. In the lower part of the block, click the **Generate** button.

The **Token info** block replaces the **Generate token** block.

6. Click the **Close** button in the lower part of the **Token info** block.

The refresh token that you have created appears in the **All tokens** list. Now, you can use this refresh token to [create an access token](#).

## Editing an API connection in Kaspersky Security Center

You can edit existing API connections.

*To edit an API connection:*

1. In the **MDR** section of Kaspersky Security Center, click the **API** tab.

The **API** list appears.

2. Click the API connection that you want to edit.

A block containing the connection information appears.

3. Change the connection settings.

4. Click the **Save** button.

The new settings of the selected API connection are saved.

## Editing an API connection in MDR Web Console

You can edit existing API connections.

*To edit an API connection:*

1. In MDR Web Console, click the **API** tab.

The **All tokens** list appears.

2. Click the token of the API connection that you want to edit.

A block containing the connection information appears.

3. Change the connection settings.

4. Click the **Save** button.

The new settings of the selected API connection are saved.

## Creating an access token in Kaspersky Security Center

An *access token* is a unique sequence of characters (letters, digits, and special characters) that authorizes you to use the methods of the REST API.

*To create an access token:*

1. In the **MDR** section of Kaspersky Security Center, click the **API** tab.

The **API** list appears.

2. Click a connection with a **Pending activation** status.

A block containing the connection information appears.

3. In the **JWT token** field, click the **Refresh** button.

A refresh token appears.

4. Select and save the value from the **Client ID** field.

5. Select and save the token's sequence of characters to the clipboard.

6. Send a POST request to the `/session/confirm` endpoint.

Replace `{client_id}` and `{refresh_token}` with the values selected and saved in the previous steps.

#### Example (Python):

```
#####
# General part
#####

import time
import datetime
import requests
import jwt

# The certificate is required for authentication of an external resource
# You can download the certificate from https://mdr.kaspersky.com,
# save it to your disk, and add the path to it in the variable:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# Your client's ID and your tokens
# For details about getting your ID and the tokens, refer to the help https://support.kaspersky.com/MDR/en-US/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Paste your value)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Paste your value)
ACCESS_TOKEN = "AcCeSsToKeN" # (Paste your value)

#####
# Get access token and a refresh token for the next access token update
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN expiration date and time: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN is actual")
    else:
        print(
            "You should update REFRESH_TOKEN; Please take it from MDR Web Console (https://support.kaspersky.com/MDR/en-US/258285.htm)"
        )
        exit()
else:
    print(
        "You should fill REFRESH_TOKEN value; Please take it from MDR Web Console (https://support.kaspersky.com/MDR/en-US/258285.htm)"
    )
    exit()

# Check the presence and validity of the access token
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 expiration date and time: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN is actual")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# If necessary, update the access token and refresh token for the next access token update
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()

    # It is necessary to save the refresh token in order to obtain next access token after the expiration of the current access token
    refresh_token = result_json["refresh_token"]
    print(
        f'Your new REFRESH_TOKEN for the next time for request ACCESS_TOKEN (please replace value of REFRESH_TOKEN with this value): "{refresh_token}"'
    )

    # A new access token is required to retrieve the data
    access_token = result_json["access_token"]
    print(f'Your new ACCESS_TOKEN (please replace value of ACCESS_TOKEN with this value): "{access_token}"')

# The access token is added to the request header
headers = {"Authorization": f"Bearer {access_token}"}
```

#### Example (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

The REST API sends a response with the access token and a new refresh token:

```
{
  "access_token": "SamPLET346yoKeNSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkENSaMP1et2590KeNS123aMP1e926tOkENSaMP1e"
}
```

Now, you can send requests to the REST API by using the access token. Each request to the REST API requires an access token; a request without an access token will return an authorization error only.

You can also [create an access token in MDR Web Console](#).

## Creating an access token in MDR Web Console

*To create an access token:*

1. In the MDR Web Console window, navigate to the **Settings** menu item.

2. Click the **API** tab.

The **All tokens** list appears. Each line represents one token. You can click anywhere on the line to view token information.

3. Click a token with a **Pending activation** status.

A **Token info** block appears.

4. In the **JWT token** field, click the **Refresh** button.

A refresh token appears.

5. Select and save the value from the **Client ID** field.

6. Select and save the token's sequence of characters to the clipboard.

7. Send a POST request to the `/session/confirm` endpoint (see the examples below).

Replace `{client_id}` and `{refresh_token}` with the values selected and saved in the previous steps.

#### Example (Python):

```
#####
# General part
#####

import time
import datetime
import requests
import jwt

# The certificate is required for authentication of an external resource
# You can download the certificate from https://mdr.kaspersky.com,
# save it to your disk, and add the path to it in the variable:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# Your client's ID and your tokens
# For details about getting your ID and the tokens, refer to the help https://support.kaspersky.com/MDR/en-US/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Paste your value)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Paste your value)
ACCESS_TOKEN = "AcCeSsToKeN" # (Paste your value)

#####
# Get access token and a refresh token for the next access token update
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN expiration date and time: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN is actual")
    else:
        print(
            "You should update REFRESH_TOKEN; Please take it from MDR Web Console (https://support.kaspersky.com/MDR/en-US/258285.htm)"
        )
        exit()
else:
    print(
        "You should fill REFRESH_TOKEN value; Please take it from MDR Web Console (https://support.kaspersky.com/MDR/en-US/258285.htm)"
    )
    exit()

# Check the presence and validity of the access token
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 expiration date and time: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN is actual")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# If necessary, update the access token and refresh token for the next access token update
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()

    # It is necessary to save the refresh token in order to obtain next access token after the expiration of the current access token
    refresh_token = result_json["refresh_token"]
    print(
        f'Your new REFRESH_TOKEN for the next time for request ACCESS_TOKEN (please replace value of REFRESH_TOKEN with this value): "{refresh_token}"'
    )

    # A new access token is required to retrieve the data
    access_token = result_json["access_token"]
    print(f'Your new ACCESS_TOKEN (please replace value of ACCESS_TOKEN with this value): "{access_token}"')

# The access token is added to the request header
headers = {"Authorization": f"Bearer {access_token}"}
```

#### Example (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

The REST API sends a response with the access token and a new refresh token:

```
{
  "access_token": "SamPLET346yoKeNSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkENSaMP1et2590KeNS123aMP1e926tOkENSaMP1e"
}
```

Now, you can send requests to the REST API by using the access token. Each request to the REST API requires an access token; a request without an access token will return an authorization error only.

## Working with the REST API

Working with MDR through the REST API includes getting, creating, and updating assets, incidents, responses, and users.

[OPEN THE REST API REFERENCE](#) 

The REST API methods require `client_id` value. You can get your `client_id` value in the **Token info** block of any refresh token in MDR Web Console.

Following are examples of script for Python and Shell that demonstrate core REST API capabilities:

- Define the certificate path, REST API URL, client ID, and the tokens
- Get access token and refresh token for the next access token update
- Get the number of asset
- Get the list of assets or asset details
- Get the number of incidents, the list of the incidents, or the incident details
- Get the list of responses for the incident
- Confirm, decline the response, or update the response list
- Get the list of comments for the specified incident, or create a new comment for the specified incident

#### Example (Python):

```
#####
# General part
#####

import time
import datetime
import requests
import jwt

# The certificate is required for authentication of an external resource
# You can download the certificate from https://mdr.kaspersky.com,
# save it to your disk, and add the path to it in the variable:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# Your client's ID and your tokens
# For details about getting your ID and the tokens, refer to the help https://support.kaspersky.com/MDR/en-US/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Paste your value)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Paste your value)
ACCESS_TOKEN = "AcCeSsToKeN" # (Paste your value)

#####
# Get access token and a refresh token for the next access token update
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN expiration date and time: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN is actual")
    else:
        print(
            "You should update REFRESH_TOKEN; Please take it from MDR Console (https://support.kaspersky.com/MDR/en-US/258285.htm)"
        )
        exit()
else:
    print(
        "You should fill REFRESH_TOKEN value; Please take it from MDR Console (https://support.kaspersky.com/MDR/en-US/258285.htm)"
    )
    exit()

# Check the presence and validity of the access token
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 expiration date and time: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN is actual")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

# If necessary, update the access token and refresh token for the next access token update
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()

    # It is necessary to save the refresh token in order to obtain next access token after the expiration of the current access token
    refresh_token = result_json["refresh_token"]
    print(
        f'Your new REFRESH_TOKEN for the next time for request ACCESS_TOKEN (please replace value of REFRESH_TOKEN with this value): "{refresh_token}"'
    )

    # A new access token is required to retrieve the data
    access_token = result_json["access_token"]
    print(f'Your new ACCESS_TOKEN (please replace value of ACCESS_TOKEN with this value): "{access_token}"')

# The access token is added to the request header
headers = {"Authorization": f"Bearer {access_token}"}

#####
# Get the number of assets
#####

# The date and time are in milliseconds since 1970-01-01T00:00:00Z
request_body = {
    "max_last_seen": int(time.time())
    * 1000, # Limiting the maximum time for the last appearance of the asset to the current time
    "min_last_seen": 163931132000, # Limiting the minimum time for the last appearance of the asset with the constant - Sunday, December 12, 2021
    12:12:12 PM (GMT)
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Get the list of assets
#####

request_body = {
    # Search parameters:
    "version": 2, # Specify 2 as the solution version
    "max_last_seen": int(time.time())
    * 1000, # Limiting the maximum time for the last appearance of the asset to the current time
    "min_last_seen": 163931132000, # Limiting the minimum time for the last appearance of the asset with the constant - Sunday, December 12, 2021
    12:12:12 PM (GMT)
}
```

```

    "domain": "",
    "host_names": ["MA-MDR-KES-S", "SIN-MDR-KSC"], # (Paste your value) Host names list
    "is_isolated": False,
    "network_interface": "10.70.104.1",
    "os_version": "Windows", # The asset must contain the specified line in the name of the OS
    "product": "",
    "search_phrase": "mdr", # Phrase to search by field contents: "host_name", "domain", "installed_product_info", "network_interfaces", "os_version"
    "statuses": ["OK", "ABSENT"], # Search for assets with the current statuses listed here
    # Options for displaying search results:
    "sort": "first_seen:asc", # Sort results by time of first occurrence; in case of page-by-page retrieval of results, it is necessary to specify a
    # field for sorting that will not change from query to query, for example, "first_seen" (do not specify fields whose values are constantly changing, for
    # example, the field "last_seen"; this may lead to incorrect results)
    "page_size": 100, # Assets per page - 100
    "page": 1, # Get the first page of search results
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Get asset details
#####

request_body = {
    "version": 2, # Specify 2 as the solution version
    "asset_id": "0xFA6A68CC9A9415963DE841048A3BE929", # (Paste your value) 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)

#####
# Get the number of incidents
#####

request_body = {
    "max_update_time": int(time.time())
    * 1000, # Limit the maximum time of the last incident update to the current time
    "min_update_time": 163931132000, # Limiting the minimum time for the last incident update with the constant - Sunday, December 12, 2021 12:12:12
    PM (GMT)
    "affected_hosts": [
        "MA-MDR-KES-S:0xFA6A68CC9A94145456E841048A3BE929"
    ], # (Paste your value) Host list in "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())

#####
# Get the list of incidents
#####

request_body = {
    # Search parameters:
    "max_creation_time": int(time.time())
    * 1000, # Limit the maximum time of the incident creation to the current time
    "min_creation_time": 163931132000, # Limiting the minimum time for the incident creation with the constant - Sunday, December 12, 2021 12:12:12 PM
    (GMT)
    "asset_ids": [
        "0xFA6A68CC9A9415963DE841048A3BE929"
    ], # (Paste your value) List of assets for which we get the incidents
    "priorities": ["HIGH"],
    "resolutions": ["True positive"],
    "response_statuses": ["Confirmed"],
    "response_types": ["hash"],
    "statuses": ["Closed"],
    # Parameters for providing results
    "markdown_to_html": True, # Results in HTML format; if the value is "False", the results are in Markdown format
    "sort": "creation_time:asc", # Sort results by date and time of incident creation; in case of page-by-page retrieval of results, it is necessary to
    # specify a field for sorting that will not change from query to query, for example, creation_time (do not specify fields whose values are constantly
    # changing, for example, the "update_time" field; this may lead to incorrect results)
    "page_size": 100, # Incidents per page - 100
    "page": 1, # Get the first page of search results
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Get incident details
#####

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m", # (Paste your value) Incident ID
    "markdown_to_html": True, # Results in HTML format; if the value is "False", the results are in Markdown format
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Get a list of responses for the incident
#####

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m", # (Paste your value) Incident ID
    "page_size": 10, # Responses per page - 10
    "page": 1, # Get the first page of search results
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)

```

```

print(result.json())

#####
# Confirm the response
#####

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W", # (Paste your value) Response ID
    "comment": "comment_text", # Comment to be added to the response
    "status": "Confirmed", # New response status - "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Decline the response
#####

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W", # (Paste your value) Response ID
    "comment": "comment_text", # Comment to be added to the response
    "status": "Declined", # New response status - "Declined"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Update response list
#####

request_body = {
    "responses_ids": [
        "CEgYG4UBMUGN-LWULP7W",
        "2ES16IgB4cAOuyXBb5IB",
    ], # (Paste your values) Response IDs
    "comment": "comment_text", # Comment to be added to the responses
    "status": "Confirmed", # New responses status - "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

```

#### Example (Shell):

```
# Get access token and new refresh token
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
# Reply example; next, you must use the access_token to retrieve the data and the refresh_token to retrieve the new access token and refresh token
{
  "access_token": "SamPLET346yoKenSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOKenSaMPlet2590KenS123aMPle926tOKenSaMPle"
}

# Get the number of assets
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}'

# Get the list of assets
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}'

# Get asset details
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}'

# Get the number of incidents
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"]}'

# Get the list of incidents
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}'

# Get incident details
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}'

# Get a list of responses for the incident
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}'

# Update the response
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"}'

# Update response list
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", "2ES16IgB4cA0UyXBb5IB"], "comment": "comment_text", "status": "Confirmed"}'
```

REST API reply example with the access token and new refresh token:

```
{
  "access_token": "SamPLET346yoKenSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOKenSaMPlet2590KenS123aMPle926tOKenSaMPle"
}
```

REST API reply example with the structure and values of comments:

```
[{
  "comment_id": "bfu6TiNghqp",
  "author_name": "John Doe",
  "text": "<p>The first comment</p>",
  "creation_time": 1601295428640
}, {
  "comment_id": "bfu6TiNghqt",
  "author_name": "Jane Doe",
  "text": "<p>The second comment</p>",
  "creation_time": 1601295433441
}]
```

REST API reply example when REST API creates a new comment and sends a response with the comment details:

```
{
  "comment_id": "AXTej0Qi4bfu6TiNgmvT",
  "author_name": "Token name",
}
```

```
"text": "This is a new comment created via the REST API ",
"creation_time": 1601461748122
}
```

## Revoking a refresh token in Kaspersky Security Center

You can revoke refresh tokens from API connections that currently have the *Active* or *Idle* status.

*To revoke a refresh token:*

1. In the **MDR** section of Kaspersky Security Center, click the **API** tab.

The **API** list appears.

2. Click the API connection from which you want to revoke a refresh token.

A block containing the connection information appears.

3. Click the **Revoke** button.

The refresh token is revoked.

## Deleting an API connection in Kaspersky Security Center

You can delete existing API connections.

*To delete an API connection:*

1. In the **MDR** section of Kaspersky Security Center, click the **API** tab.

The **API** list appears.

2. Select the radio button next to the API connection that you want to delete and click **Delete connection**.

The selected API connection is deleted.

## Deleting an API connection in MDR Web Console

You can edit existing API connections.

*To edit an API connection:*

1. In MDR Web Console, click the **API** tab.

The **All tokens** list appears.

2. Point to the API connection that you want to delete, and then click the trash can icon (🗑️) on the right side of the line.

The selected API connection is deleted.

# Deactivating Kaspersky Managed Detection and Response

If you want to stop using Kaspersky Managed Detection and Response, you can either permanently terminate its usage or temporarily suspend it on particular assets.

## Terminating the use of Kaspersky Managed Detection and Response

You can manually terminate the use of Kaspersky Managed Detection and Response if you want to stop using it.

When you terminate the use of Kaspersky Managed Detection and Response, Kaspersky Managed Detection and Response stops sending telemetry from your assets. To delete the data about your organization from the infrastructure of Kaspersky Managed Detection and Response, please contact [technical support](#).

*To terminate the use of Kaspersky Managed Detection and Response:*

1. In Kaspersky Security Center Web Console or Kaspersky Next Expert View, go to the **Assets (Devices)** → **Policies & profiles** section, if you are using the [EPP applications](#) that support policies.  
If you are using an EPP application that does not support policies, go to the **Assets (Devices)** → **Tasks** section.  
The list of policies (or the list of tasks) opens.
2. Click a policy or task that you created during the deployment of Kaspersky Managed Detection and Response to set up integration between an EPP application and Kaspersky Managed Detection and Response.  
The policy settings window (or the task settings window) opens.
3. On the **Application settings** tab, in the left pane, select **Detection and Response**, and then in the right pane, select **Managed Detection and Response**.  
The **Managed Detection and Response** settings pane opens.
4. Disable the **Managed Detection and Response enabled** option.  
The name of the option changes to **Managed Detection and Response disabled**.
5. Save the changes to the policy or task.
6. [Revoke your consent with the terms of using the MDR solution](#).
7. If you are using the on-premises Kaspersky Security Center Web Console to work with Kaspersky MDR, it is additionally recommended to [remove the KPSN configuration file from Kaspersky Security Center Administration Server](#) <sup>2</sup>.

The use of Kaspersky Managed Detection and Response is terminated.

# Suspending the use of Kaspersky Managed Detection and Response temporarily

In order to comply with the [terms of using the MDR solution](#) it is required to suspend the use of the solution on the assets if they are temporarily located on the United States territory (for example, during a business trip).

*To suspend the use of the MDR solution temporarily on particular assets:*

1. In Kaspersky Security Center, create a new [administration group](#) to manage assets on which you want to suspend the use of the MDR solution. You will be able to modify the list of assets in this group later.
2. For this administration group, [create new policies](#) of the EPP applications used to provide the MDR telemetry from the assets, and then disable the use of the MDR solution and Kaspersky Security Network in the policy settings.  
For details about configuring the policies, refer to the help articles for a particular EPP application. For example, Kaspersky Endpoint Security for Windows help contains instructions on [managing policies](#) and configuring [integration with the MDR solution](#).

3. [Move the assets](#) on which you want to suspend the use of the MDR solution to the created administration group.  
The new policy where the use of MDR solution and Kaspersky Security Network are disabled will be applied to the assets after synchronization. You can also manually [force the synchronization](#).

*To resume the use of Kaspersky Managed Detection and Response after suspension:*

1. Exclude the asset from the administration group used for suspension.
2. Apply a regular policy where the use of MDR solution is enabled and configured to this asset.

The assets will not be monitored by the MDR solution until a policy where the use of MDR solution is enabled and configured is applied to them.

## Revoking your consent with the terms of using the MDR solution

If you decide to stop using Kaspersky Managed Detection and Response, revoke your consent with the terms of using the MDR solution, and then [disable the use of Kaspersky Managed Detection and Response on the assets](#).

This feature is only available if you have the **Application integration** access right set in [Kaspersky Security Center Web Console](#) or [Kaspersky Next Expert View](#).

*To revoke your consent with the terms of using the MDR solution:*

1. In the MDR section of Kaspersky Security Center window, click the **MDR Usage** tab.
2. Expand the **Terms of Use for the MDR solution** block by clicking its name.
3. Click the **Revoke the confirmation of acceptance of Terms of Use for the MDR solution** link.
4. Confirm that you want to revoke your consent with the terms of using the MDR solution.

Your consent with the terms of using the MDR solution is revoked.

If you want to remove the information about your organization from the MDR infrastructure, please contact [Technical Support](#).

# Known issues

Kaspersky Managed Detection and Response has a number of limitations that are not critical to operation of the application:

- If you clone a virtual or physical asset with Kaspersky Endpoint Security for Linux that is already connected to the MDR solution, telemetry data from the cloned assets is not transmitted correctly. For these cloned assets, remove Kaspersky Endpoint Security for Linux, delete install\_id file in /var/opt/kaspersky/epagent/ folder, and then reinstall Kaspersky Endpoint Security for Linux.
- For assets with the Kaspersky Endpoint Security for Windows in the Endpoint Detection and Response Agent (EDR Agent) configuration, the *Warning* and *Critical* statuses for protection and control components are not displayed.
- You can not use [Kaspersky Endpoint Detection and Response Optimum features](#) for the assets with Kaspersky Endpoint Security for Windows in EDR Agent configuration.
- The **Kaspersky applications that work with MDR** section of the asset card in MDR Web Console can contain outdated Endpoint Protection Platform (EPP) applications, that are no longer used to work with Kaspersky Managed Detection and Response. It occurs when an outdated EPP application was replaced with a new one on the asset. For these outdated applications, the **Last seen** field contains the old date, while for the new EPP application, the **Last seen** field contains the newer date.
- The MDR solution that uses KPSN configuration does not support a hierarchy of Kaspersky Security Center Administration Servers if only the primary Server in the hierarchy has internet access.
- The MDR solution does not support automatic uploading of files larger than 64 MB when using the [Get artefacts response](#) that is available from Kaspersky Endpoint Detection and Response Expert integrated in the Open Single Management Platform.
- The MDR Plug-in for Kaspersky Security Center and the MDR Plug-in for Open Single Management Platform do not support displaying information about Kaspersky Embedded Systems Security for Linux version 4.0 or later in the list of non-working assets.

# Contact Technical Support

This section describes how to get technical support and the terms on which it is available.

## How to get technical support

If you can't find a solution to your issue in the [Kaspersky Managed Detection and Response documentation or in any of the sources of information about Kaspersky Managed Detection and Response](#), contact Kaspersky Customer Service. Technical Support specialists will answer all your questions about installing and using Kaspersky Managed Detection and Response.

Kaspersky provides support of Kaspersky Managed Detection and Response during its lifecycle (see the [application support lifecycle page](#)). Before contacting Technical Support, please read the [support rules](#).

You can contact Technical Support in one of the following ways:

- [By visiting the Technical Support website](#)
- By sending a request to Technical Support from the [Kaspersky CompanyAccount portal](#)

## Technical support via Kaspersky CompanyAccount

[Kaspersky CompanyAccount](#) is a portal for companies that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky specialists through online requests. You can use Kaspersky CompanyAccount to track the status of your online requests and store a history of them as well.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian

- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the [Technical Support website](#)<sup>2</sup>.

# Sources of information about the solution

On the [Kaspersky Managed Detection and Response page](#), you can view general information about the solution, its functions, and its features.

# Glossary

## Asset

A device with an installed Kaspersky EPP application (for example, Kaspersky Endpoint Security for Windows).

## Endpoint Protection Platform (EPP)

An integrated system of complex protection for endpoint devices (for example, mobile devices, computers, or laptops) that includes various security technologies. An example of an Endpoint Protection Platform is Kaspersky Endpoint Security for Business.

## EPP application

An application included in a protection system for endpoint devices (Endpoint Protection Platform, or EPP). EPP applications are installed on endpoint devices within the IT infrastructure of an organization (for example, mobile devices, computers, or laptops). An example of an EPP application is Kaspersky Endpoint Security for Windows, as part of the EPP solution Kaspersky Endpoint Security for Business.

## Incident

An activity evaluated as critical by the detection technology and which requires immediate reaction from Kaspersky Managed Detection and Response.

## IOC

An indicator of compromise (or IOC) shows the evidence on a device that points to a security breach.

## MITRE tactic

The objective that an attacker wanted to achieve during a cyber attack on the Client infrastructure.

## MITRE technique

The method used by the attacker to perform malicious actions during a cyberattack on the Client infrastructure. Each MITRE tactic contains an array of MITRE techniques.

## Response

Incident response is a structured methodology for handling security incidents, breaches, and cyberthreats.

## Telemetry

Data that is sent from assets to Kaspersky Managed Detection and Response.

## Tenant

A tenant is an organization to which you supply Kaspersky Managed Detection and Response.

# Information about third-party code

Third-party code has been used in the development of the solution.

For information about third-party code in MDR Web Console, contact Kaspersky Managed Detection and Response Support.

Information about third-party code used in MDR Plug-in is contained in the file [legal\\_notices.txt](#).

# Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Apple, Mac, macOS, and Safari are trademarks of Apple Inc.

Amazon AWS, Amazon Web Services are trademarks of Amazon.com, Inc. or its affiliates.

Active Directory, Internet Explorer, Microsoft, Microsoft Edge, Outlook, PowerShell, Windows PowerShell, Windows, and Windows Server are trademarks of the Microsoft group of companies.

Firefox and Mozilla are trademarks of the Mozilla Foundation in the U.S. and other countries.

Google and Google Chrome are trademarks of Google LLC.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Python is a trademark or registered trademark of the Python Software Foundation.

# Configuring audit settings for work with Kaspersky Managed Detection and Response

We recommend configuring the following audit settings to ensure stable operation and maximize efficiency of Kaspersky Managed Detection and Response:

- **Configuring Windows Event Audit Policy**

To maximize efficiency of Kaspersky Managed Detection and Response, you need to configure Windows Event Audit Policy on your assets.

*To configure Windows Event Audit Policy:*

1. On your assets running Windows, press **Win+R** to open the **Run** window.
2. In the **Open** field, type `gpedit.msc`, and then press **Enter** or click **OK**. The **Local Group Policy Editor** window appears.
3. In the console tree, click **Computer Configuration** → **Windows Settings** → **Security Settings** → **Advanced Audit Policy Configuration** → **System Audit Policies - Local Group Policy Object**.
4. Click the **Account Logon** node. Set the following values in the right side of the window:

| Subcategory                              | Audit Events        |
|------------------------------------------|---------------------|
| Audit Credential Validation              | Success and Failure |
| Audit Kerberos Authentication Service    | Success and Failure |
| Audit Kerberos Service Ticket Operations | Success and Failure |

5. Click the **Account Management** node. Set the following values in the right side of the window:

| Subcategory                       | Audit Events        |
|-----------------------------------|---------------------|
| Audit Computer Account Management | Success and Failure |
| Audit Security Group Management   | Success             |
| Audit User Account Management     | Success and Failure |

6. Click the **DS access** node. Set the following values in the right side of the window:

| Subcategory                     | Audit Events        |
|---------------------------------|---------------------|
| Audit Directory Service Access  | Success and Failure |
| Audit Directory Service Changes | Success and Failure |

7. Click the **Logon/Logoff** node. Set the following values in the right side of the window:

| Subcategory           | Audit Events        |
|-----------------------|---------------------|
| Audit Account Lockout | Failure             |
| Audit Logon           | Success and Failure |
| Audit Special Logon   | Success and Failure |

8. Click the **Object Access** node. Set the following values in the right side of the window:

| Subcategory                         | Audit Events        |
|-------------------------------------|---------------------|
| Audit Certification Services        | Success and Failure |
| Audit File Share                    | Success             |
| Audit Filtering Platform Connection | Success             |
| Audit Other Object Access Events    | Success             |

9. Click the **Policy Change** node. Set the following values in the right side of the window:

| Subcategory                           | Audit Events |
|---------------------------------------|--------------|
| Audit Policy Change                   | Success      |
| Audit MPSSVC Rule-Level Policy Change | Success      |

10. Click the **Privilege Use** node. Set the following value in the right side of the window:

| Subcategory                   | Audit Events |
|-------------------------------|--------------|
| Audit Sensitive Privilege Use | Success      |

11. Click the **System** node. Set the following values in the right side of the window:

| Subcategory                     | Audit Events |
|---------------------------------|--------------|
| Audit Security State Change     | Success      |
| Audit Security System Extension | Success      |

12. In the console tree, click the **Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell**. Set the following value in the right side of the window:

| Subcategory                             | Audit Events |
|-----------------------------------------|--------------|
| Turn on PowerShell Script Block Logging | Enabled      |

13. Close the **Local Group Policy Editor** window.

All changes are saved automatically.

The Windows Event Audit Policy is now configured for use with Kaspersky Managed Detection and Response.

#### • Configuring Audit for Active Directory objects

To maximize efficiency of Kaspersky Managed Detection and Response, you need to configure audit on your Windows Domain controllers.

*To configure audit for Active Directory objects:*

1. On your Windows Domain controller, press **Win+R** to open the **Run** window.
2. In the **Open** field, type `dsa.msc`, and then press **Enter** or click **OK**. The **Active Directory User and Computers** window appears.
3. In the console tree, right-click <your domain name>, and then select **Find**. The **Find Users, Contacts and Groups** window appears.
4. Enter **Administrator** in the **Name** field, and then click **Find Now**.
5. In the **Search results** area, right-click **Administrator** object, and then select the **Properties → Security → Advanced - Auditing** tab.

6. Click **Add** to open the **Auditing Entry for Administrator** window. Click **Select a principal**, enter **Everyone**, click **Check Names**, and then click **OK**.

7. In the **Auditing Entry for Administrator** window, select the **List contents**, **Read permissions**, **Modify permissions**, **Modify owner**, **Read all properties**, and **Write all properties** checkboxes.

8. Click **OK** → **Apply** → **OK** buttons.

The audit for Active Directory object **Administrator** is now configured to use with Kaspersky Managed Detection and Response.

9. Perform the same steps for the following default Active Directory objects and for your sensitive domain users and groups, that exist and are enabled in your system:

- **Administrators**
- **Allowed RODC Password Replication Group**
- **Cert Publishers**
- **Cloneable Domain Controllers**
- **Denied RODC Password Replication Group**
- **DnsAdmins**
- **DnsUpdateProxy**
- **Domain Admins**
- **Domain Computers**
- **Domain Controllers**
- **Enterprise Admins**
- **Enterprise Key Admins**
- **Enterprise Read-only Domain Controllers**
- **Group Policy Creator Owners**
- **Key Admins**
- **krbtgt**
- **Protected Users**
- **RAS and IAS Servers**
- **Read-only Domain Controllers**
- **Schema Admins**

- **Configuring audit for Active Directory Certificate Services, certificate templates, and certificate objects**

To maximize efficiency of Kaspersky Managed Detection and Response, you need to configure audit for the **Active Directory Certificate Services** service, certificate templates, and objects on the hosts with **Active Directory Certificate Services** (AD CS) enabled.

*To configure audit for the **Active Directory Certificate Services** service:*

1. Press **Win+R** to open the **Run** window.
2. In the **Open** field, type in `cmd`, and then press **Enter** or click **OK**. The **Command Prompt** window appears.
3. To configure audit settings for Certification Authority, enter the commands below, and then press Enter:  
`certutil -setreg CA\AuditFilter 127`  
`certutil -setreg policy\EditFlags +EDITF_AUDITCERTTEMPLATELOAD`
4. To restart the **Certificate Services** service, enter the command below, and then press Enter:  
`net stop certsvc && net start certsvc`

*To configure security auditing for certificate templates:*

1. Press **Win+R** to open the **Run** window.
2. In the **Open** field, type in `adsiedit.msc`, and then press **Enter** or click **OK**.
3. Right-click **ADSI Edit**, and then select **Connect to**.
4. In the **Connection Point** section, select the **Configuration** value in the Select a **Well Known Naming Context** field.
5. Double click **Configuration/Schema** on the left pane.
6. Select the **CN=Configuration,DC=...** → **CN=Services** → **CN=Public Key Services** → **CN=Certificate Templates** folder.
7. Right-click the **CN=Certificate Templates** folder, select **Properties**, and then open the **Security** tab.
8. Click the **Advanced** button, and then select the **Auditing** tab.
9. Click the **Everyone** principal, select the **Write all properties**, **Delete**, **Modify permissions**, **Modify owner**, **All validated writes** checkboxes, and then click **OK**.

*To configure security auditing for NTAuthCertificates object:*

1. In the **Open** field, type `adsiedit.msc`, and then press **Enter** or click **OK**.
2. Right-click **ADSI Edit**, and then select **Connect to**.
3. In the **Connection Point** section, select the **Configuration** value in the Select a **Well Known Naming Context** field.
4. Double click **Configuration/Schema** on the left pane.
5. Select the **CN=Configuration,DC=...** → **CN=Services** → **CN=Public Key Services** → **CN=NTAuthCertificates** folder.

6. Right-click the **CN=NTAuthCertificates** folder, select **Properties**, and then open the **Security** tab.
7. Click the **Advanced** button, and then select the **Auditing** tab.
8. Click the **Everyone** principal, select the **Write all properties**, **Delete**, **Modify permissions**, **Modify owner**, **All validated writes** checkboxes, and then click **OK**.

# Onboarding video

Watch the video to learn more about the main features of the MDR solution.



MDR Solution. Onboarding video